

EX 1009

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Netskope hereby provides the following preliminary claim chart relating the accused Fortinet product and/or service “FortiEDR and FortiWeb Cloud products,” and all products that operate in a similar matter, to the asserted claims FortiEDR and FortiWeb Cloud products infringe. The claim chart below includes exemplary evidence demonstrating infringement of Claims 1-22 of U.S. Pat. No. 7,593,936 (the “’936 Patent.”) by FortiEDR and FortiWeb Cloud products.

On information and belief, Netskope asserts direct and/or indirect infringement of the ’936 Patent by FortiEDR and FortiWeb Cloud products. To the extent any limitation of the asserted claims is not met literally, such limitation is met under the doctrine of equivalents. On information and belief and unless otherwise noted, predecessors and previous versions of FortiEDR and FortiWeb Cloud products operate in the same or substantially the same way as that set forth in the present chart and are also accused. In addition, Netskope has not identified any differences between versions of FortiEDR and FortiWeb Cloud products that are material to infringement. These infringement contentions are based upon information available to Netskope, and Netskope’s reasonable diligence in reviewing this information, as of the date of these contentions. Netskope’s investigation is ongoing and discovery has not yet concluded. Netskope reserves the right to supplement its infringement contentions based on review and analysis of information provided to date and Fortinet’s responses to Netskope’s discovery requests and document productions, the testimony of knowledgeable witnesses, and expert testimony. Netskope reserves the right to amend and/or modify these contentions as discovery in this case progresses, including as otherwise permitted by the Patent Local Rules, procedural schedule, or any other applicable order of the Court.

U.S. Patent No. 7,593,936	Fortinet’s FortiEDR and FortiWeb Cloud Products – Representative Evidence
1(pre) A method of detecting abnormal system states in computers, comprising:	FortiEDR and FortiWeb Cloud detect abnormal system states in computers. <i>See, e.g.:</i> <u>FortiEDR</u> “Threat Hunting FortiEDR’s threat-hunting capabilities features a set of software tools and information sources focused on detecting, investigating, containing and mitigating suspicious activities on end-user devices.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	FortiEDR provides post- and pre-infection endpoint protection management, while delivering high detection rates with realtime blocking and response capabilities when compared to traditional Endpoint Detection and Response (EDR) tools. FortiEDR provides malware classification, displays Indicators of Compromise (IOCs) and delivers full attack-chain views – all while simultaneously enabling users to conduct further threat hunting, if and when needed.”¹ “FortiEDR Collector The FortiEDR Collector is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers. By default, the Collector runs in autonomous mode. Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate. You can configure the Collector to use a Core for the metadata analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.”² <u>FortiWeb Cloud</u> “Anomaly Detection Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks: • Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
--	--

¹ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/354083/introducing-fortiedr>.

² <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/970632/fortiedr-components>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

Model settings

FortiWeb Cloud parses all the URLs in a domain, and builds anomaly detection models for all parameters attached to the URLs.

After anomaly detection model is built, the system will keep on calculating the probability of the new samples and compare it against the model. If the probability of the new samples varies to a large extent for a long period, the system determines this parameter has changed and automatically rebuilds the model based on the new samples.

To configure anomaly detection:

1. Go to **SECURITY RULES> Anomaly Detection**.
You must have already enabled this module in **Add Modules**. See [How to add or remove a module](#).
2. Configure the following settings.

IP List Type

- **Trust:** The system will collect samples only from the IP ranges in the **Source IP list**.
- **Block:** The system will collect sample from any IP addresses except the ones in the **Source IP list**.

Whichever option you choose, if you leave the **Source IP list** blank, the system will collect traffic data samples from any IP address.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Source IP List Click Create New to list the IP ranges of the samples. Depending on whether you select Trust or Block, FortiWeb Cloud will or will not collect samples from the specified IP ranges. 3. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the Advanced Configuration in Global > System Settings > Settings. <table> <tr> <td>Alert</td><td>Accept the request and generate a log message.</td></tr> <tr> <td>Alert & Deny</td><td>Block the request (or reset the connection) and generate a log message.</td></tr> </table> 4. Click SAVE.³	Alert	Accept the request and generate a log message.	Alert & Deny	Block the request (or reset the connection) and generate a log message.
Alert	Accept the request and generate a log message.				
Alert & Deny	Block the request (or reset the connection) and generate a log message.				
1(a) receiving snapshots from a plurality of computers within a population of computers,	FortiEDR and FortiWeb Cloud receive snapshots from a plurality of computers within a population of computers. <i>See, e.g.:</i> <u>FortiEDR</u> “FortiEDR Collector The FortiEDR Collector is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers. By default, the Collector runs in autonomous mode. Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate. You can configure the Collector to use a Core for the metadata				

³ <https://docs.fortinet.com/document/fortiweb-cloud/23.3.0/user-guide/81976/anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.”⁴ “How does FortiEDR work?” 1. The FortiEDR Collector collects OS metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device. 2. Communicating device makes a connection establishment request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established. 3. The FortiEDR Core identifies malicious requests: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies. 4. Pass or block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked. 5. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog. 6. Forensic analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”⁵ FortiWeb Cloud
--	---

⁴ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/970632/fortiedr-components>.

⁵ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/717228/how-does-fortiedr-work>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	For example, FortiWeb Cloud “captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access.” At least those inputs are “snapshots.”⁶ Anomaly Detection Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks: • Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access • Matches anomalies against pre-trained threat models • Detects attacks Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service. 7
1(a)(i) wherein individual snapshots include data indicating a state of a respective computer;	FortiEDR and FortiWeb Cloud disclose individual snapshots that include data indicating a state of a respective computer. <i>See, e.g:</i> <u>FortiEDR</u> “FortiEDR Collector

⁶ <https://docs.fortinet.com/document/fortiweb-cloud/23.3.0/user-guide/81976/anomaly-detection>.

⁷ *Id.*

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	The FortiEDR Collector is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers. By default, the Collector runs in autonomous mode. Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate. You can configure the Collector to use a Core for the metadata analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.”⁸ “FortiEDR Core The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked. FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows. • When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious. • When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it. • The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization’s policy by blocking (or only logging) the connection request in order to prevent/log exfiltration. • The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred. • When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
--	---

⁸ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/970632/fortiedr-components>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.”⁹

FortiWeb Cloud

For example, FortiWeb Cloud “captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access.” At least those inputs are “snapshots.”¹⁰

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

11

⁹ *Id.*

¹⁰ <https://docs.fortinet.com/document/fortiweb-cloud/23.3.0/user-guide/81976/anomaly-detection>.

¹¹ *Id.*

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

1(b) automatically generating an adaptive reference model comprising a rule set customized to characteristics of the population of computers,	FortiEDR and FortiWeb Cloud automatically generate an adaptive reference model comprising a rule set customized to characteristics of the population of computers. <i>See, e.g.:</i> <u>FortiEDR</u> “Out-of-the-box policies FortiEDR provides out-of-the-box policies. Each policy comes with multiple highly intelligent rules that enforce it. eXtended Detection Policy: This policy provides visibility into data across multiple security systems and identifies abnormal or malicious activity by applying analytics and correlating data from various systems. Events are logged and displayed in the Event Viewer. No blocking options are provided. The exceptions and forensics options are not available in the Event Viewer for security events triggered by this policy.”¹² “eXtended detection source integration To connect to external systems in order to collect activity data, you must add a new connector for extended detection, which will automatically collect activity logs and activity data from external systems. Currently, this feature connects to a FortiAnalyzer device type, which collects the logs from other systems, such as firewalls, Active Directory and other security products. The aggregated data is then being sent to Fortinet Cloud Services (FCS) where it is correlated and analyzed to detect malicious indications that will result in security events of eXtended Detection policy rule violations.”¹³
--	--

¹² <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/236616/out-of-the-box-policies>.

¹³ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/176732/extended-detection-source-integration>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiWeb Cloud

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

14

For example, FortiWeb Cloud “captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access.”¹⁵

¹⁴ <https://docs.fortinet.com/document/fortiweb-cloud/23.3.0/user-guide/81976/anomaly-detection>.

¹⁵ *Id.*

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	At least the “mathematical model of allowed access” is an adaptive reference model comprising a rule set. The “mathematical model of allowed access” is a reference model, at least because it is a model of normal activity (“normal user behavior” and “allowed access”) that can be referred to for later anomaly detection. The “mathematical model of allowed access” is adaptive at least because FortiWeb Cloud “automatically and continuously builds and maintains” the model.¹⁶ The “mathematical model of allowed access” is “customized to characteristics of the population of computers,” at least based on the mathematical model of allowed access being built based on the inputs captured and collected for the computers.¹⁷
1(b)(i) the rule set being developed by identifying patterns among the snapshots from the plurality of computers such that the adaptive reference model is indicative of normal states in the computers within the population; and	FortiEDR and FortiWeb Cloud disclose the rule set being developed by identifying patterns among the snapshots from the plurality of computers such that the adaptive reference model is indicative of normal states in the computers within the population. <i>See, e.g.:</i> <u>FortiEDR</u> “Out-of-the-box policies FortiEDR provides out-of-the-box policies. Each policy comes with multiple highly intelligent rules that enforce it. eXtended Detection Policy: This policy provides visibility into data across multiple security systems and identifies abnormal or malicious activity by applying analytics and correlating data from various systems. Events are logged and displayed in the Event Viewer. No blocking options are provided. The exceptions and forensics options are not available in the Event Viewer for security events triggered by this policy.”¹⁸

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/236616/out-of-the-box-policies>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiWeb Cloud

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

19

The rule set in the “mathematical model of allowed access” is developed by identifying patterns among the snapshots from the plurality of computers, at least because the “mathematical model of allowed access” is built based on the snapshots (“captures and collects inputs”) and because the “mathematical model of allowed access” is built and maintained based on those inputs to be a “model of normal user behavior.”²⁰

¹⁹ <https://docs.fortinet.com/document/fortiweb-cloud/23.3.0/user-guide/81976/anomaly-detection>.

²⁰ *Id.*

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	The “mathematical model of allowed access” is indicative of normal states in the computers within the population, at least because it models normal behavior on the protected computers (“Machine learning automatically and continuously builds and maintains a model of normal user behavior”; “to build a mathematical model of allowed access”).²¹
1(c) comparing a snapshot from at least one of the computers to the adaptive reference model to determine whether an anomaly is present in the state of the at least one of the computers.	FortiEDR and FortiWeb Cloud compare a snapshot from at least one of the computers to the adaptive reference model to determine whether an anomaly is present in the state of the at least one of the computers. <i>See, e.g.:</i> <u>FortiEDR</u> “FortiEDR Core The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked. FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows. • When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious. • When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it. • The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization’s policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.

²¹ *Id.*

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.”²²

“How does FortiEDR work?

1. The FortiEDR Collector collects OS metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.
2. Communicating device makes a connection establishment request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established.
3. The FortiEDR Core identifies malicious requests: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies.
4. Pass or block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked.
5. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog.
6. Forensic analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”²³

FortiWeb Cloud

For example, FortiWeb Cloud uses the “mathematical model of allowed access” to “identify malicious application traffic.” FortiWeb Cloud uses the model to determine “whether a request is legitimate or a potential malicious attack attempt,” including by “match[ing] anomalies against pre-trained threat models.”²⁴

²² <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/970632/fortiedr-components>.

²³ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/717228/how-does-fortiedr-work>.

²⁴ <https://docs.fortinet.com/document/fortiweb-cloud/23.3.0/user-guide/81976/anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Anomaly Detection Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks: • Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access • Matches anomalies against pre-trained threat models • Detects attacks Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service. 25
2(pre) The method of claim 1, further comprising: comparing the anomaly to a recognition filter to diagnose a trouble condition on the at least one of the computers; and	FortiEDR and FortiWeb Cloud compare the anomaly to a recognition filter to diagnose a trouble condition on the at least one of the computers. <i>See, e.g.:</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional

²⁵ *Id.*

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”²⁶ “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution • Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups) • Gain full visibility of the attack chain and malicious changes with patented code tracing • Automate cleanup and roll back malicious changes while preserving system uptime • Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords
--	--

²⁶ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- Get additional help with the optional managed detection and response (MDR) service”²⁷

“Pre- and Post-infection Real-time Endpoint Threat Protection

FortiEDR can help protect retail organizations from constant threats, whether attackers are trying to steal customer financial data or sabotage operations. Its capabilities include:

- **Proactive attack surface risk mitigation.** FortiEDR delivers advanced automated attack surface policy control with vulnerability assessments and Internet-of-Things (IoT) security.
- **Malware prevention.** A machine-learning (ML) antivirus engine helps stop malware pre-execution. This cross-operating system NGAV capability is configurable and comes built into the single, lightweight agent, so users can assign anti-malware protection to any endpoint group without requiring additional installation.
- **Real-time automated breach protection.** FortiEDR detects suspicious process flows and behaviors and immediately defuses potential threats by blocking outbound communications and access to the file system from suspicious processes, which prevents data exfiltration, command-and-control communications, file tampering, and ransomware encryption. At the same time, the FortiEDR back end continues to gather additional evidence, enrich event data, and classify the incidents. The solution surgically stops data breach and ransomware damage in real time to automatically keep the business running even on devices that have been compromised.
- **Customizable incident response.** With FortiEDR, you can orchestrate incident response operations using tailor-made playbooks with cross-environment insights. You can streamline incident response and remediation processes and manually or automatically roll back malicious changes done by already contained threats on a single device or on devices across the environment.
- **Guided interface with data enrichment.** FortiEDR automatically enriches data with detailed information on malware both pre- and post-infection to conduct forensics on infiltrated endpoints. This unique interface provides helpful guidance, recommends best practices, and suggests the next logical steps for security analysts.

Retailers that use FortiEDR also benefit from the Fortinet Security Fabric architecture and integration with other components of the Security Fabric, including FortiGate, FortiSandbox, and FortiSIEM.

Detection and Remediation Without the Aggravation

²⁷ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

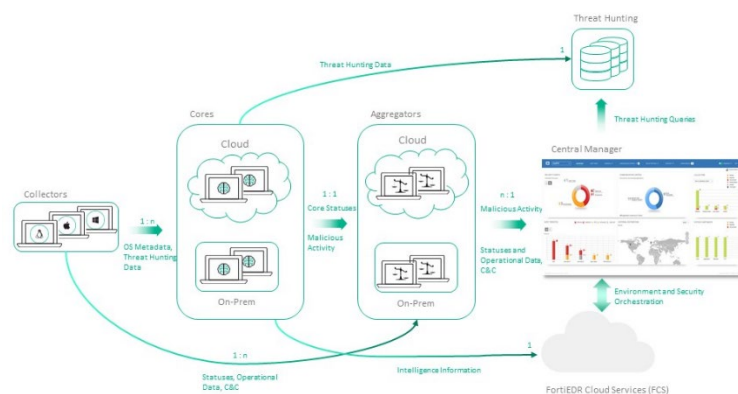
Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

With FortiEDR, retail organizations can strategically reduce the complexity and cost associated with the detection and remediation of advanced malware across POS and other endpoints. In addition, FortiEDR minimizes incident response time pressures and alert fatigue, while preventing the exploitation of vulnerable endpoints that commonly leads to data breaches and disruption from cyberattacks.”²⁸

“Overview

The FortiEDR platform is a distributed architecture that collects the connection establishment flow of your organization’s communicating devices directly from each device’s operating system internals. FortiEDR analyzes the flow of events that preceded the connection establishment and determines whether the connection establishment request was malicious. The system can enforce your organization’s policy by blocking the connection establishment request in order to prevent exfiltration.

The FortiEDR platform is comprised of the following components:



FortiEDR Collector

The FortiEDR Collector is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers.

²⁸ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-retail-edr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

By default, the Collector runs in autonomous mode. Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate. You can configure the Collector to use a Core for the metadata analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.

- Pass: Legitimate requests are allowed with extremely negligible latency.
- Block: Malicious exfiltration and file changing attempts are blocked.

A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows, macOS, and Linux systems. The following are the connections established between the FortiEDR Collector and other FortiEDR components:

- To the FortiEDR Aggregator: The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health, status information, and security events.
- From the FortiEDR Aggregator: The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.
- To the FortiEDR Core: The FortiEDR Collector sends the following information:
 - Compressed activity events that are later used for Threat Hunting
 - Communication-related data to be used for the Communication Control
 - (Non-autonomous mode only) Metadata for determining whether a specific action should be blocked or passed
- From the FortiEDR Core: The FortiEDR Collector receives connection establishment authorization or denial (blocking) from the FortiEDR Core.

FortiEDR Core

The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.

One or more FortiEDR Cores are required, according to the size of your network based on deployment size (up to 50 FortiEDR Cores). Refer to Appendix C – ON PREMISE DEPLOYMENTS for the exact specifications of the system requirements.) The following are the connections established between the FortiEDR Core and other FortiEDR components:

- **To the FortiEDR Aggregator:** The FortiEDR Core sends registration information the first time it connects to the FortiEDR Aggregator and then sends events and ongoing health and status information.
- **From the FortiEDR Aggregator:** The FortiEDR Core receives its configuration from the FortiEDR Aggregator.

