

EX 1008

EXHIBIT 15

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

Netskope sets forth the allegations in this claim chart based on information and belief, relying on the precedent established in *Hoffman-La Roche Inc. v. Invamend Inc.*, 213 F.3d 1359 (Fed. Cir. 2000). The accused product, FortiEDR, and other products which operate in a reasonably similar manner infringe at least claim 1 of U.S. Patent No. 7,593,936 (the “’936 Patent”).

U.S. Patent No. 7,593,936	Fortinet’s FortiEDR Product – Representative Evidence
1(pre) A method of detecting abnormal system states in computers, comprising:	FortiEDR detects abnormal system states in computers. <i>See, e.g.:</i> “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. 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.

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

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.”²
1(a) receiving snapshots from a plurality of computers within a population of computers,	FortiEDR receives snapshots from a plurality of computers within a population of computers. <i>See, e.g.:</i> “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.”³ “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.

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

³ <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

	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.”⁴
1(a)(i) wherein individual snapshots include data indicating a state of a respective computer;	FortiEDR discloses individual snapshots that include data indicating a state of a respective computer. <i>See, e.g:</i> “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.”⁵

⁴ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/717228/how-does-fortiedr-work>.

⁵ <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

	“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.
--	---

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.”⁶
1(b) automatically generating an adaptive reference model comprising a rule set customized to characteristics of the population of computers,	FortiEDR automatically generates an adaptive reference model comprising a rule set customized to characteristics of the population of computers. <i>See, e.g.:</i> “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.”⁷ “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.”⁸

⁶ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/970632/fortiedr-components>.

⁷ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/236616/out-of-the-box-policies>.

⁸ <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

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 discloses 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> “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.”⁹
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 compares 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> “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.

⁹ <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

	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.”¹⁰ “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.
--	--

¹⁰ <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

	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.”¹¹
--	--

¹¹ <https://docs.fortinet.com/document/fortiedr/5.2.0/administration-guide/717228/how-does-fortiedr-work>.