The FortiEDR Core is located on exit points from your organization. It only reviews FortiEDR Collector metadata; it does not see the outgoing traffic. It is a central Linux-based software-only entity that can run on any workstation or VM that is assigned with a static IP address.

FortiEDR Cloud Service

The FortiEDR Cloud Service (FCS) enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event. The FCS is a cloud-based, GDPR-compliant, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy.

The FCS security event classification process is done via data enrichment and enhanced deep, thorough analysis and investigation, enabled by automated and manual processes. The enhanced processes may include (partial list)

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

intelligence services, file analysis (static and dynamic), sandboxing, flow analysis via machine learning, commonalities analysis, crowdsourced data deduction and more.

Along with potential classification reassurance or reclassification, once connected, FCS can also enable several followed actions, which can be divided into two main activities:

- Tuning: Automated security event exception (allowlisting). After a triggered security event is reclassified as Safe, an automated cross-environment exception can be pushed downstream and expire the event, preventing it from triggering again. For more details, see Exception Manager
- Playbook Actions: All Playbook policy remediation actions are based on the final determination of the FCS. For more details see Remediation.”²⁹

“FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”³⁰

“Real-time automated response. When FortiEDR detects potentially malicious processes, it defuses them in real time with automatic blocking. At the same time, the Fortinet Cloud Service continues to gather evidence, validate, and classify the events with its multiple sandboxes and code tracing technologies. Customized playbooks allow security teams to prescribe automated actions based on endpoint group, mission criticality, and threat classification. Automated response and remediation actions may include terminating processes, deleting malicious or infected files, cleaning up persistency, notifying users, and forwarding event logs to a syslog server. This all helps FortiEDR eliminate alert fatigue and breach anxiety, standardize incident response procedures, and optimize security and operations resources.

²⁹ <https://docs.fortinet.com/document/fortiedr/7.0.0/administration-guide/970632/fortiedr-components>.

³⁰ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiEDR—Cloud-native EPP + EDR

Detect, Defuse, Respond, and Remote Remediation

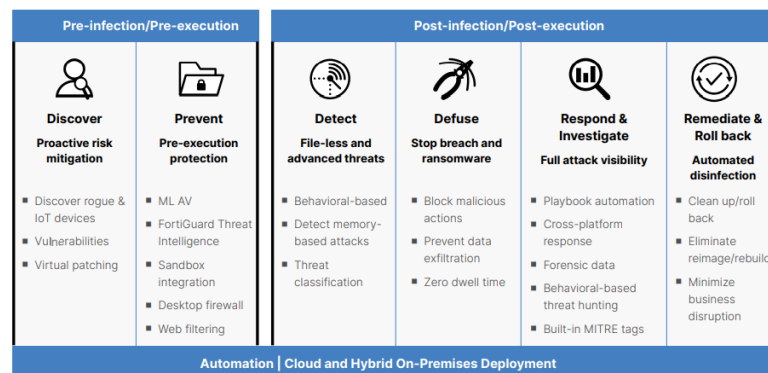


Figure 1: FortiEDR combines both pre-infection and post-infection endpoint defenses.

“How Does FortiEDR Work?”

1. The FortiEDR Collector Collects OS Metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.
2. Communicating Device Makes a Connection Establishment Request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established.
3. The FortiEDR Core Identifies Malicious Requests: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies.
4. Pass or Block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked.
5. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is

³¹ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog.

Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”³²

FortiWeb Cloud

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

7. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

³² <https://docs.fortinet.com/document/fortiedr/5.0.0/administration-guide/717228/how-does-fortiedr-work>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Block mode On Applications page, you can turn on/off the Block Mode for each application. When to enable block mode • When Block Mode is enabled, FortiWeb Cloud will take actions as specified in Action of each WAF module. blocks requests if they trigger violations. Your application server does not receive these requests. • When Block Mode is disabled, FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests. Check the following prerequisites before you enable the Block Mode: • The endpoints and servers are configured properly. The traffic flow between the clients, FortiWeb Cloud, and your application servers is stable. • Observe the attack logs in FortiView or Logs. If legitimate traffic is falsely detected as attacks (also called false positives), add exceptions or modify the web protection configurations to avoid false positives in the future. 33 Action When you have enabled Advanced Configuration in Global > System Settings > Settings, you can configure actions for each WAF feature specifically. If Advanced Configuration is disabled, the default actions of each WAF feature will work instead. When Block Mode is disabled, FortiWeb Cloud will accept all requests and generate logs for all violations without considering the specified actions in each WAF feature. When Block Mode is enabled, all requests will be blocked if they trigger the violation, and the specific actions you have configured in each WAF feature will prevail. For example, if you set the Action for Known Attacks as Alert & Deny, FortiWeb Cloud will block the request (or reset the connection) and generate a log message. “How an anomaly detection model is built?” FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html;
--	--

³³ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- The request packet must have parameter(s) in URL or body.

When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples.

FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it.

Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built:

- If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model.
- If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable.

The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced.

Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page.

Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting.

To create an Anomaly Detection policy:

1. Click Policy > Server Policy.
2. Select an existing server policy.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

3. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy.
4. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens.
5. Click the + (Add) sign after the Domain field to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains.
6. Select whether to trust or block the specified source IP addresses.
7. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range.
8. Click OK.

After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”³⁴

“Machine learning

Starting with the 6.0 release, FortiWeb offers a machine-learning function that enables it to automatically detect malicious web traffic and bots . In addition to detecting known attacks, the feature can detect potential unknown zero-day attacks to provide real-time protection for web servers.

Machine Learning is intended to replace Auto Learn, which is now removed from 6.1 release.

Anomaly detection

The anomaly detection model of machine learning feature observes the URLs, parameters, and HTTP Method of HTTP and/or HTTPS sessions passing to your web servers. It builds mathematical models to detect abnormal traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Observes the HTTP method of the traffic
- Matches anomalies against pre-trained threat models
- Detects attacks

³⁴ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiWeb employs two layers of machine learning to detect malicious attacks. The first layer uses the Hidden Markov Model (HMM) and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method. Once completed, it will verify every request against the model to determine whether it's an anomaly or not.

Once the first layer of machine learning triggers a request as an anomaly, FortiWeb will use the second layer of machine learning to verify whether it's a real attack or just a benign anomaly that should be ignored. To do so, FortiWeb includes pre-built trained threat models. Each represents a certain attack category, such as SQL Injection, Cross-site Scripting, and so on. Each threat model is already trained based on analysis of thousands of attack samples. Threat models are continuously updated using the FortiWeb Security Service. When new attack types are released, the FortiGuard team analyzes the new threats and re-trains the relevant threat model. The new threat model is then pushed to all customer installations in a way similar to how signatures are updated.

Bot detection

The AI-based machine learning bot detection model complements the existing signature and threshold based rules. It detects sophisticated bots that can sometimes go undetected. The bot detection model observes user behaviors from thirteen dimensions, for example, how many times of HTTP requests are initiated by the user, whether the request uses illegal HTTP versions, whether it fetches JSON/XML resources, etc.

Compared with the traditional mechanisms to detect bots, the bot detection model saves you the trouble to experiment on an appropriate threshold to detect abnormal user behaviors. For example, how could you know how many times of HTTP requests initiated by a user should be considered as abnormal? With the traditional mechanism, you may need to experiment on different threshold values and continuously check the attack log until no related attack logs are reported for the regular traffic.

Things are much easier if you use the bot detection model. FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model that self-learns the traffic profiles of regular clients. When the traffic from a new client flows in, it is compared against that of the regular clients. If they don't match, the bot detection model classifies the new client as an anomaly. When the traffic profiles of the regular clients vary dramatically (e.g. the functions of your application have changed, so that users behave differently when they visit your application), FortiWeb automatically refreshes the bot detection model to adapt to the changes.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Moreover, test shows that the bot detection model performs much better, specially when it detects crawlers and scrapers. The traffic is comprehensively evaluated from 13 dimensions. It helps increase the detection accuracy and decrease the false positive rate.”³⁵ “How an anomaly detection model is built? FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html; • The request packet must have parameter(s) in URL or body. When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples. FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it. Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built: • If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model. • If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable. The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of
--	---

³⁵ <https://docs.fortinet.com/document/fortiweb/6.3.23/administration-guide/193258>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced. Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page. Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting. To create an Anomaly Detection policy: 1. Click Policy > Server Policy. 2. Select an existing server policy. 3. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy. 4. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens. 5. Click the + (Add) sign after the Domain filed to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains. 6. Select whether to trust or block the specified source IP addresses. 7. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range. 8. Click OK. After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”³⁶
2(a) in the event of a trouble condition, generating an	FortiEDR and FortiWeb Cloud, in the event of a trouble condition, generate an automated response to the trouble condition.

³⁶ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

automated response to the trouble condition.	<i>See, e.g.:</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”³⁷ “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution • Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
--	--

³⁷ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords
- Get additional help with the optional managed detection and response (MDR) service”³⁸

“Pre- and Post-infection Real-time Endpoint Threat Protection

FortiEDR can help protect retail organizations from constant threats, whether attackers are trying to steal customer financial data or sabotage operations. Its capabilities include:

- **Proactive attack surface risk mitigation.** FortiEDR delivers advanced automated attack surface policy control with vulnerability assessments and Internet-of-Things (IoT) security.
- **Malware prevention.** A machine-learning (ML) antivirus engine helps stop malware pre-execution. This cross-operating system NGAV capability is configurable and comes built into the single, lightweight agent, so users can assign anti-malware protection to any endpoint group without requiring additional installation.
- **Real-time automated breach protection.** FortiEDR detects suspicious process flows and behaviors and immediately defuses potential threats by blocking outbound communications and access to the file system from suspicious processes, which prevents data exfiltration, command-and-control communications, file tampering, and ransomware encryption. At the same time, the FortiEDR back end continues to gather additional evidence, enrich event data, and classify the incidents. The solution surgically stops data breach and ransomware damage in real time to automatically keep the business running even on devices that have been compromised.
- **Customizable incident response.** With FortiEDR, you can orchestrate incident response operations using tailor-made playbooks with cross-environment insights. You can streamline incident response and remediation processes and manually or automatically roll back malicious changes done by already contained threats on a single device or on devices across the environment.

³⁸ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- **Guided interface with data enrichment.** FortiEDR automatically enriches data with detailed information on malware both pre- and post-infection to conduct forensics on infiltrated endpoints. This unique interface provides helpful guidance, recommends best practices, and suggests the next logical steps for security analysts.

Retailers that use FortiEDR also benefit from the Fortinet Security Fabric architecture and integration with other components of the Security Fabric, including FortiGate, FortiSandbox, and FortiSIEM.

Detection and Remediation Without the Aggravation

With FortiEDR, retail organizations can strategically reduce the complexity and cost associated with the detection and remediation of advanced malware across POS and other endpoints. In addition, FortiEDR minimizes incident response time pressures and alert fatigue, while preventing the exploitation of vulnerable endpoints that commonly leads to data breaches and disruption from cyberattacks.”³⁹

FortiWeb Cloud

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

³⁹ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-retail-edr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

7. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

Block mode

On **Applications** page, you can turn on/off the **Block Mode** for each application.

When to enable block mode

- When Block Mode is enabled, FortiWeb Cloud will take actions as specified in Action of each WAF module. blocks requests if they trigger violations. Your application server does not receive these requests.
- When Block Mode is disabled, FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests.

Check the following prerequisites before you enable the Block Mode:

- The **endpoints** and **servers** are configured properly. The traffic flow between the clients, FortiWeb Cloud, and your application servers is stable.
- Observe the attack logs in **FortiView** or **Logs**. If legitimate traffic is falsely detected as attacks (also called false positives), add exceptions or **modify the web protection configurations** to avoid false positives in the future.

40

Action

When you have enabled **Advanced Configuration** in **Global > System Settings > Settings**, you can configure actions for each WAF feature specifically. If **Advanced Configuration** is disabled, the default actions of each WAF feature will work instead.

When Block Mode is disabled, FortiWeb Cloud will accept all requests and generate logs for all violations without considering the specified actions in each WAF feature.

When Block Mode is enabled, all requests will be blocked if they trigger the violation, and the specific actions you have configured in each WAF feature will prevail. For example, if you set the Action for Known Attacks as Alert & Deny, FortiWeb Cloud will block the request (or reset the connection) and generate a log message.

“How an anomaly detection model is built?”

⁴⁰ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain.

The traffic should meet all of the following conditions to be treated as a sample:

- The response code of response packet must be 200 or 302;
- The response content-type of response packet must be text or html;
- The request packet must have parameter(s) in URL or body.

When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples.

FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it.

Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built:

- If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model.
- If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable.

The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced.

Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting. To create an Anomaly Detection policy: 1. Click Policy > Server Policy. 2. Select an existing server policy. 3. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy. 4. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens. 5. Click the + (Add) sign after the Domain field to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains. 6. Select whether to trust or block the specified source IP addresses. 7. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range. 8. Click OK. After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁴¹
3(pre) The method of claim 2, wherein the automated response is a generic response not specific to a particular asset of the at least one computer, and	FortiEDR and FortiWeb Cloud’s automated response is a generic response not specific to a particular asset of the at least one computer. <i>See, e.g.:</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential

⁴¹ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

wherein the method further comprises:	threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR's back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁴² “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution • Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups) • Gain full visibility of the attack chain and malicious changes with patented code tracing • Automate cleanup and roll back malicious changes while preserving system uptime
---------------------------------------	---

⁴² <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords • Get additional help with the optional managed detection and response (MDR) service”⁴³ “How Does FortiEDR Work? 6. The FortiEDR Collector Collects OS Metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device. 7. Communicating Device Makes a Connection Establishment Request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established. 8. The FortiEDR Core Identifies Malicious Requests: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies. 9. Pass or Block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked. 10. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog. Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”⁴⁴ FortiWeb Cloud
--	--

⁴³ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

⁴⁴ <https://docs.fortinet.com/document/fortiedr/5.0.0/administration-guide/717228/how-does-fortiedr-work>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

7. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Block mode On Applications page, you can turn on/off the Block Mode for each application. When to enable block mode • When Block Mode is enabled, FortiWeb Cloud will take actions as specified in Action of each WAF module. blocks requests if they trigger violations. Your application server does not receive these requests. • When Block Mode is disabled, FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests. Check the following prerequisites before you enable the Block Mode: • The endpoints and servers are configured properly. The traffic flow between the clients, FortiWeb Cloud, and your application servers is stable. • Observe the attack logs in FortiView or Logs. If legitimate traffic is falsely detected as attacks (also called false positives), add exceptions or modify the web protection configurations to avoid false positives in the future. Action When you have enabled Advanced Configuration in Global > System Settings > Settings, you can configure actions for each WAF feature specifically. If Advanced Configuration is disabled, the default actions of each WAF feature will work instead. When Block Mode is disabled, FortiWeb Cloud will accept all requests and generate logs for all violations without considering the specified actions in each WAF feature. When Block Mode is enabled, all requests will be blocked if they trigger the violation, and the specific actions you have configured in each WAF feature will prevail. For example, if you set the Action for Known Attacks as Alert & Deny, FortiWeb Cloud will block the request (or reset the connection) and generate a log message. “How an anomaly detection model is built?” FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html; • The request packet must have parameter(s) in URL or body.
--	--

⁴⁵ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples. FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it. Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built: • If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model. • If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable. The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced. Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page. Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting. To create an Anomaly Detection policy: 1. Click Policy > Server Policy. 2. Select an existing server policy. 3. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy.
--	---

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	4. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens. 5. Click the + (Add) sign after the Domain field to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains. 6. Select whether to trust or block the specified source IP addresses. 7. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range. 8. Click OK. After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁴⁶
3(a) sending the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of anomalies indicating assets of the at least one computer whose states are anomalous; and	FortiEDR and FortiWeb Cloud send the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of anomalies indicating assets of the at least one computer whose states are anomalous. <i>See, e.g.:</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁴⁷ “Respond and Remediate

⁴⁶ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

⁴⁷ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution • Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups) • Gain full visibility of the attack chain and malicious changes with patented code tracing • Automate cleanup and roll back malicious changes while preserving system uptime • Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords • Get additional help with the optional managed detection and response (MDR) service”⁴⁸ “How Does FortiEDR Work? 11. The FortiEDR Collector Collects OS Metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device. 12. Communicating Device Makes a Connection Establishment Request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the
--	--

⁴⁸ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established. 13. The FortiEDR Core Identifies Malicious Requests: Using FortiEDR's patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies. 14. Pass or Block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked. 15. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog. 16. Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”⁴⁹ FortiWeb Cloud
--	--

⁴⁹ <https://docs.fortinet.com/document/fortiedr/5.0.0/administration-guide/717228/how-does-fortiedr-work>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Logs

FortiWeb Cloud saves the attack logs for two months and the audit logs for three months. After that, they will be deleted. Exceptions are added in Attack Logs. It can't be reversed once being added.

If you believe that the Anomaly Detection model is inaccurate with certain exceptions, you have the option to access the TreeView page of the Anomaly Detection module. From there, you can locate the parameter to which the exception is applied and rebuild the model specifically for that parameter. When the new model is rebuilt, the exceptions added to the Anomaly Detection attack logs corresponding to that parameter will be cleared.

In the scanning process, when a request passes through different modules in sequence, the configured action for certain modules can be set to "Alert" or "Monitor". In this case, if an attack is detected by a module with such an action, it will allow the request to continue to the next module for further scanning. However, an attack log will be generated by the module that identified the attack.

As the request progresses through subsequent modules, it is possible for the attack to be logged multiple times by different preceding modules before it is blocked by a module with a different action, such as "Block Period" or "Deny".

As for the scan sequence, please refer to <https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/234292/sequence-of-scans>.

If the `https_host` in GEO IP attack logs shows `none`, it can be solved by enabling **Use X-Header to Identify Original Clients' IP** and **Add X-Forwarded-For** in the **Rewriting Requests** module.

To observe the client's original source IP, it is advised to enable the **Rewriting Requests** module, turning on **X-Forwarded-For**, **X-Real-IP**, and **Use X-Header to Identify Original Clients' IP** options.

Logs are sent from FortiWeb Cloud to the origin server, so the `IP` header (layer 3) of the logs is supposed to be FortiWeb Cloud's IP address. This is expected behavior.

To check the client real IP, you need to find it in the `X-Forwarded-For` or `X-Real-IP` header in the packets forwarded from FortiWeb Cloud to your server. Be aware that to record the client real IP it's required to enable both **Add X-Forwarded-For** and **Use X-Header to Identify Original Client's IP** in the **Rewriting Requests** module.

The signatures used in Known Attacks are primarily designed to detect known patterns of malicious code. However, they may not cover all variants or newly emerging forms of attacks.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	In cases where an attack is logged under the Anomaly Detection threat type instead of being matched with a signature, it in fact indicates the successful functioning of the machine learning model in Anomaly Detection. It effectively screened out unknown or new variant attacks that do not align with existing signatures. You can view the blocked requests in three places: 1) Attack Logs; 2) FortiView ; 3) Blocked Requests widget on Dashboard. The ways they count the blocked requests are slightly different. • To prevent Information Leakage, FortiWeb Cloud may cloak the error pages or erase sensitive HTTP headers in response packets. Such item are logged only once per minute in Attack Logs and FortiView for you to know the Information Leakage rule took effect. In the meanwhile, the actual count is recorded in Blocked Requests Widget. • If you have set FortiWeb Cloud to block attacks but do not generate a log when certain violation occurs, such as Alert & Deny (no log), then the attacks will not be logged in Attack Logs and FortiView , but will be counted in the Blocked Requests widget. • The invalid requests to the host header HOST will be blocked without generating any log. • When the Block Mode is in disabled state, attacks won't be blocked but logs are generated. If you have set FortiWeb Cloud to block attacks but not generate a log when certain violation occurs, such as 'Alert & Deny (no log)', then the attacks will not be logged in Attack Logs and FortiView but will be counted in the Blocked Requests widget. If you need to have detailed logs for auditing or analysis purposes, you may consider using a different action, such as 'Alert & Deny' or 'Block Period', which will not only block the request but also generate a log entry. To identify the security feature blocking your request, map the Attack ID value to the corresponding description in the table below. “Select a trigger policy that you have set in Log&Report > Log Policy > Trigger Policy. If potential or definite anomaly or HTTP Method Violation is detected, it will trigger the system to send email and/or log messages according to the trigger policy.”⁵¹
3(b) applying the generic response to the anomalous assets to correct the trouble condition.	FortiEDR and FortiWeb Cloud apply the generic response to the anomalous assets to correct the trouble condition. <i>See, e.g.:</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested.

⁵⁰ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

⁵¹ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR's back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁵² “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution • Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups) • Gain full visibility of the attack chain and malicious changes with patented code tracing • Automate cleanup and roll back malicious changes while preserving system uptime • Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords
--	--

⁵² <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• Get additional help with the optional managed detection and response (MDR) service”⁵³ “How Does FortiEDR Work? 7. The FortiEDR Collector Collects OS Metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device. 8. Communicating Device Makes a Connection Establishment Request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established. 9. The FortiEDR Core Identifies Malicious Requests: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies. 10. Pass or Block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked. 11. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog. Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”⁵⁴ FortiWeb Cloud
--	--

⁵³ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

⁵⁴ <https://docs.fortinet.com/document/fortiedr/5.0.0/administration-guide/717228/how-does-fortiedr-work>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

7. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Block mode On Applications page, you can turn on/off the Block Mode for each application. When to enable block mode • When Block Mode is enabled, FortiWeb Cloud will take actions as specified in Action of each WAF module. blocks requests if they trigger violations. Your application server does not receive these requests. • When Block Mode is disabled, FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests. Check the following prerequisites before you enable the Block Mode: • The endpoints and servers are configured properly. The traffic flow between the clients, FortiWeb Cloud, and your application servers is stable. • Observe the attack logs in FortiView or Logs. If legitimate traffic is falsely detected as attacks (also called false positives), add exceptions or modify the web protection configurations to avoid false positives in the future. 55 Action When you have enabled Advanced Configuration in Global > System Settings > Settings, you can configure actions for each WAF feature specifically. If Advanced Configuration is disabled, the default actions of each WAF feature will work instead. When Block Mode is disabled, FortiWeb Cloud will accept all requests and generate logs for all violations without considering the specified actions in each WAF feature. When Block Mode is enabled, all requests will be blocked if they trigger the violation, and the specific actions you have configured in each WAF feature will prevail. For example, if you set the Action for Known Attacks as Alert & Deny, FortiWeb Cloud will block the request (or reset the connection) and generate a log message. “How an anomaly detection model is built?” FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html; • The request packet must have parameter(s) in URL or body.
--	--

⁵⁵ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples. FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it. Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built: • If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model. • If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable. The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced. Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page. Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting. To create an Anomaly Detection policy: 1. Click Policy > Server Policy. 2. Select an existing server policy. 3. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy.
--	---

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	4. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens. 5. Click the + (Add) sign after the Domain field to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains. 6. Select whether to trust or block the specified source IP addresses. 7. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range. 8. Click OK. After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁵⁶
4. The method of claim 3, wherein the generic response includes at least one of: installing a missing software component, removing an undesirable software component, and restoring an incorrect registry setting.	FortiEDR and FortiWeb Cloud’s generic response includes at least one of: installing a missing software component, removing an undesirable software component, and restoring an incorrect registry setting. <i>See, e.g.:</i> FortiEDR “Discover and Predict FortiEDR delivers the most advanced automated attack surface policy control with vulnerability assessments and discovery that allows security teams to: • Discover and control rogue devices (such as unprotected or unmanaged devices) and IoT devices • Track applications and their CVE status • Discover and mitigate the exploit of system and application vulnerabilities with virtual patching and risk-based proactive policies”⁵⁷ “Real-time automated response. When FortiEDR detects potentially malicious processes, it defuses them in real time with automatic blocking. At the same time, the Fortinet Cloud Service continues to gather evidence, validate, and classify the events with its multiple sandboxes and code tracing technologies. Customized playbooks allow security teams to prescribe automated actions based on endpoint group, mission criticality, and threat classification. Automated

⁵⁶ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

⁵⁷ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

response and remediation actions may include terminating processes, deleting malicious or infected files, cleaning up persistency, notifying users, and forwarding event logs to a syslog server. This all helps FortiEDR eliminate alert fatigue and breach anxiety, standardize incident response procedures, and optimize security and operations resources.”⁵⁸

“Respond and Remediate

Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux.

- Automate incident classification to improve incident response and ease of resolution
- Recommends response actions to security analysts
- Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation
- Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets
- Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords

⁵⁸ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• Get additional help with the optional managed detection and response (MDR) service”⁵⁹
5. The method of claim 2, wherein the recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions.	FortiEDR and FortiWeb Cloud’s recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions. <i>See also, e.g.:</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁶⁰ “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution

⁵⁹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

⁶⁰ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups) • Gain full visibility of the attack chain and malicious changes with patented code tracing • Automate cleanup and roll back malicious changes while preserving system uptime • Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords • Get additional help with the optional managed detection and response (MDR) service”⁶¹ “Pre- and Post-infection Real-time Endpoint Threat Protection FortiEDR can help protect retail organizations from constant threats, whether attackers are trying to steal customer financial data or sabotage operations. Its capabilities include: • Proactive attack surface risk mitigation. FortiEDR delivers advanced automated attack surface policy control with vulnerability assessments and Internet-of-Things (IoT) security. • Malware prevention. A machine-learning (ML) antivirus engine helps stop malware pre-execution. This cross-operating system NGAV capability is configurable and comes built into the single, lightweight agent, so users can assign anti-malware protection to any endpoint group without requiring additional installation. • Real-time automated breach protection. FortiEDR detects suspicious process flows and behaviors and immediately defuses potential threats by blocking outbound communications and access to the file system from suspicious processes, which prevents data exfiltration, command-and-control communications, file tampering,
--	--

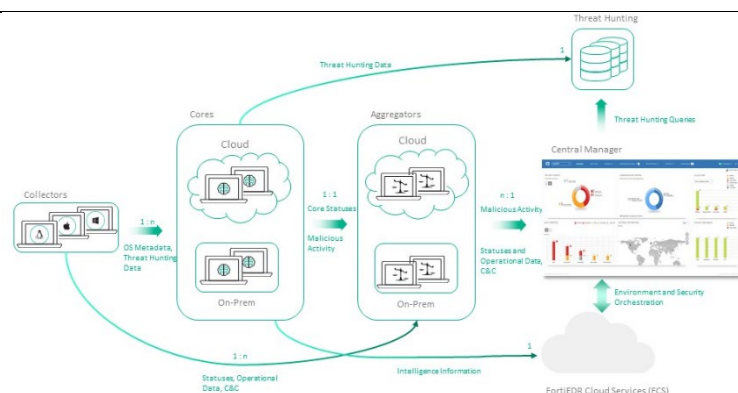
⁶¹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	and ransomware encryption. At the same time, the FortiEDR back end continues to gather additional evidence, enrich event data, and classify the incidents. The solution surgically stops data breach and ransomware damage in real time to automatically keep the business running even on devices that have been compromised. • Customizable incident response. With FortiEDR, you can orchestrate incident response operations using tailor-made playbooks with cross-environment insights. You can streamline incident response and remediation processes and manually or automatically roll back malicious changes done by already contained threats on a single device or on devices across the environment. • Guided interface with data enrichment. FortiEDR automatically enriches data with detailed information on malware both pre- and post-infection to conduct forensics on infiltrated endpoints. This unique interface provides helpful guidance, recommends best practices, and suggests the next logical steps for security analysts. Retailers that use FortiEDR also benefit from the Fortinet Security Fabric architecture and integration with other components of the Security Fabric, including FortiGate, FortiSandbox, and FortiSIEM. Detection and Remediation Without the Aggravation With FortiEDR, retail organizations can strategically reduce the complexity and cost associated with the detection and remediation of advanced malware across POS and other endpoints. In addition, FortiEDR minimizes incident response time pressures and alert fatigue, while preventing the exploitation of vulnerable endpoints that commonly leads to data breaches and disruption from cyberattacks.”⁶² “Overview The FortiEDR platform is a distributed architecture that collects the connection establishment flow of your organization’s communicating devices directly from each device’s operating system internals. FortiEDR analyzes the flow of events that preceded the connection establishment and determines whether the connection establishment request was malicious. The system can enforce your organization’s policy by blocking the connection establishment request in order to prevent exfiltration. The FortiEDR platform is comprised of the following components:
--	---

⁶² <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-retail-edr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet



FortiEDR Collector

The FortiEDR Collector is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers.

By default, the Collector runs in autonomous mode. Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate. You can configure the Collector to use a Core for the metadata analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.

- Pass: Legitimate requests are allowed with extremely negligible latency.
- Block: Malicious exfiltration and file changing attempts are blocked.

A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows, macOS, and Linux systems. The following are the connections established between the FortiEDR Collector and other FortiEDR components:

- To the FortiEDR Aggregator: The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health, status information, and security events.
- From the FortiEDR Aggregator: The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- To the FortiEDR Core: The FortiEDR Collector sends the following information:
 - Compressed activity events that are later used for Threat Hunting
 - Communication-related data to be used for the Communication Control
 - (Non-autonomous mode only) Metadata for determining whether a specific action should be blocked or passed
- From the FortiEDR Core: The FortiEDR Collector receives connection establishment authorization or denial (blocking) from the FortiEDR Core.

FortiEDR Core

The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows.

- When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.

One or more FortiEDR Cores are required, according to the size of your network based on deployment size (up to 50 FortiEDR Cores). Refer to Appendix C – ON PREMISE DEPLOYMENTS for the exact specifications of the system requirements.) The following are the connections established between the FortiEDR Core and other FortiEDR components:

- **To the FortiEDR Aggregator:** The FortiEDR Core sends registration information the first time it connects to the FortiEDR Aggregator and then sends events and ongoing health and status information.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• From the FortiEDR Aggregator: The FortiEDR Core receives its configuration from the FortiEDR Aggregator. The FortiEDR Core is located on exit points from your organization. It only reviews FortiEDR Collector metadata; it does not see the outgoing traffic. It is a central Linux-based software-only entity that can run on any workstation or VM that is assigned with a static IP address. FortiEDR Cloud Service The FortiEDR Cloud Service (FCS) enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event. The FCS is a cloud-based, GDPR-compliant, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy. The FCS security event classification process is done via data enrichment and enhanced deep, thorough analysis and investigation, enabled by automated and manual processes. The enhanced processes may include (partial list) intelligence services, file analysis (static and dynamic), sandboxing, flow analysis via machine learning, commonalities analysis, crowdsourced data deduction and more. Along with potential classification reassurance or reclassification, once connected, FCS can also enable several followed actions, which can be divided into two main activities: • Tuning: Automated security event exception (allowlisting). After a triggered security event is reclassified as Safe, an automated cross-environment exception can be pushed downstream and expire the event, preventing it from triggering again. For more details, see Exception Manager • Playbook Actions: All Playbook policy remediation actions are based on the final determination of the FCS. For more details see Remediation.”⁶³ “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware
--	--

⁶³ <https://docs.fortinet.com/document/fortiedr/7.0.0/administration-guide/970632/fortiedr-components>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR's back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁶⁴

“Real-time automated response. When FortiEDR detects potentially malicious processes, it defuses them in real time with automatic blocking. At the same time, the Fortinet Cloud Service continues to gather evidence, validate, and classify the events with its multiple sandboxes and code tracing technologies. Customized playbooks allow security teams to prescribe automated actions based on endpoint group, mission criticality, and threat classification. Automated response and remediation actions may include terminating processes, deleting malicious or infected files, cleaning up persistency, notifying users, and forwarding event logs to a syslog server. This all helps FortiEDR eliminate alert fatigue and breach anxiety, standardize incident response procedures, and optimize security and operations resources.

FortiEDR—Cloud-native EPP + EDR

Detect, Defuse, Respond, and Remote Remediation

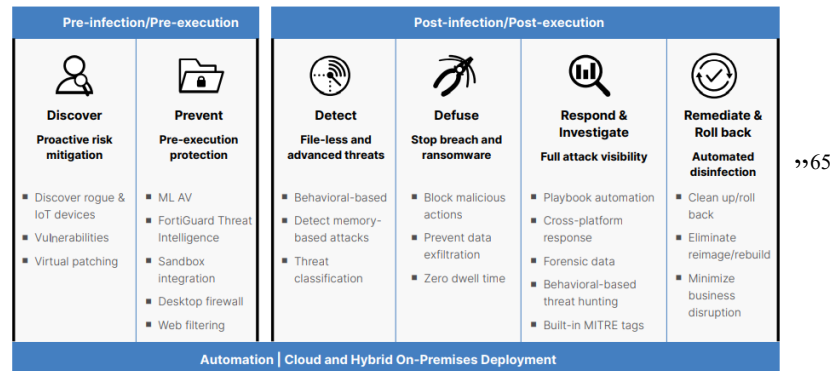


Figure 1: FortiEDR combines both pre-infection and post-infection endpoint defenses.

⁶⁴ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

⁶⁵ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	“How Does FortiEDR Work? 17. The FortiEDR Collector Collects OS Metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device. 18. Communicating Device Makes a Connection Establishment Request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established. 19. The FortiEDR Core Identifies Malicious Requests: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies. 20. Pass or Block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked. 21. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog. Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”⁶⁶ FortiWeb Cloud
--	--

⁶⁶ <https://docs.fortinet.com/document/fortiedr/5.0.0/administration-guide/717228/how-does-fortiedr-work>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

7. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Block mode On Applications page, you can turn on/off the Block Mode for each application. When to enable block mode • When Block Mode is enabled, FortiWeb Cloud will take actions as specified in Action of each WAF module. blocks requests if they trigger violations. Your application server does not receive these requests. • When Block Mode is disabled, FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests. Check the following prerequisites before you enable the Block Mode: • The endpoints and servers are configured properly. The traffic flow between the clients, FortiWeb Cloud, and your application servers is stable. • Observe the attack logs in FortiView or Logs. If legitimate traffic is falsely detected as attacks (also called false positives), add exceptions or modify the web protection configurations to avoid false positives in the future. Action When you have enabled Advanced Configuration in Global > System Settings > Settings, you can configure actions for each WAF feature specifically. If Advanced Configuration is disabled, the default actions of each WAF feature will work instead. When Block Mode is disabled, FortiWeb Cloud will accept all requests and generate logs for all violations without considering the specified actions in each WAF feature. When Block Mode is enabled, all requests will be blocked if they trigger the violation, and the specific actions you have configured in each WAF feature will prevail. For example, if you set the Action for Known Attacks as Alert & Deny, FortiWeb Cloud will block the request (or reset the connection) and generate a log message. “How an anomaly detection model is built?” FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html;
--	--

⁶⁷ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- The request packet must have parameter(s) in URL or body.

When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples.

FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it.

Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built:

- If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model.
- If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable.

The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced.

Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page.

Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting.

To create an Anomaly Detection policy:

9. Click Policy > Server Policy.
10. Select an existing server policy.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

11. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy.
12. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens.
13. Click the + (Add) sign after the Domain field to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains.
14. Select whether to trust or block the specified source IP addresses.
15. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range.
16. Click OK.

After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁶⁸

“Machine learning

Starting with the 6.0 release, FortiWeb offers a machine-learning function that enables it to automatically detect malicious web traffic and bots . In addition to detecting known attacks, the feature can detect potential unknown zero-day attacks to provide real-time protection for web servers.

Machine Learning is intended to replace Auto Learn, which is now removed from 6.1 release.

Anomaly detection

The anomaly detection model of machine learning feature observes the URLs, parameters, and HTTP Method of HTTP and/or HTTPS sessions passing to your web servers. It builds mathematical models to detect abnormal traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Observes the HTTP method of the traffic
- Matches anomalies against pre-trained threat models
- Detects attacks

⁶⁸ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiWeb employs two layers of machine learning to detect malicious attacks. The first layer uses the Hidden Markov Model (HMM) and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method. Once completed, it will verify every request against the model to determine whether it's an anomaly or not.

Once the first layer of machine learning triggers a request as an anomaly, FortiWeb will use the second layer of machine learning to verify whether it's a real attack or just a benign anomaly that should be ignored. To do so, FortiWeb includes pre-built trained threat models. Each represents a certain attack category, such as SQL Injection, Cross-site Scripting, and so on. Each threat model is already trained based on analysis of thousands of attack samples. Threat models are continuously updated using the FortiWeb Security Service. When new attack types are released, the FortiGuard team analyzes the new threats and re-trains the relevant threat model. The new threat model is then pushed to all customer installations in a way similar to how signatures are updated.

Bot detection

The AI-based machine learning bot detection model complements the existing signature and threshold based rules. It detects sophisticated bots that can sometimes go undetected. The bot detection model observes user behaviors from thirteen dimensions, for example, how many times of HTTP requests are initiated by the user, whether the request uses illegal HTTP versions, whether it fetches JSON/XML resources, etc.

Compared with the traditional mechanisms to detect bots, the bot detection model saves you the trouble to experiment on an appropriate threshold to detect abnormal user behaviors. For example, how could you know how many times of HTTP requests initiated by a user should be considered as abnormal? With the traditional mechanism, you may need to experiment on different threshold values and continuously check the attack log until no related attack logs are reported for the regular traffic.

Things are much easier if you use the bot detection model. FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model that self-learns the traffic profiles of regular clients. When the traffic from a new client flows in, it is compared against that of the regular clients. If they don't match, the bot detection model classifies the new client as an anomaly. When the traffic profiles of the regular clients vary dramatically (e.g. the functions of your application have changed, so that users behave differently when they visit your application), FortiWeb automatically refreshes the bot detection model to adapt to the changes.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Moreover, test shows that the bot detection model performs much better, specially when it detects crawlers and scrapers. The traffic is comprehensively evaluated from 13 dimensions. It helps increase the detection accuracy and decrease the false positive rate.”⁶⁹ “How an anomaly detection model is built? FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html; • The request packet must have parameter(s) in URL or body. When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples. FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it. Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built: • If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model. • If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable. The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of
--	---

⁶⁹ <https://docs.fortinet.com/document/fortiweb/6.3.23/administration-guide/193258>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced.

Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page.

Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting.

To create an Anomaly Detection policy:

1. Click Policy > Server Policy.
2. Select an existing server policy.
3. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy.
4. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens.
5. Click the + (Add) sign after the Domain filed to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains.
6. Select whether to trust or block the specified source IP addresses.
7. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range.
8. Click OK.

After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁷⁰

⁷⁰ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

6(pre) The method of claim 1, further comprising: comparing a plurality of anomalies associated with a particular snapshot with a recognition filter to diagnose a trouble condition; and	FortiEDR and FortiWeb Cloud compare a plurality of anomalies associated with a particular snapshot with a recognition filter to diagnose a trouble condition. <i>See, e.g.,</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁷¹ “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution • Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets
---	---

⁷¹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords
- Get additional help with the optional managed detection and response (MDR) service”⁷²

“Pre- and Post-infection Real-time Endpoint Threat Protection

FortiEDR can help protect retail organizations from constant threats, whether attackers are trying to steal customer financial data or sabotage operations. Its capabilities include:

- **Proactive attack surface risk mitigation.** FortiEDR delivers advanced automated attack surface policy control with vulnerability assessments and Internet-of-Things (IoT) security.
- **Malware prevention.** A machine-learning (ML) antivirus engine helps stop malware pre-execution. This cross-operating system NGAV capability is configurable and comes built into the single, lightweight agent, so users can assign anti-malware protection to any endpoint group without requiring additional installation.
- **Real-time automated breach protection.** FortiEDR detects suspicious process flows and behaviors and immediately defuses potential threats by blocking outbound communications and access to the file system from suspicious processes, which prevents data exfiltration, command-and-control communications, file tampering, and ransomware encryption. At the same time, the FortiEDR back end continues to gather additional evidence, enrich event data, and classify the incidents. The solution surgically stops data breach and ransomware damage in real time to automatically keep the business running even on devices that have been compromised.
- **Customizable incident response.** With FortiEDR, you can orchestrate incident response operations using tailor-made playbooks with cross-environment insights. You can streamline incident response and remediation processes and manually or automatically roll back malicious changes done by already contained threats on a single device or on devices across the environment.

⁷² <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- **Guided interface with data enrichment.** FortiEDR automatically enriches data with detailed information on malware both pre- and post-infection to conduct forensics on infiltrated endpoints. This unique interface provides helpful guidance, recommends best practices, and suggests the next logical steps for security analysts.

Retailers that use FortiEDR also benefit from the Fortinet Security Fabric architecture and integration with other components of the Security Fabric, including FortiGate, FortiSandbox, and FortiSIEM.

Detection and Remediation Without the Aggravation

With FortiEDR, retail organizations can strategically reduce the complexity and cost associated with the detection and remediation of advanced malware across POS and other endpoints. In addition, FortiEDR minimizes incident response time pressures and alert fatigue, while preventing the exploitation of vulnerable endpoints that commonly leads to data breaches and disruption from cyberattacks.”⁷³

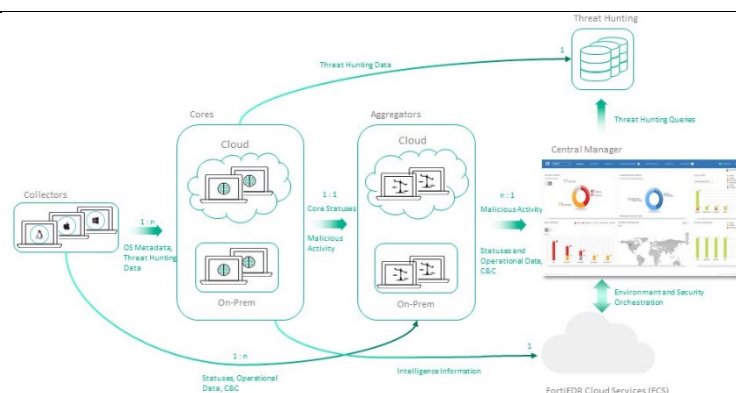
“Overview

The FortiEDR platform is a distributed architecture that collects the connection establishment flow of your organization’s communicating devices directly from each device’s operating system internals. FortiEDR analyzes the flow of events that preceded the connection establishment and determines whether the connection establishment request was malicious. The system can enforce your organization’s policy by blocking the connection establishment request in order to prevent exfiltration.

The FortiEDR platform is comprised of the following components:

⁷³ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-retail-edr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet



FortiEDR Collector

The FortiEDR Collector is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers.

By default, the Collector runs in autonomous mode. Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate. You can configure the Collector to use a Core for the metadata analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.

- Pass: Legitimate requests are allowed with extremely negligible latency.
- Block: Malicious exfiltration and file changing attempts are blocked.

A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows, macOS, and Linux systems. The following are the connections established between the FortiEDR Collector and other FortiEDR components:

- To the FortiEDR Aggregator: The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health, status information, and security events.
- From the FortiEDR Aggregator: The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- To the FortiEDR Core: The FortiEDR Collector sends the following information:
 - Compressed activity events that are later used for Threat Hunting
 - Communication-related data to be used for the Communication Control
 - (Non-autonomous mode only) Metadata for determining whether a specific action should be blocked or passed
- From the FortiEDR Core: The FortiEDR Collector receives connection establishment authorization or denial (blocking) from the FortiEDR Core.

FortiEDR Core

The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows.

- When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.

One or more FortiEDR Cores are required, according to the size of your network based on deployment size (up to 50 FortiEDR Cores). Refer to Appendix C – ON PREMISE DEPLOYMENTS for the exact specifications of the system requirements.) The following are the connections established between the FortiEDR Core and other FortiEDR components:

- **To the FortiEDR Aggregator:** The FortiEDR Core sends registration information the first time it connects to the FortiEDR Aggregator and then sends events and ongoing health and status information.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• From the FortiEDR Aggregator: The FortiEDR Core receives its configuration from the FortiEDR Aggregator. The FortiEDR Core is located on exit points from your organization. It only reviews FortiEDR Collector metadata; it does not see the outgoing traffic. It is a central Linux-based software-only entity that can run on any workstation or VM that is assigned with a static IP address. FortiEDR Cloud Service The FortiEDR Cloud Service (FCS) enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event. The FCS is a cloud-based, GDPR-compliant, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy. The FCS security event classification process is done via data enrichment and enhanced deep, thorough analysis and investigation, enabled by automated and manual processes. The enhanced processes may include (partial list) intelligence services, file analysis (static and dynamic), sandboxing, flow analysis via machine learning, commonalities analysis, crowdsourced data deduction and more. Along with potential classification reassurance or reclassification, once connected, FCS can also enable several followed actions, which can be divided into two main activities: • Tuning: Automated security event exception (allowlisting). After a triggered security event is reclassified as Safe, an automated cross-environment exception can be pushed downstream and expire the event, preventing it from triggering again. For more details, see Exception Manager • Playbook Actions: All Playbook policy remediation actions are based on the final determination of the FCS. For more details see Remediation.”⁷⁴ “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware
--	--

⁷⁴ <https://docs.fortinet.com/document/fortiedr/7.0.0/administration-guide/970632/fortiedr-components>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR's back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁷⁵

“Real-time automated response. When FortiEDR detects potentially malicious processes, it defuses them in real time with automatic blocking. At the same time, the Fortinet Cloud Service continues to gather evidence, validate, and classify the events with its multiple sandboxes and code tracing technologies. Customized playbooks allow security teams to prescribe automated actions based on endpoint group, mission criticality, and threat classification. Automated response and remediation actions may include terminating processes, deleting malicious or infected files, cleaning up persistency, notifying users, and forwarding event logs to a syslog server. This all helps FortiEDR eliminate alert fatigue and breach anxiety, standardize incident response procedures, and optimize security and operations resources.

FortiEDR—Cloud-native EPP + EDR

Detect, Defuse, Respond, and Remote Remediation

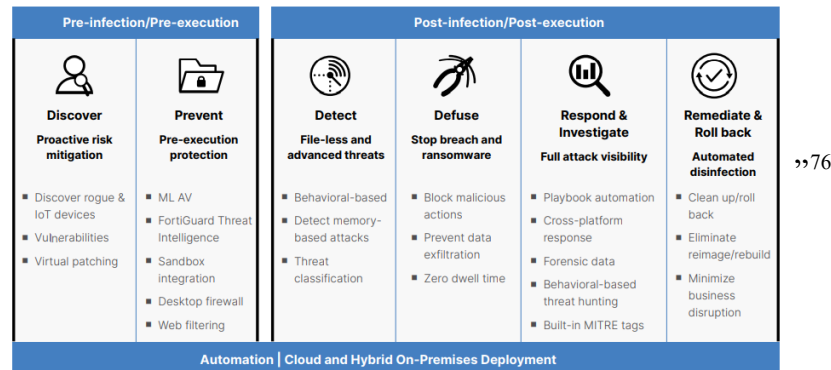


Figure 1: FortiEDR combines both pre-infection and post-infection endpoint defenses.

⁷⁵ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

⁷⁶ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	“How Does FortiEDR Work? 22. The FortiEDR Collector Collects OS Metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device. 23. Communicating Device Makes a Connection Establishment Request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established. 24. The FortiEDR Core Identifies Malicious Requests: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies. 25. Pass or Block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked. 26. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog. Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”⁷⁷ FortiWeb Cloud
--	--

⁷⁷ <https://docs.fortinet.com/document/fortiedr/5.0.0/administration-guide/717228/how-does-fortiedr-work>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

7. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Block mode On Applications page, you can turn on/off the Block Mode for each application. When to enable block mode • When Block Mode is enabled, FortiWeb Cloud will take actions as specified in Action of each WAF module. blocks requests if they trigger violations. Your application server does not receive these requests. • When Block Mode is disabled, FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests. Check the following prerequisites before you enable the Block Mode: • The endpoints and servers are configured properly. The traffic flow between the clients, FortiWeb Cloud, and your application servers is stable. • Observe the attack logs in FortiView or Logs. If legitimate traffic is falsely detected as attacks (also called false positives), add exceptions or modify the web protection configurations to avoid false positives in the future. Action When you have enabled Advanced Configuration in Global > System Settings > Settings, you can configure actions for each WAF feature specifically. If Advanced Configuration is disabled, the default actions of each WAF feature will work instead. When Block Mode is disabled, FortiWeb Cloud will accept all requests and generate logs for all violations without considering the specified actions in each WAF feature. When Block Mode is enabled, all requests will be blocked if they trigger the violation, and the specific actions you have configured in each WAF feature will prevail. For example, if you set the Action for Known Attacks as Alert & Deny, FortiWeb Cloud will block the request (or reset the connection) and generate a log message. 78 “How an anomaly detection model is built?” FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html;
--	--

⁷⁸ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- The request packet must have parameter(s) in URL or body.

When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples.

FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it.

Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built:

- If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model.
- If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable.

The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced.

Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page.

Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting.

To create an Anomaly Detection policy:

9. Click Policy > Server Policy.
10. Select an existing server policy.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

11. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy.
12. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens.
13. Click the + (Add) sign after the Domain field to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains.
14. Select whether to trust or block the specified source IP addresses.
15. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range.
16. Click OK.

After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁷⁹

“Machine learning

Starting with the 6.0 release, FortiWeb offers a machine-learning function that enables it to automatically detect malicious web traffic and bots . In addition to detecting known attacks, the feature can detect potential unknown zero-day attacks to provide real-time protection for web servers.

Machine Learning is intended to replace Auto Learn, which is now removed from 6.1 release.

Anomaly detection

The anomaly detection model of machine learning feature observes the URLs, parameters, and HTTP Method of HTTP and/or HTTPS sessions passing to your web servers. It builds mathematical models to detect abnormal traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Observes the HTTP method of the traffic
- Matches anomalies against pre-trained threat models
- Detects attacks

⁷⁹ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiWeb employs two layers of machine learning to detect malicious attacks. The first layer uses the Hidden Markov Model (HMM) and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method. Once completed, it will verify every request against the model to determine whether it's an anomaly or not.

Once the first layer of machine learning triggers a request as an anomaly, FortiWeb will use the second layer of machine learning to verify whether it's a real attack or just a benign anomaly that should be ignored. To do so, FortiWeb includes pre-built trained threat models. Each represents a certain attack category, such as SQL Injection, Cross-site Scripting, and so on. Each threat model is already trained based on analysis of thousands of attack samples. Threat models are continuously updated using the FortiWeb Security Service. When new attack types are released, the FortiGuard team analyzes the new threats and re-trains the relevant threat model. The new threat model is then pushed to all customer installations in a way similar to how signatures are updated.

Bot detection

The AI-based machine learning bot detection model complements the existing signature and threshold based rules. It detects sophisticated bots that can sometimes go undetected. The bot detection model observes user behaviors from thirteen dimensions, for example, how many times of HTTP requests are initiated by the user, whether the request uses illegal HTTP versions, whether it fetches JSON/XML resources, etc.

Compared with the traditional mechanisms to detect bots, the bot detection model saves you the trouble to experiment on an appropriate threshold to detect abnormal user behaviors. For example, how could you know how many times of HTTP requests initiated by a user should be considered as abnormal? With the traditional mechanism, you may need to experiment on different threshold values and continuously check the attack log until no related attack logs are reported for the regular traffic.

Things are much easier if you use the bot detection model. FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model that self-learns the traffic profiles of regular clients. When the traffic from a new client flows in, it is compared against that of the regular clients. If they don't match, the bot detection model classifies the new client as an anomaly. When the traffic profiles of the regular clients vary dramatically (e.g. the functions of your application have changed, so that users behave differently when they visit your application), FortiWeb automatically refreshes the bot detection model to adapt to the changes.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Moreover, test shows that the bot detection model performs much better, specially when it detects crawlers and scrapers. The traffic is comprehensively evaluated from 13 dimensions. It helps increase the detection accuracy and decrease the false positive rate.”⁸⁰ “How an anomaly detection model is built? FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html; • The request packet must have parameter(s) in URL or body. When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples. FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it. Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built: • If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model. • If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable. The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of
--	---

⁸⁰ <https://docs.fortinet.com/document/fortiweb/6.3.23/administration-guide/193258>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced. Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page. Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting. To create an Anomaly Detection policy: 1. Click Policy > Server Policy. 2. Select an existing server policy. 3. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy. 4. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens. 5. Click the + (Add) sign after the Domain filed to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains. 6. Select whether to trust or block the specified source IP addresses. 7. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range. 8. Click OK. After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁸¹
6(a) diagnosing a trouble condition on the at least one	FortiEDR and FortiWeb Cloud diagnose a trouble condition on the at least one of the computers in response to at least a subset of the plurality of anomalies matching information in the recognition filter.

⁸¹ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

of the computers in response to at least a subset of the plurality of anomalies matching information in the recognition filter.	<i>See, e.g.:</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁸² “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution • Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
---	--

⁸² <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords
- Get additional help with the optional managed detection and response (MDR) service”⁸³

“Pre- and Post-infection Real-time Endpoint Threat Protection

FortiEDR can help protect retail organizations from constant threats, whether attackers are trying to steal customer financial data or sabotage operations. Its capabilities include:

- **Proactive attack surface risk mitigation.** FortiEDR delivers advanced automated attack surface policy control with vulnerability assessments and Internet-of-Things (IoT) security.
- **Malware prevention.** A machine-learning (ML) antivirus engine helps stop malware pre-execution. This cross-operating system NGAV capability is configurable and comes built into the single, lightweight agent, so users can assign anti-malware protection to any endpoint group without requiring additional installation.
- **Real-time automated breach protection.** FortiEDR detects suspicious process flows and behaviors and immediately defuses potential threats by blocking outbound communications and access to the file system from suspicious processes, which prevents data exfiltration, command-and-control communications, file tampering, and ransomware encryption. At the same time, the FortiEDR back end continues to gather additional evidence, enrich event data, and classify the incidents. The solution surgically stops data breach and ransomware damage in real time to automatically keep the business running even on devices that have been compromised.
- **Customizable incident response.** With FortiEDR, you can orchestrate incident response operations using tailor-made playbooks with cross-environment insights. You can streamline incident response and remediation processes and manually or automatically roll back malicious changes done by already contained threats on a single device or on devices across the environment.

⁸³ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- **Guided interface with data enrichment.** FortiEDR automatically enriches data with detailed information on malware both pre- and post-infection to conduct forensics on infiltrated endpoints. This unique interface provides helpful guidance, recommends best practices, and suggests the next logical steps for security analysts.

Retailers that use FortiEDR also benefit from the Fortinet Security Fabric architecture and integration with other components of the Security Fabric, including FortiGate, FortiSandbox, and FortiSIEM.

Detection and Remediation Without the Aggravation

With FortiEDR, retail organizations can strategically reduce the complexity and cost associated with the detection and remediation of advanced malware across POS and other endpoints. In addition, FortiEDR minimizes incident response time pressures and alert fatigue, while preventing the exploitation of vulnerable endpoints that commonly leads to data breaches and disruption from cyberattacks.”⁸⁴

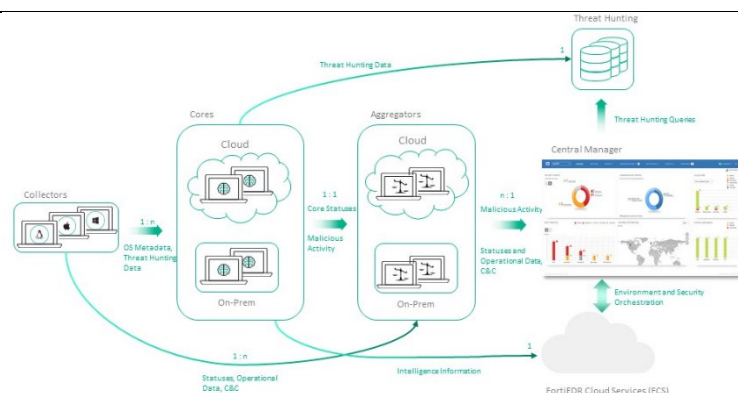
“Overview

The FortiEDR platform is a distributed architecture that collects the connection establishment flow of your organization’s communicating devices directly from each device’s operating system internals. FortiEDR analyzes the flow of events that preceded the connection establishment and determines whether the connection establishment request was malicious. The system can enforce your organization’s policy by blocking the connection establishment request in order to prevent exfiltration.

The FortiEDR platform is comprised of the following components:

⁸⁴ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-retail-edr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet



FortiEDR Collector

The FortiEDR Collector is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers.

By default, the Collector runs in autonomous mode. Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate. You can configure the Collector to use a Core for the metadata analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.

- Pass: Legitimate requests are allowed with extremely negligible latency.
- Block: Malicious exfiltration and file changing attempts are blocked.

A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows, macOS, and Linux systems. The following are the connections established between the FortiEDR Collector and other FortiEDR components:

- To the FortiEDR Aggregator: The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health, status information, and security events.
- From the FortiEDR Aggregator: The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- To the FortiEDR Core: The FortiEDR Collector sends the following information:
 - Compressed activity events that are later used for Threat Hunting
 - Communication-related data to be used for the Communication Control
 - (Non-autonomous mode only) Metadata for determining whether a specific action should be blocked or passed
- From the FortiEDR Core: The FortiEDR Collector receives connection establishment authorization or denial (blocking) from the FortiEDR Core.

FortiEDR Core

The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows.

- When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.

One or more FortiEDR Cores are required, according to the size of your network based on deployment size (up to 50 FortiEDR Cores). Refer to Appendix C – ON PREMISE DEPLOYMENTS for the exact specifications of the system requirements.) The following are the connections established between the FortiEDR Core and other FortiEDR components:

- **To the FortiEDR Aggregator:** The FortiEDR Core sends registration information the first time it connects to the FortiEDR Aggregator and then sends events and ongoing health and status information.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• From the FortiEDR Aggregator: The FortiEDR Core receives its configuration from the FortiEDR Aggregator. The FortiEDR Core is located on exit points from your organization. It only reviews FortiEDR Collector metadata; it does not see the outgoing traffic. It is a central Linux-based software-only entity that can run on any workstation or VM that is assigned with a static IP address. FortiEDR Cloud Service The FortiEDR Cloud Service (FCS) enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event. The FCS is a cloud-based, GDPR-compliant, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy. The FCS security event classification process is done via data enrichment and enhanced deep, thorough analysis and investigation, enabled by automated and manual processes. The enhanced processes may include (partial list) intelligence services, file analysis (static and dynamic), sandboxing, flow analysis via machine learning, commonalities analysis, crowdsourced data deduction and more. Along with potential classification reassurance or reclassification, once connected, FCS can also enable several followed actions, which can be divided into two main activities: • Tuning: Automated security event exception (allowlisting). After a triggered security event is reclassified as Safe, an automated cross-environment exception can be pushed downstream and expire the event, preventing it from triggering again. For more details, see Exception Manager • Playbook Actions: All Playbook policy remediation actions are based on the final determination of the FCS. For more details see Remediation.”⁸⁵ “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware
--	--

⁸⁵ <https://docs.fortinet.com/document/fortiedr/7.0.0/administration-guide/970632/fortiedr-components>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR's back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁸⁶

“Real-time automated response. When FortiEDR detects potentially malicious processes, it defuses them in real time with automatic blocking. At the same time, the Fortinet Cloud Service continues to gather evidence, validate, and classify the events with its multiple sandboxes and code tracing technologies. Customized playbooks allow security teams to prescribe automated actions based on endpoint group, mission criticality, and threat classification. Automated response and remediation actions may include terminating processes, deleting malicious or infected files, cleaning up persistency, notifying users, and forwarding event logs to a syslog server. This all helps FortiEDR eliminate alert fatigue and breach anxiety, standardize incident response procedures, and optimize security and operations resources.

FortiEDR—Cloud-native EPP + EDR

Detect, Defuse, Respond, and Remote Remediation

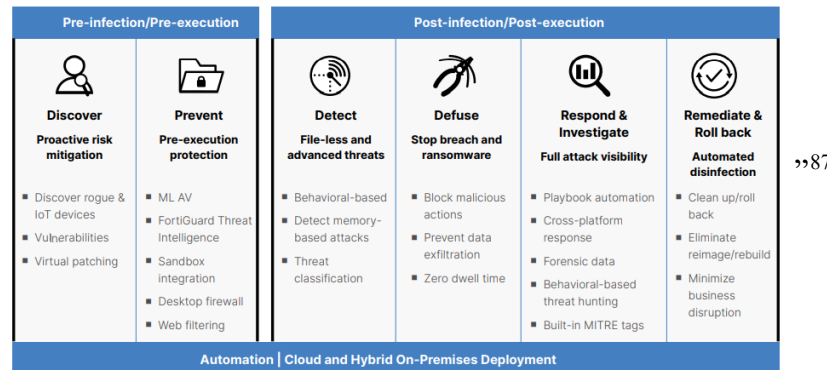


Figure 1: FortiEDR combines both pre-infection and post-infection endpoint defenses.

⁸⁶ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

⁸⁷ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	“How Does FortiEDR Work? 27. The FortiEDR Collector Collects OS Metadata: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device. 28. Communicating Device Makes a Connection Establishment Request: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established. 29. The FortiEDR Core Identifies Malicious Requests: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies. 30. Pass or Block: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked. 31. Event Generation: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog. Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.”⁸⁸ FortiWeb Cloud
--	--

⁸⁸ <https://docs.fortinet.com/document/fortiedr/5.0.0/administration-guide/717228/how-does-fortiedr-work>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

7. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Block mode On Applications page, you can turn on/off the Block Mode for each application. When to enable block mode • When Block Mode is enabled, FortiWeb Cloud will take actions as specified in Action of each WAF module. blocks requests if they trigger violations. Your application server does not receive these requests. • When Block Mode is disabled, FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests. Check the following prerequisites before you enable the Block Mode: • The endpoints and servers are configured properly. The traffic flow between the clients, FortiWeb Cloud, and your application servers is stable. • Observe the attack logs in FortiView or Logs. If legitimate traffic is falsely detected as attacks (also called false positives), add exceptions or modify the web protection configurations to avoid false positives in the future. 89 Action When you have enabled Advanced Configuration in Global > System Settings > Settings, you can configure actions for each WAF feature specifically. If Advanced Configuration is disabled, the default actions of each WAF feature will work instead. When Block Mode is disabled, FortiWeb Cloud will accept all requests and generate logs for all violations without considering the specified actions in each WAF feature. When Block Mode is enabled, all requests will be blocked if they trigger the violation, and the specific actions you have configured in each WAF feature will prevail. For example, if you set the Action for Known Attacks as Alert & Deny, FortiWeb Cloud will block the request (or reset the connection) and generate a log message. “How an anomaly detection model is built?” FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html;
--	--

⁸⁹ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- The request packet must have parameter(s) in URL or body.

When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples.

FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it.

Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built:

- If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model.
- If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable.

The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced.

Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page.

Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting.

To create an Anomaly Detection policy:

17. Click Policy > Server Policy.
18. Select an existing server policy.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

19. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy.
20. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens.
21. Click the + (Add) sign after the Domain field to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains.
22. Select whether to trust or block the specified source IP addresses.
23. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range.
24. Click OK.

After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁹⁰

“Machine learning

Starting with the 6.0 release, FortiWeb offers a machine-learning function that enables it to automatically detect malicious web traffic and bots . In addition to detecting known attacks, the feature can detect potential unknown zero-day attacks to provide real-time protection for web servers.

Machine Learning is intended to replace Auto Learn, which is now removed from 6.1 release.

Anomaly detection

The anomaly detection model of machine learning feature observes the URLs, parameters, and HTTP Method of HTTP and/or HTTPS sessions passing to your web servers. It builds mathematical models to detect abnormal traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Observes the HTTP method of the traffic
- Matches anomalies against pre-trained threat models
- Detects attacks

⁹⁰ <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiWeb employs two layers of machine learning to detect malicious attacks. The first layer uses the Hidden Markov Model (HMM) and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method. Once completed, it will verify every request against the model to determine whether it's an anomaly or not.

Once the first layer of machine learning triggers a request as an anomaly, FortiWeb will use the second layer of machine learning to verify whether it's a real attack or just a benign anomaly that should be ignored. To do so, FortiWeb includes pre-built trained threat models. Each represents a certain attack category, such as SQL Injection, Cross-site Scripting, and so on. Each threat model is already trained based on analysis of thousands of attack samples. Threat models are continuously updated using the FortiWeb Security Service. When new attack types are released, the FortiGuard team analyzes the new threats and re-trains the relevant threat model. The new threat model is then pushed to all customer installations in a way similar to how signatures are updated.

Bot detection

The AI-based machine learning bot detection model complements the existing signature and threshold based rules. It detects sophisticated bots that can sometimes go undetected. The bot detection model observes user behaviors from thirteen dimensions, for example, how many times of HTTP requests are initiated by the user, whether the request uses illegal HTTP versions, whether it fetches JSON/XML resources, etc.

Compared with the traditional mechanisms to detect bots, the bot detection model saves you the trouble to experiment on an appropriate threshold to detect abnormal user behaviors. For example, how could you know how many times of HTTP requests initiated by a user should be considered as abnormal? With the traditional mechanism, you may need to experiment on different threshold values and continuously check the attack log until no related attack logs are reported for the regular traffic.

Things are much easier if you use the bot detection model. FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model that self-learns the traffic profiles of regular clients. When the traffic from a new client flows in, it is compared against that of the regular clients. If they don't match, the bot detection model classifies the new client as an anomaly. When the traffic profiles of the regular clients vary dramatically (e.g. the functions of your application have changed, so that users behave differently when they visit your application), FortiWeb automatically refreshes the bot detection model to adapt to the changes.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Moreover, test shows that the bot detection model performs much better, specially when it detects crawlers and scrapers. The traffic is comprehensively evaluated from 13 dimensions. It helps increase the detection accuracy and decrease the false positive rate.”⁹¹ “How an anomaly detection model is built? FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain. The traffic should meet all of the following conditions to be treated as a sample: • The response code of response packet must be 200 or 302; • The response content-type of response packet must be text or html; • The request packet must have parameter(s) in URL or body. When a sample is collected, the system generalized it into a pattern. For example, “abcd_123@abc.com” and “abcdefgcedf_12345678@efg.com” will both be generalized to the pattern “A_N@A.A”. The anomaly detection model is built based on the patterns, not the raw samples. FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it. Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built: • If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model. • If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable. The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of
--	---

⁹¹ <https://docs.fortinet.com/document/fortiweb/6.3.23/administration-guide/193258>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced.

Anomaly detection policy is part of a server policy. It is created on the Policy > Sever Policy page.

Anomaly detection must learn the charset for each domain before it can work properly. The charset can be learned automatically from the server's response or configured via CLI. Certain conditions should be met for the learning to be successful. For more information, see "ML based Anomaly Detection does not learn parameters successfully" in Machine learning trouble-shooting.

To create an Anomaly Detection policy:

1. Click Policy > Server Policy.
2. Select an existing server policy.
3. Please note that the machine learning policies can't be created during the server policy creation process. You should first create a server policy, then click its Edit button to create a machine learning policy.
4. Scroll down to the Machine Learning section at the bottom of the page, click the Anomaly Detection tab, then click Create. The New Machine Learning dialog opens.
5. Click the + (Add) sign after the Domain filed to add the desired domains, so that the system collects samples and builds up a machine learning model for the domains.
6. Select whether to trust or block the specified source IP addresses.
7. Click the + (Add) sign after the IP Range field to add IP/Range, so as to limit the system to collect data only (When IP List Type is Trust) or exclude data (When IP List Type is Block) from the specified IP range.
8. Click OK.

After it's completed, go back to Server Policy. Select the one which contains the anomaly detection policy you just created. You will see the following buttons in the Anomaly Detection tab.”⁹²

⁹² <https://docs.fortinet.com/document/fortiweb/7.4.1/administration-guide/94907/ml-based-anomaly-detection>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

7. The method of claim 1, wherein individual snapshots include data associated with at least one of: system files, application files, a registry entry, a performance counter, a process, a communication port, a hardware configuration, a log file, a running task, services, and network connections.	FortiEDR and FortiWeb Cloud’s individual snapshots include data associated with at least one of: system files, application files, a registry entry, a performance counter, a process, a communication port, a hardware configuration, a log file, a running task, services, and network connections. <i>See, e.g.:</i> FortiEDR “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”⁹³ “FortiEDR surgically stops data breaches and ransomware damage in real time, automatically allowing business continuity even on already compromised devices. • Leverage OS-centric detection, highly accurate in detecting stealthy infiltrated attacks, including memory-based and “living off the land” attacks • Stop breaches in real time and eliminate threat dwell time • Achieve analysis of entire log history • Prevent ransomware encryption, and file/registry tempering • Continuously validate the classification of threats with FortiGuard Threat Intelligence and
---	---

⁹³ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	multi-engine sandboxing, both within Fortinet Cloud Services • Enhance signal-to-noise ratio and eliminate alert fatigue • Support for Mobile OS, including Android and iOS”⁹⁴ “Real-time automated response. When FortiEDR detects potentially malicious processes, it defuses them in real time with automatic blocking. At the same time, the Fortinet Cloud Service continues to gather evidence, validate, and classify the events with its multiple sandboxes and code tracing technologies. Customized playbooks allow security teams to prescribe automated actions based on endpoint group, mission criticality, and threat classification. Automated response and remediation actions may include terminating processes, deleting malicious or infected files, cleaning up persistency, notifying users, and forwarding event logs to a syslog server. This all helps FortiEDR eliminate alert fatigue and breach anxiety, standardize incident response procedures, and optimize security and operations resources. Production continuity. Real-time automatic responses can make life difficult for security teams when a legitimate application triggers the detection system and generates a false alarm. Blunt-force response actions can interfere with applications—or worse, cause operating system crashes that bring down a mission-critical production system. FortiEDR continuously classifies events until a final verdict is made. If Fortinet Cloud services classifies an event as safe, an automatic exception is created to prevent such occurrences in the future. FortiEDR’s policy baselining and simulation features can help OT plant managers and security professionals avoid these sorts of occurrences. By running the system in simulation mode, the plant team can exercise all normal plant activities and ensure that endpoint protection and critical plant floor operations are in tune with one another. Recent FortiEDR deployments have been able to find critical OT policy violations such as connected mobile devices, Android services, and unauthorized systems—even before the system was taken out of simulation mode.”⁹⁵ “Discover and Predict FortiEDR delivers the most advanced automated attack surface policy control with vulnerability assessments and discovery that allows security teams to: • Discover and control rogue devices (such as unprotected or unmanaged devices) and IoT devices • Track applications and their CVE status
--	--

⁹⁴ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

⁹⁵ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- Discover and mitigate the exploit of system and application vulnerabilities with virtual patching and risk-based proactive policies”⁹⁶

“FortiEDR Core

The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows.

- When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization’s policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization’s policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.”⁹⁷

⁹⁶ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

⁹⁷ *Id.*

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiWeb Cloud

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Audit logs

Audit logs report system-level events such as user login, server creation. You can view the audit logs through **Global > Log & Report > Audit Logs**. A maximum of 10,000 audit logs are displayed per each filter. An audit log is saved for three months. After that it will be deleted.

To configure the log display settings:

1. Go to **Global > Log & Report > Audit Logs**.
2. Configure the following settings.

Reload	Click to update the page with any logs that have been recorded since you previously loaded the page.
Add Filter	Click to create a filter based on log message fields. Only messages that are in the most recent 100,000 messages and match the criteria in the filter are displayed. When you search by time, all messages with the selected date are displayed.

To view before&after comparison:

Audit logs provide details on the configuration changes with before&after information.

For the logs on configuration updates, the log item is a clickable link, as shown below.

2023-02-17 10:54:43 INFO test_block 1245460@qq.com EDIT [Module Rewriting Requests of application test_block updated](#)

By clicking on the link, a before&after comparison view will display. You can click the **Diffs** or **All** at the top right corner to show only the differences or expand the whole configuration.

Change Details

Module Rewriting Requests of application test_block updated Diffs All

Before:	After:
@@ -1,3 +1,3 @@	
1 - identify_original_ip: true	1 + identify_original_ip: false
2 rule_list	2 rule_list
3 []	3 []

Return

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Attack logs

Unlike **FortiView** which displays threat data in different categories, **Attack Logs** straightforwardly lists all the threats.

Attack log now displays logs from all applications. In **Attack Logs**, You can click an entry to see threat details, or use **Add Filter** to filter out threats as desired. Click **Reload** to update the page with any logs that have been recorded since you previously loaded the page.

A maximum of 10,000 logs are displayed per each filter. FortiWeb Cloud saves the attack logs for two months. After that, they will be deleted.

If you know that certain URL tends to falsely trigger violations by matching an attack signature during normal use, you can click **Add Exception** beside the signature ID. The traffic to the specified URL and/or parameter in the exception rule will not be treated as an attack even if it matches this particular signature. For Request URL and Parameter Name, you should enable at least one. Please wait several minutes for the configuration to take effect.

Date	Action	Threat Level	URL	Client IP	Message																																										
2019-03-29 15:01:56	BLOCK	Critical	/bttatsticajpcsetup.xml	1.83.218.56	Known Attacks: Known Exploits violation in URL																																										
<table><tr><th colspan="2">Client Information</th><th colspan="2">Server Information</th><th colspan="2">Threat Information</th></tr><tr><td>IP Address:</td><td>1.83.218.56</td><td>Domain:</td><td>demo.wafest.cf</td><td>Threat Main Type:</td><td>Known Attacks</td></tr><tr><td>Source Port:</td><td>55862</td><td>Destination Port:</td><td>80</td><td>Threat Sub Type:</td><td>Known Exploits</td></tr><tr><td>Country:</td><td>United States</td><td>HTTP Version:</td><td>1.x</td><td>Signature ID:</td><td>0903000563 Add Exception</td></tr><tr><td>Protocol:</td><td>http</td><td>URL:</td><td>/bttatsticajpcsetup.xml</td><td>CVE-ID:</td><td>CVE-2018-15534</td></tr><tr><td>User Agent:</td><td>python-requests/2.18.4</td><td>Refer:</td><td>none</td><td>OWASP Top 10:</td><td>A3.2017-Using Components with Known Vulnerabilities</td></tr><tr><td colspan="6">Click to view data packet details</td></tr></table>						Client Information		Server Information		Threat Information		IP Address:	1.83.218.56	Domain:	demo.wafest.cf	Threat Main Type:	Known Attacks	Source Port:	55862	Destination Port:	80	Threat Sub Type:	Known Exploits	Country:	United States	HTTP Version:	1.x	Signature ID:	0903000563 Add Exception	Protocol:	http	URL:	/bttatsticajpcsetup.xml	CVE-ID:	CVE-2018-15534	User Agent:	python-requests/2.18.4	Refer:	none	OWASP Top 10:	A3.2017-Using Components with Known Vulnerabilities	Click to view data packet details					
Client Information		Server Information		Threat Information																																											
IP Address:	1.83.218.56	Domain:	demo.wafest.cf	Threat Main Type:	Known Attacks																																										
Source Port:	55862	Destination Port:	80	Threat Sub Type:	Known Exploits																																										
Country:	United States	HTTP Version:	1.x	Signature ID:	0903000563 Add Exception																																										
Protocol:	http	URL:	/bttatsticajpcsetup.xml	CVE-ID:	CVE-2018-15534																																										
User Agent:	python-requests/2.18.4	Refer:	none	OWASP Top 10:	A3.2017-Using Components with Known Vulnerabilities																																										
Click to view data packet details																																															

Request URL

Specify a URL value to match. For example, `/testpage.php`, which match requests for `http://www.test.com/testpage.php`.

- If **String Match** is selected, ensure the value starts with a forward slash (/) (for example, `/testpage.php`). You can enter a precise URL, such as `/folder1/index.htm` or use wildcards to match multiple URLs, such as `/folder1/*`, or `/folder1*/index.htm`.
- If **Regular Expression Match** is selected, the value does not require a forward slash (/). However, ensure that it can match values that contain a

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	forward slash. For details, see Frequently used regular expressions on page 220. Do not include a domain name because it's by default the domain name of this application. Parameter Name Specify a parameter name to match. For example, <code>http://www.test.com/testpage.php?a=1</code>, the parameter name is "a". To create a regular expression, see Frequently used regular expressions on page 220. Please note that the number of attacks displayed in Attack Logs, FortiView , and Blocked Requests widget on Dashboard are slightly different. • Certain attack types such as Bot and DDoS attacks generate a large amount of requests in a short time. To prevent numerous identical attack logs flooding the UI, FortiWeb Cloud only logs the first request in Attack Logs and FortiView , while it shows the actual count in Blocked Requests Widget so you can know how many actual attack requests were blocked. • To prevent Information Leakage, FortiWeb Cloud may cloak the error pages or erase sensitive HTTP headers in response packets. Such items are logged only once per minute in Attack Logs and FortiView for you to know the Information Leakage rule took effect. In the meanwhile, the actual count is recorded in Blocked Requests Widget. • If you have set FortiWeb Cloud to block attacks but not generate a log when certain violation occurs, such as Alert & Deny (no log), then the attacks will not be logged in Attack Logs and FortiView , but will be counted in the Blocked Requests widget. To identify the security feature blocking your request, map the Attack ID value to the corresponding description in the table below.
--	---

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Logs

FortiWeb Cloud saves the attack logs for two months and the audit logs for three months. After that, they will be deleted. Exceptions are added in Attack Logs. It can't be reversed once being added.

If you believe that the Anomaly Detection model is inaccurate with certain exceptions, you have the option to access the TreeView page of the Anomaly Detection module. From there, you can locate the parameter to which the exception is applied and rebuild the model specifically for that parameter. When the new model is rebuilt, the exceptions added to the Anomaly Detection attack logs corresponding to that parameter will be cleared.

In the scanning process, when a request passes through different modules in sequence, the configured action for certain modules can be set to "Alert" or "Monitor". In this case, if an attack is detected by a module with such an action, it will allow the request to continue to the next module for further scanning. However, an attack log will be generated by the module that identified the attack.

As the request progresses through subsequent modules, it is possible for the attack to be logged multiple times by different preceding modules before it is blocked by a module with a different action, such as "Block Period" or "Deny".

As for the scan sequence, please refer to <https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/234292/sequence-of-scans>.

If the `https_host` in GEO IP attack logs shows `none`, it can be solved by enabling **Use X-Header to Identify Original Clients' IP** and **Add X-Forwarded-For** in the **Rewriting Requests** module.

To observe the client's original source IP, it is advised to enable the **Rewriting Requests** module, turning on **X-Forwarded-For**, **X-Real-IP**, and **Use X-Header to Identify Original Clients' IP** options.

Logs are sent from FortiWeb Cloud to the origin server, so the `IP:` header (layer 3) of the logs is supposed to be FortiWeb Cloud's IP address. This is expected behavior.

To check the client real IP, you need to find it in the `X-Forwarded-For:` or `X-Real-IP:` header in the packets forwarded from FortiWeb Cloud to your server. Be aware that to record the client real IP it's required to enable both **Add X-Forwarded-For** and **Use X-Header to Identify Original Client's IP** in the **Rewriting Requests** module.

The signatures used in Known Attacks are primarily designed to detect known patterns of malicious code. However, they may not cover all variants or newly emerging forms of attacks.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

In cases where an attack is logged under the Anomaly Detection threat type instead of being matched with a signature, it in fact indicates the successful functioning of the machine learning model in Anomaly Detection. It effectively screened out unknown or new variant attacks that do not align with existing signatures.

You can view the blocked requests in three places: 1) Attack Logs; 2) FortiView ; 3) Blocked Requests widget on Dashboard. The ways they count the blocked requests are slightly different.

- To prevent Information Leakage, FortiWeb Cloud may cloak the error pages or erase sensitive HTTP headers in response packets. Such item are logged only once per minute in Attack Logs and FortiView for you to know the Information Leakage rule took effect. In the meanwhile, the actual count is recorded in Blocked Requests Widget.
- If you have set FortiWeb Cloud to block attacks but do not generate a log when certain violation occurs, such as Alert & Deny (no log), then the attacks will not be logged in Attack Logs and FortiView , but will be counted in the Blocked Requests widget.
- The invalid requests to the host header HOST will be blocked without generating any log.
- When the Block Mode is in disabled state, attacks won't be blocked but logs are generated.

If you have set FortiWeb Cloud to block attacks but not generate a log when certain violation occurs, such as 'Alert & Deny (no log)', then the attacks will not be logged in Attack Logs and FortiView but will be counted in the Blocked Requests widget.

If you need to have detailed logs for auditing or analysis purposes, you may consider using a different action, such as 'Alert & Deny' or 'Block Period', which will not only block the request but also generate a log entry.

To identify the security feature blocking your request, map the Attack ID value to the corresponding description in the table below.

Incidents

Attack events are aggregated and then grouped into incidents by common characteristics. In this way, you can quickly find out which attack types occur frequently, the most malicious source IP addresses, etc.

By clicking the incident number, you will see the incident details including the attack type, the target application, source IPs, etc.

You can mark an incident as Acknowledged or False Positive, then the corresponding icons will display in the incident's **Status** column. Please note that marking **Acknowledge** or **False Positive** is only for your convenience to track the incidents. The system doesn't take this into account when it detects threats. You can also click the **Comments** link to add comments for the incident.

Last Time	Incident Description	Threads	Blocked	Status
2022-08-29 13:53:21	Known Exploits by 2 IPs from Germany and United States On App: yjgmg-prsd-dtlg/fortiweb-cloud-test.com	5	100/0%	Acknowledged
2022-08-29 13:53:20	Known Exploits by 2 IPs from United Kingdom and United States On App: yjgmg-prsd-dtlg/fortiweb-cloud-test.com	4	100/0%	Acknowledged
2022-08-29 13:53:21	Generic Attacks, SQL Injection by 2 IPs from Russian Federation and Spain On Device: 10.2.1.10	5	100/0%	Acknowledged

Incident Details
App: yjgmg-prsd-dtlg/fortiweb-cloud-test.com
From: 194.233.184.177, 54.90.295.123
Attack Type: Known Exploits
Host: yjgmg-prsd-dtlg/fortiweb-cloud-test.com
CVE IDs: None
URL: /lighttpd/101_status_server-status

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

You can use predefined tags for Threat Analytics incidents. This helps in labeling incidents for future usage such as sorting, filtering and acknowledging incidents. It's supported to edit the tag name according to you needs.

Incident Details

Moderate

Device:

⌵ Azure_on_premise (FVVM08TM22090027)

Policy:

Azureserverpolicy

From:

🇨🇭 Switzerland

34.65.113.188

Attack Type:

Known Exploits

Host:

20.234.81.219

CVE IDs:

N/A

URL:

/DS_Store, /server-status, /git/config

Comments:

0 Comments

Add a tag:

Add a tag

Acknowledged

False Positive

Action Required

Action Taken

22Veryloo

Tag6_subuser_change

123abc

test asdasdad

nTFv&&iK^C@bvqC8U@Re3u*Z1dJlSo

\$t54eL%*sRYr#D3hUw6sR4jgFC0o

Threat Details

Number of Threats:

Blocked:

Timeline:

4

3

2

1

0

Roll down to the bottom of the **Incident Details** page, you can use the **Click to see details** button to open the threat view page which categorizes the attacks by Attack Type, Countries, Hosts, etc.

98

⁹⁸ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

8. The method of claim 1, further comprising: inserting rules into the rule set of the adaptive reference model to augment or override rules of the rule set automatically generated from the snapshots.	FortiEDR and FortiWeb Cloud insert rules into the rule set of the adaptive reference model to augment or override rules of the rule set automatically generated from the snapshots. <i>See, e.g.,</i> FortiEDR “Prevent FortiEDR uses a machine learning anti-malware engine to stop attacks before execution. This cross-OS NGAV capability is configurable and comes built into the single, lightweight agent, allowing users to assign anti-malware protection to any endpoint group without requiring additional installation. • Enable machine learning, kernel-based NGAV • Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database via FortiGuard Threat Intelligence • Protect disconnected endpoints with offline protection • Leverage application control to easily add allowed or blocked applications to pre-defined lists and also provide granular management of applications • USB device control”⁹⁹ Production continuity. Real-time automatic responses can make life difficult for security teams when a legitimate application triggers the detection system and generates a false alarm. Blunt-force response actions can interfere with applications—or worse, cause operating system crashes that bring down a mission-critical production system. FortiEDR continuously classifies events until a final verdict is made. If Fortinet Cloud services classifies an event as safe, an automatic exception is created to prevent such occurrences in the future. FortiEDR’s policy baselining and

⁹⁹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

simulation features can help OT plant managers and security professionals avoid these sorts of occurrences. By running the system in simulation mode, the plant team can exercise all normal plant activities and ensure that endpoint protection and critical plant floor operations are in tune with one another. Recent FortiEDR deployments have been able to find critical OT policy violations such as connected mobile devices, Android services, and unauthorized systems—even before the system was taken out of simulation mode.”¹⁰⁰

“Respond and Remediate

Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux.

- Automate incident classification to improve incident response and ease of resolution
- Recommends response actions to security analysts
- Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation
- Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets
- Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords

¹⁰⁰ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• Get additional help with the optional managed detection and response (MDR) service”¹⁰¹ “Defining security event exceptions Exceptions enable you to limit the enforcement of a rule, meaning to create an allowlist for a specific flow of security events that was used to establish a connection request or perform a specific operation. FortiEDR exception management is highly flexible and provides various options that enable you to define pinpointed, granular exceptions. You can access the Exception Manager by clicking the Exception Manager button at the top of the Events pane or by selecting SECURITY SETTINGS > Exception Manager. Additional options for managing exceptions are provided in the SECURITY SETTINGS tab, as described in Exception Manager. An exception that applies to a security event can result in the creation of several exception pairs. An exception pair specifies the rule that was violated and the process on which the violation occurred, including or excluding its entire location path. For more details, see Playbook policies After an exception is defined for a security event, new identical events will no longer be triggered and different indication icons are added to existing events, depending on the exception's coverage of the raw data items in the events: Security events fully covered by the exception have the icon to indicate that an exception has already been defined (although the exception was created after the event occurred) and there is no need to create another exception for them. The indication icon does not refresh afterward when new raw data items uncovered by the exception come in. If the exception does not fully cover all the existing occurrences or raw data items of an event, the icon is displayed.”¹⁰² “FortiEDR Cloud Service The FortiEDR Cloud Service (FCS) enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event. The FCS is a cloud-based, GDPR-compliant, software-only
--	---

¹⁰¹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

¹⁰² <https://docs.fortinet.com/document/fortiedr/6.2.0/administration-guide/182447/defining-security-event-exceptions>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy.

The FCS security event classification process is done via data enrichment and enhanced deep, thorough analysis and investigation, enabled by automated and manual processes. The enhanced processes may include (partial list) intelligence services, file analysis (static and dynamic), sandboxing, flow analysis via machine learning, commonalities analysis, crowdsourced data deduction and more.

Along with potential classification reassurance or reclassification, once connected, FCS can also enable several followed actions, which can be divided into two main activities:

- **Tuning:** Automated security event exception (allowlisting). After a triggered security event is reclassified as Safe, an automated cross-environment exception can be pushed downstream and expire the event, preventing it from triggering again. For more details, see Exception Manager
- **Playbook Actions:** All Playbook policy remediation actions are based on the final determination of the FCS. For more details see Remediation.”¹⁰³

FortiWeb Cloud

Global Trustlist

You can configure FortiWeb Cloud to ignore scanning parameters specified for modules of signature based detection, syntax based detection, and anomaly detection across the entire application.

1. Go to **SECURITY RULES > Global Trustlist**.
You must have already enabled this module in **Add Modules**. See [How to add or remove a module](#).
2. Click **Create New**.
3. Configure these settings.

Parameter Name	Enter a unique name for the parameter as it appears in the URL or HTTP body.
Request Status	Optionally, you can enable to indicate a regular expression designed to match multiple URLs, which carry the trustlist parameters.

¹⁰³ <https://docs.fortinet.com/document/fortiedr/7.0.0/administration-guide/970632/fortiedr-components>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Request URL

Specify a URL value to match, such as `^/*.php`, which matches requests for `http://www.test.com/^/*.php`. The pattern does not require a slash (`/`); however, it must at match URLs that begin with a slash, such as `/index.cfm`.
See [Frequently used regular expressions on page 242](#).
Do not include a domain name because it's by default the domain name of this application.

4. Click OK.

In the global trustlist table, you can click buttons    to edit, or delete the parameter rule; also, you can choose to enable or disable to indicate the URL to match.

Attack logs

Unlike **FortiView** which displays threat data in different categories, **Attack Logs** straightforwardly lists all the threats.

Attack log now displays logs from all applications. In **Attack Logs**, You can click an entry to see threat details, or use **Add Filter** to filter out threats as desired. Click **Reload** to update the page with any logs that have been recorded since you previously loaded the page.

A maximum of 10,000 logs are displayed per each filter. FortiWeb Cloud saves the attack logs for two months. After that, they will be deleted.

If you know that certain URL tends to falsely trigger violations by matching an attack signature during normal use, you can click **Add Exception** beside the signature ID. The traffic to the specified URL and/or parameter in the exception rule will not be treated as an attack even if it matches this particular signature. For Request URL and Parameter Name, you should enable at least one. Please wait several minutes for the configuration to take effect.

Date	Action	Threat Level	URL	Client IP	Message																																										
2019-03-29 15:01:56	BLOCK	Critical	ibattobidgpcsetup.xml	1.83.218.56	Known Attacks: Known Exploits violation in URL																																										
<table><tr><th colspan="2">Client Information</th><th colspan="2">Server Information</th><th colspan="2">Threat Information</th></tr><tr><td>IP Address:</td><td>1.83.218.56</td><td>Domain:</td><td>demo.wafest.cf</td><td>Threat Main Type:</td><td>Known Attacks</td></tr><tr><td>Source Port:</td><td>55862</td><td>Destination Port:</td><td>80</td><td>Threat Sub Type:</td><td>Known Exploits</td></tr><tr><td>Country:</td><td>United States</td><td>HTTP Version:</td><td>1.x</td><td>Signature ID:</td><td>090300052 Add Exception</td></tr><tr><td>Protocol:</td><td>http</td><td>URL:</td><td>ibattobidgpcsetup.xml</td><td>CVE-ID:</td><td>CVE-2018-15534</td></tr><tr><td>User Agent:</td><td>python-requests/2.18.4</td><td>Refer:</td><td>none</td><td>OWASP Top 10:</td><td>A3.2017-Using Components with Known Vulnerabilities</td></tr><tr><td colspan="6">Click to view data packet details</td></tr></table>						Client Information		Server Information		Threat Information		IP Address:	1.83.218.56	Domain:	demo.wafest.cf	Threat Main Type:	Known Attacks	Source Port:	55862	Destination Port:	80	Threat Sub Type:	Known Exploits	Country:	United States	HTTP Version:	1.x	Signature ID:	090300052 Add Exception	Protocol:	http	URL:	ibattobidgpcsetup.xml	CVE-ID:	CVE-2018-15534	User Agent:	python-requests/2.18.4	Refer:	none	OWASP Top 10:	A3.2017-Using Components with Known Vulnerabilities	Click to view data packet details					
Client Information		Server Information		Threat Information																																											
IP Address:	1.83.218.56	Domain:	demo.wafest.cf	Threat Main Type:	Known Attacks																																										
Source Port:	55862	Destination Port:	80	Threat Sub Type:	Known Exploits																																										
Country:	United States	HTTP Version:	1.x	Signature ID:	090300052 Add Exception																																										
Protocol:	http	URL:	ibattobidgpcsetup.xml	CVE-ID:	CVE-2018-15534																																										
User Agent:	python-requests/2.18.4	Refer:	none	OWASP Top 10:	A3.2017-Using Components with Known Vulnerabilities																																										
Click to view data packet details																																															

Request URL

Specify a URL value to match. For example, `/testpage.php`, which match requests for `http://www.test.com/testpage.php`.

- If **String Match** is selected, ensure the value starts with a forward slash (`/`) (for example, `/testpage.php`). You can enter a precise URL, such as `/folder1/index.htm` or use wildcards to match multiple URLs, such as `/folder1/*`, or `/folder1*/index.htm`.
- If **Regular Expression Match** is selected, the value does not require a forward slash (`/`). However, ensure that it can match values that contain a

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	3. Click +Create Exception Rule under Signature Based Detection section to omit attack signature scans when you know that some parameters or URLs cause false positives by matching an attack signature during normal use. Logs FortiWeb Cloud saves the attack logs for two months and the audit logs for three months. After that, they will be deleted. Exceptions are added in Attack Logs. It can't be reversed once being added. If you believe that the Anomaly Detection model is inaccurate with certain exceptions, you have the option to access the TreeView page of the Anomaly Detection module. From there, you can locate the parameter to which the exception is applied and rebuild the model specifically for that parameter. When the new model is rebuilt, the exceptions added to the Anomaly Detection attack logs corresponding to that parameter will be cleared. In the scanning process, when a request passes through different modules in sequence, the configured action for certain modules can be set to "Alert" or "Monitor". In this case, if an attack is detected by a module with such an action, it will allow the request to continue to the next module for further scanning. However, an attack log will be generated by the module that identified the attack. As the request progresses through subsequent modules, it is possible for the attack to be logged multiple times by different preceding modules before it is blocked by a module with a different action, such as "Block Period" or "Deny". As for the scan sequence, please refer to https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/234292/sequence-of-scans. If the <code>https_host</code> in GEO IP attack logs shows <code>none</code>, it can be solved by enabling Use X-Header to Identify Original Clients' IP and Add X-Forwarded-For in the Rewriting Requests module. To observe the client's original source IP, it is advised to enable the Rewriting Requests module, turning on X-Forwarded-For, X-Real-IP, and Use X-Header to Identify Original Clients' IP options. Logs are sent from FortiWeb Cloud to the origin server, so the <code>IP:</code> header (layer 3) of the logs is supposed to be FortiWeb Cloud's IP address. This is expected behavior. To check the client real IP, you need to find it in the <code>X-Forwarded-For:</code> or <code>X-Real-IP:</code> header in the packets forwarded from FortiWeb Cloud to your server. Be aware that to record the client real IP it's required to enable both Add X-Forwarded-For and Use X-Header to Identify Original Client's IP in the Rewriting Requests module. The signatures used in Known Attacks are primarily designed to detect known patterns of malicious code. However, they may not cover all variants or newly emerging forms of attacks.
9. The method of claim 1, wherein the adaptive reference model is generated to include a value layer that	FortiEDR and FortiWeb Cloud's adaptive reference model is generated to include a value layer that determines whether an asset value contained in a snapshot is anomalous. <i>See, e.g.,</i> FortiEDR

¹⁰⁴ https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9687b55-f2f2-11ee-8c42-fa163e15d75b/FortiWeb_Cloud_User_Guide.pdf.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

determines whether an asset value contained in a snapshot is anomalous.	“FortiEDR surgically stops data breaches and ransomware damage in real time, automatically allowing business continuity even on already compromised devices. • Leverage OS-centric detection, highly accurate in detecting stealthy infiltrated attacks, including memory-based and “living off the land” attacks • Stop breaches in real time and eliminate threat dwell time • Achieve analysis of entire log history • Prevent ransomware encryption, and file/registry tempering • Continuously validate the classification of threats with FortiGuard Threat Intelligence and multi-engine sandboxing, both within Fortinet Cloud Services • Enhance signal-to-noise ratio and eliminate alert fatigue • Support for Mobile OS, including Android and iOS”¹⁰⁵ “FortiEDR Core The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked. FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows. • When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
---	--

¹⁰⁵ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it. • The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration. • The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred. • When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it. • The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration. • The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.”¹⁰⁶ “Prevent FortiEDR uses a machine learning anti-malware engine to stop attacks before execution. This cross-OS NGAV capability is configurable and comes built into the single, lightweight agent, allowing users to assign anti-malware protection to any endpoint group without requiring additional installation. • Enable machine learning, kernel-based NGAV • Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database via FortiGuard Threat Intelligence • Protect disconnected endpoints with offline protection • Leverage application control to easily add allowed or blocked applications to pre-defined lists and also provide granular management of applications
--	---

¹⁰⁶ *Id.*

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• USB device control”¹⁰⁷ “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution • Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups) • Gain full visibility of the attack chain and malicious changes with patented code tracing • Automate cleanup and roll back malicious changes while preserving system uptime • Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords • Get additional help with the optional managed detection and response (MDR) service”¹⁰⁸
--	--

¹⁰⁷ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

¹⁰⁸ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Production continuity. Real-time automatic responses can make life difficult for security teams when a legitimate application triggers the detection system and generates a false alarm. Blunt-force response actions can interfere with applications—or worse, cause operating system crashes that bring down a mission-critical production system. FortiEDR continuously classifies events until a final verdict is made. If Fortinet Cloud services classifies an event as safe, an automatic exception is created to prevent such occurrences in the future. FortiEDR’s policy baselining and simulation features can help OT plant managers and security professionals avoid these sorts of occurrences. By running the system in simulation mode, the plant team can exercise all normal plant activities and ensure that endpoint protection and critical plant floor operations are in tune with one another. Recent FortiEDR deployments have been able to find critical OT policy violations such as connected mobile devices, Android services, and unauthorized systems—even before the system was taken out of simulation mode.”¹⁰⁹

“Discover and Predict FortiEDR delivers the most advanced automated attack surface policy control with vulnerability assessments and discovery that allows security teams to:

- Discover and control rogue devices (such as unprotected or unmanaged devices) and IoT devices
- Track applications and their CVE status
- Discover and mitigate the exploit of system and application vulnerabilities with virtual patching and risk-based proactive policies”¹¹⁰

“FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”¹¹¹

¹⁰⁹ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

¹¹⁰ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

¹¹¹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiEDR—Cloud-native EPP + EDR

Detect, Defuse, Respond, and Remote Remediation

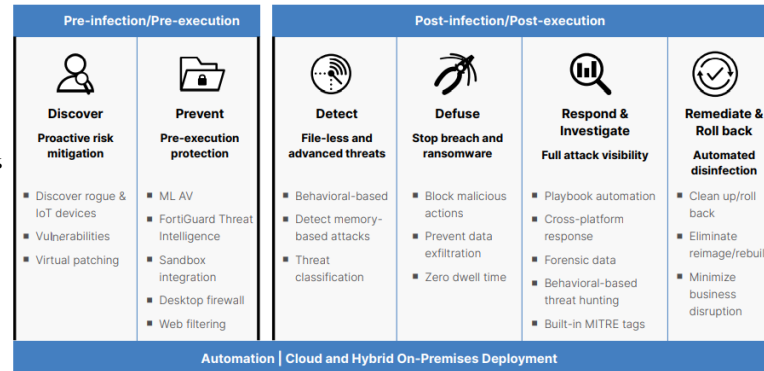


Figure 1: FortiEDR combines both pre-infection and post-infection endpoint defenses.

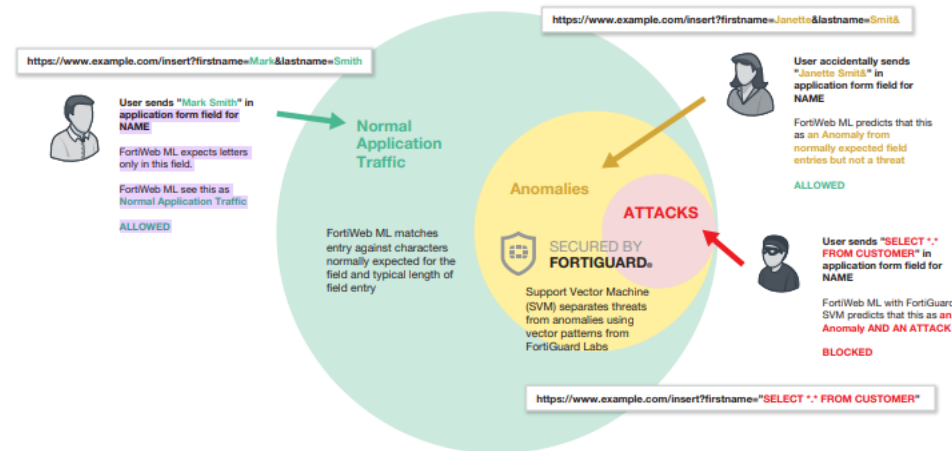
FortiWeb Cloud

¹¹² <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Highlights

FortiWeb's machine learning accurately detects anomalies and identifies which are threats. Unlike prevailing auto-learning detection models used by other WAF vendors that treat every anomaly as a threat, FortiWeb's precision nearly eliminates false positive detections and catches attack types that others cannot.



113

FortiWeb's AI-based machine learning evaluates application requests to determine if they are normal, benign anomalies, or anomalies that are threats.

Parameter list

The Parameters list shows all the parameters attached to the URL. For example, if the URL is http://www.demo.com/1.php?user_name=jack, then user_name is the parameter. The system builds machine learning model for each parameter, and detects the abnormal parameter values.

¹¹³ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Anomaly Detection Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks: • Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access • Matches anomalies against pre-trained threat models • Detects attacks Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service. Model settings FortiWeb Cloud parses all the URLs in a domain, and builds anomaly detection models for all parameters attached to the URLs. After anomaly detection model is built, the system will keep on calculating the probability of the new samples and compare it against the model. If the probability of the new samples varies to a large extent for a long period, the system determines this parameter has changed and automatically rebuilds the model based on the new samples.
10. The method of claim 1, wherein the adaptive reference model is generated to include a cluster layer that tracks relationships between assets and identifies an anomaly in response to an asset being unexpectedly absent from or	FortiEDR and FortiWeb Cloud’s adaptive reference model is generated to include a cluster layer that tracks relationships between assets and identifies an anomaly in response to an asset being unexpectedly absent from or present in a set of assets in a snapshot. <i>See, e.g.,</i> FortiEDR “FortiEDR surgically stops data breaches and ransomware damage in real time, automatically allowing business continuity even on already compromised devices. • Leverage OS-centric detection, highly accurate in detecting stealthy infiltrated attacks, including memory-based and “living off the land” attacks • Stop breaches in real time and eliminate threat dwell time

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

present in a set of assets in a snapshot.	• Achieve analysis of entire log history • Prevent ransomware encryption, and file/registry tempering • Continuously validate the classification of threats with FortiGuard Threat Intelligence and multi-engine sandboxing, both within Fortinet Cloud Services • Enhance signal-to-noise ratio and eliminate alert fatigue • Support for Mobile OS, including Android and iOS”¹¹⁴ “FortiEDR Core The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked. FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows. • When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious. • When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it. • The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization’s policy by blocking (or only logging) the connection request in order to prevent/log exfiltration. • The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred. • When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
---	--

¹¹⁴ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization’s policy by blocking (or only logging) the connection request in order to prevent/log exfiltration. • The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.”¹¹⁵ “Prevent FortiEDR uses a machine learning anti-malware engine to stop attacks before execution. This cross-OS NGAV capability is configurable and comes built into the single, lightweight agent, allowing users to assign anti-malware protection to any endpoint group without requiring additional installation. • Enable machine learning, kernel-based NGAV • Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database via FortiGuard Threat Intelligence • Protect disconnected endpoints with offline protection • Leverage application control to easily add allowed or blocked applications to pre-defined lists and also provide granular management of applications • USB device control”¹¹⁶ “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution
--	---

¹¹⁵ *Id.*

¹¹⁶ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- Recommends response actions to security analysts
- Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation
- Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets
- Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords
- Get additional help with the optional managed detection and response (MDR) service”¹¹⁷

Production continuity. Real-time automatic responses can make life difficult for security teams when a legitimate application triggers the detection system and generates a false alarm. Blunt-force response actions can interfere with applications—or worse, cause operating system crashes that bring down a mission-critical production system. FortiEDR continuously classifies events until a final verdict is made. If Fortinet Cloud services classifies an event as safe, an automatic exception is created to prevent such occurrences in the future. FortiEDR’s policy baselining and simulation features can help OT plant managers and security professionals avoid these sorts of occurrences. By running the system in simulation mode, the plant team can exercise all normal plant activities and ensure that endpoint protection and critical plant floor operations are in tune with one another. Recent FortiEDR deployments have been able to find critical OT policy violations such as connected mobile devices, Android services, and unauthorized systems—even before the system was taken out of simulation mode.”¹¹⁸

¹¹⁷ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

¹¹⁸ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	“Discover and Predict FortiEDR delivers the most advanced automated attack surface policy control with vulnerability assessments and discovery that allows security teams to: • Discover and control rogue devices (such as unprotected or unmanaged devices) and IoT devices • Track applications and their CVE status • Discover and mitigate the exploit of system and application vulnerabilities with virtual patching and risk-based proactive policies”¹¹⁹ “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”¹²⁰
--	---

¹¹⁹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

¹²⁰ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiEDR—Cloud-native EPP + EDR

Detect, Defuse, Respond, and Remote Remediation

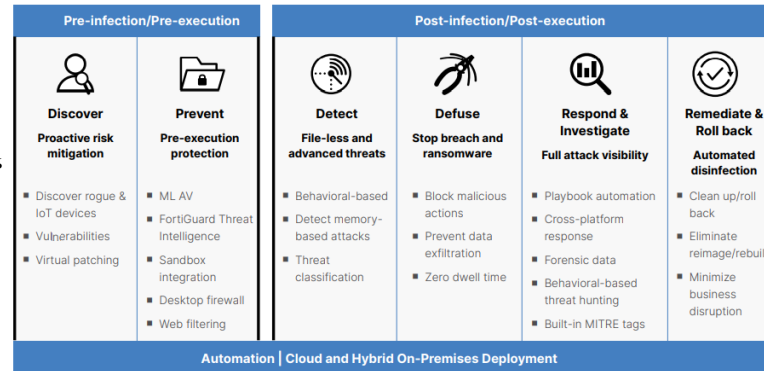


Figure 1: FortiEDR combines both pre-infection and post-infection endpoint defenses.

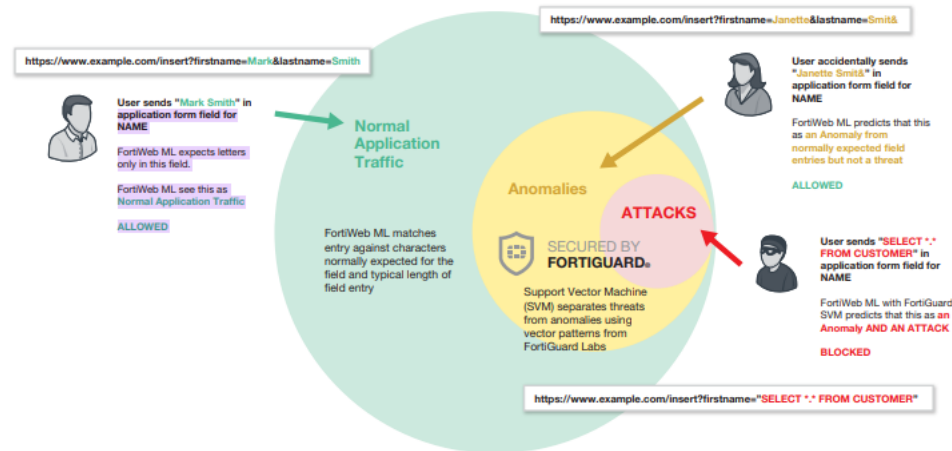
FortiWeb Cloud

¹²¹ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Highlights

FortiWeb's machine learning accurately detects anomalies and identifies which are threats. Unlike prevailing auto-learning detection models used by other WAF vendors that treat every anomaly as a threat, FortiWeb's precision nearly eliminates false positive detections and catches attack types that others cannot.



122

FortiWeb's AI-based machine learning evaluates application requests to determine if they are normal, benign anomalies, or anomalies that are threats.

Parameter list

The Parameters list shows all the parameters attached to the URL. For example, if the URL is `http://www.demo.com/1.php?user_name=jack`, then `user_name` is the parameter. The system builds machine learning model for each parameter, and detects the abnormal parameter values.

¹²² <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Anomaly Detection Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks: • Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access • Matches anomalies against pre-trained threat models • Detects attacks Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service. Model settings FortiWeb Cloud parses all the URLs in a domain, and builds anomaly detection models for all parameters attached to the URLs. After anomaly detection model is built, the system will keep on calculating the probability of the new samples and compare it against the model. If the probability of the new samples varies to a large extent for a long period, the system determines this parameter has changed and automatically rebuilds the model based on the new samples.
11. The method of claim 1, wherein the adaptive reference model is generated to include a profile layer that identifies anomalies in response to violation of relationships of clusters of assets in a snapshot.	FortiEDR and FortiWeb Cloud’s adaptive reference model is generated to include a profile layer that identifies anomalies in response to violation of relationships of clusters of assets in a snapshot. <i>See, e.g.,</i> FortiEDR “FortiEDR surgically stops data breaches and ransomware damage in real time, automatically allowing business continuity even on already compromised devices. • Leverage OS-centric detection, highly accurate in detecting stealthy infiltrated attacks, including memory-based and “living off the land” attacks • Stop breaches in real time and eliminate threat dwell time

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

- Achieve analysis of entire log history
- Prevent ransomware encryption, and file/registry tempering
- Continuously validate the classification of threats with FortiGuard Threat Intelligence and multi-engine sandboxing, both within Fortinet Cloud Services
- Enhance signal-to-noise ratio and eliminate alert fatigue
- Support for Mobile OS, including Android and iOS”¹²³

“FortiEDR Core

The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows.

- When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization’s policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.

¹²³ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization’s policy by blocking (or only logging) the connection request in order to prevent/log exfiltration. • The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.”¹²⁴ “Prevent FortiEDR uses a machine learning anti-malware engine to stop attacks before execution. This cross-OS NGAV capability is configurable and comes built into the single, lightweight agent, allowing users to assign anti-malware protection to any endpoint group without requiring additional installation. • Enable machine learning, kernel-based NGAV • Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database via FortiGuard Threat Intelligence • Protect disconnected endpoints with offline protection • Leverage application control to easily add allowed or blocked applications to pre-defined lists and also provide granular management of applications • USB device control”¹²⁵ “Respond and Remediate Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes. Manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment on Windows (without reliance on VSS images which are targeted by ransomware), macOS, and Linux. • Automate incident classification to improve incident response and ease of resolution
--	---

¹²⁴ *Id.*

¹²⁵ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	• Recommends response actions to security analysts • Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation • Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets • Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups) • Gain full visibility of the attack chain and malicious changes with patented code tracing • Automate cleanup and roll back malicious changes while preserving system uptime • Integrates with identity-based tools like ZTNA and others to drive detections and tag devices as well as reset passwords • Get additional help with the optional managed detection and response (MDR) service”¹²⁶ Production continuity. Real-time automatic responses can make life difficult for security teams when a legitimate application triggers the detection system and generates a false alarm. Blunt-force response actions can interfere with applications—or worse, cause operating system crashes that bring down a mission-critical production system. FortiEDR continuously classifies events until a final verdict is made. If Fortinet Cloud services classifies an event as safe, an automatic exception is created to prevent such occurrences in the future. FortiEDR’s policy baselining and simulation features can help OT plant managers and security professionals avoid these sorts of occurrences. By running the system in simulation mode, the plant team can exercise all normal plant activities and ensure that endpoint protection and critical plant floor operations are in tune with one another. Recent FortiEDR deployments have been able to find critical OT policy violations such as connected mobile devices, Android services, and unauthorized systems—even before the system was taken out of simulation mode.”¹²⁷
--	--

¹²⁶ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

¹²⁷ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	“Discover and Predict FortiEDR delivers the most advanced automated attack surface policy control with vulnerability assessments and discovery that allows security teams to: • Discover and control rogue devices (such as unprotected or unmanaged devices) and IoT devices • Track applications and their CVE status • Discover and mitigate the exploit of system and application vulnerabilities with virtual patching and risk-based proactive policies”¹²⁸ “FortiEDR detects and defuses file-less malware and other advanced attacks in real time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR’s back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.”¹²⁹
--	---

¹²⁸ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

¹²⁹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

FortiEDR—Cloud-native EPP + EDR

Detect, Defuse, Respond, and Remote Remediation

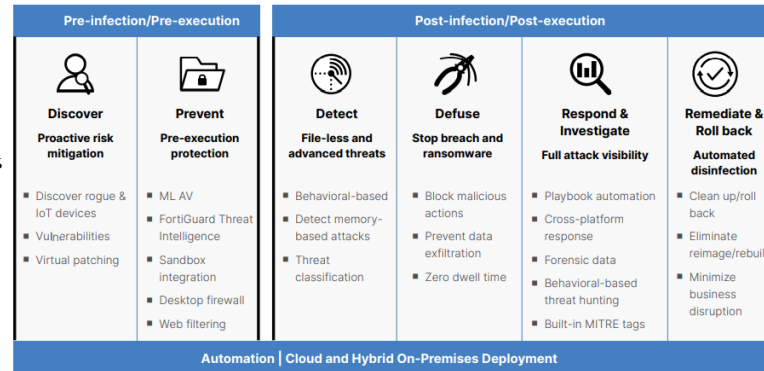


Figure 1: FortiEDR combines both pre-infection and post-infection endpoint defenses.

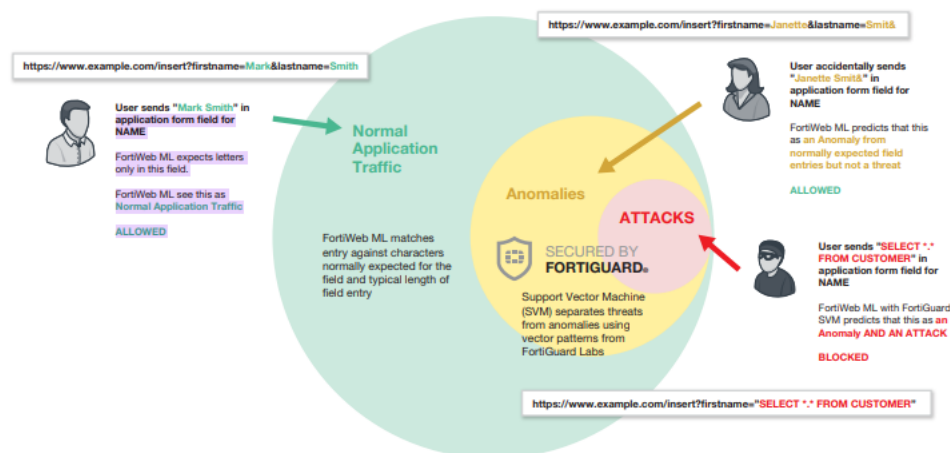
FortiWeb Cloud

¹³⁰ <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-ot-infrastructures.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

Highlights

FortiWeb's machine learning accurately detects anomalies and identifies which are threats. Unlike prevailing auto-learning detection models used by other WAF vendors that treat every anomaly as a threat, FortiWeb's precision nearly eliminates false positive detections and catches attack types that others cannot.



131

FortiWeb's AI-based machine learning evaluates application requests to determine if they are normal, benign anomalies, or anomalies that are threats.

Parameter list

The Parameters list shows all the parameters attached to the URL. For example, if the URL is `http://www.demo.com/1.php?user_name=jack`, then `user_name` is the parameter. The system builds machine learning model for each parameter, and detects the abnormal parameter values.

¹³¹ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf>.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

	Anomaly Detection Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks: • Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access • Matches anomalies against pre-trained threat models • Detects attacks Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service. Model settings FortiWeb Cloud parses all the URLs in a domain, and builds anomaly detection models for all parameters attached to the URLs. After anomaly detection model is built, the system will keep on calculating the probability of the new samples and compare it against the model. If the probability of the new samples varies to a large extent for a long period, the system determines this parameter has changed and automatically rebuilds the model based on the new samples.
12(pre) A computer readable medium storing instructions, that when executed by a computer, cause the computer to perform functions of:	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim limitation 1(pre).</i>
12(a) receiving snapshots from a plurality of computers within a population of computers, wherein individual	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim limitation 1(a) and 1(a)(i).</i>

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

snapshots include data indicating a state of a respective computer;	
12(b) automatically generating an adaptive reference model comprising a rule set customized to characteristics of the population of computers, the rule set being developed by identifying patterns among the snapshots from the plurality of computers such that the adaptive reference model is indicative of normal states in the computers within the population; and	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim limitation 1(b) and 1(b)(i).</i>
12(c) comparing a snapshot from at least one of the computers to the adaptive reference model to determine whether an	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim limitation 1(c).</i>

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

anomaly is present in the state of the at least one of the computers.	
13. The computer readable medium of claim 12, further comprising instructions, that when executed, cause the computer to compare the anomaly to a recognition filter to diagnose a trouble condition on the at least one of the computers, and, in the event of a trouble condition, to generate an automated response to the trouble condition.	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 2.</i>
14(pre) The computer readable medium of claim 13, wherein the automated response is a generic response not	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 3.</i>

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

specific to a particular asset of the at least one computer, and wherein the computer readable medium further comprises instructions, that when executed, cause the computer to:	
14(a) send the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of anomalies indicating assets of the at least one computer whose states are anomalous; and	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 3.</i>
14(b) apply the generic response to the anomalous assets to correct the trouble condition.	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 3.</i>

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

15. The computer readable medium of claim 14, wherein the generic responses include at least one of: installing a missing software component, removing an undesirable software component, and restoring an incorrect registry setting.	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 4.</i>
16. The computer readable medium of claim 13, wherein the recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions.	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 5.</i>
17. The computer readable medium of	FortiEDR and FortiWeb Cloud disclose this limitation.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

claim 12, wherein the instructions for comparing the snapshot to the adaptive reference model include instructions for determining whether an asset value contained in a snapshot is anomalous.	<i>See, e.g.,</i> claim 9.
18. The computer readable medium of claim 12, wherein the instructions for comparing the snapshot to the adaptive reference model include instructions for tracking relationships between assets and identifying an anomaly in response to an asset being unexpectedly absent from or present in a set of assets in a snapshot.	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g.,</i> claim 10.

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

19. The computer readable medium of claim 12, wherein the instructions for comparing the snapshot to the adaptive reference model include instructions for identifying anomalies in response to violation of relationships of clusters of assets in a snapshot.	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 11.</i>
20(pre) The computer readable medium of claim 12, wherein the computer readable medium further comprises instructions, that when executed, cause the computer to:	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 6.</i>
20(a) compare a plurality of anomalies associated with a	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 6.</i>

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

particular snapshot with a recognition filter to diagnose a trouble condition; and	
20(b) diagnose a trouble condition on the at least one of the computers in response to at least a subset of the plurality of anomalies matching information in the recognition filter.	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 6.</i>
21. The computer readable medium of claim 12, wherein individual snapshots include data associated with at least one of: system files, application files, a registry entry, a performance counter, a process, a communication port, a hardware configuration, a log file, a running task,	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 7.</i>

Exhibit 15: Infringement of U.S. Patent No. 7,593,936 by Fortinet

services, and network connections.	
22(pre) The computer readable medium of claim 12, wherein the computer readable medium further comprises instructions, that when executed, cause the computer to:	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 8.</i>
22(a) insert rules into the rule set of the adaptive reference model to augment or override rules of the rule set automatically generated from the snapshots.	FortiEDR and FortiWeb Cloud disclose this limitation. <i>See, e.g., claim 8.</i>