

Uncover hidden risks

Watch how the Wiz platform can expose unseen risks in your cloud environment without drowning your team in alerts.

 [Get a demo](#)

[All articles](#)

Agentless vs. Agent-Based is Better for the Cloud?

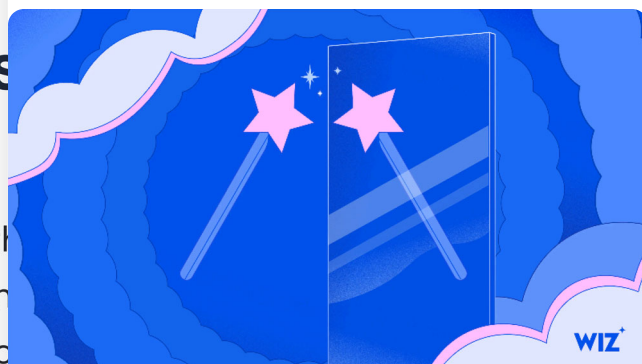
Agentless and agent-based systems are both used for cloud security. There is no single right answer when it comes to which is better, as each comes with its own advantages and drawbacks.



Greg Zemlin

November 26, 2023

7 minutes read



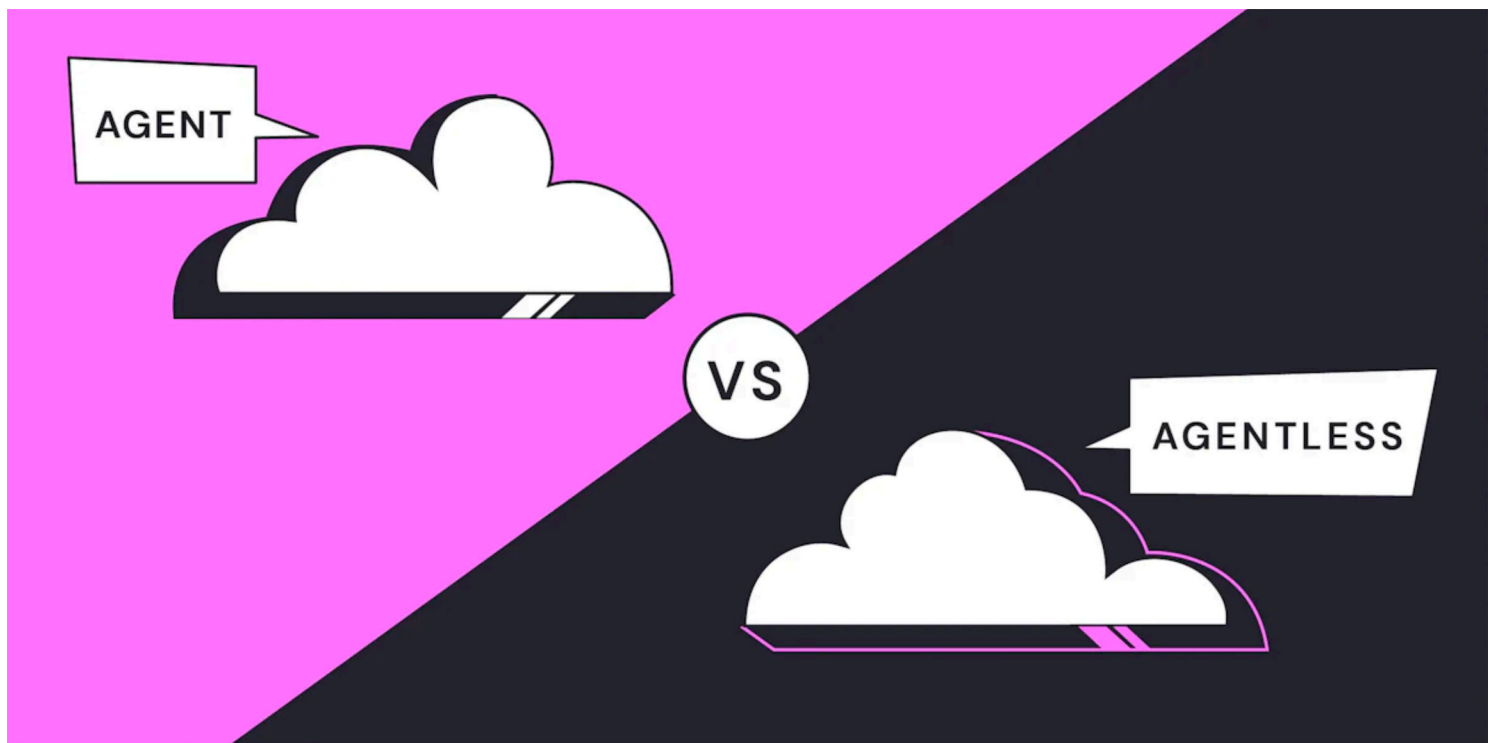
Welcome 🤝

Looking to create a secure cloud environment to accelerate your business?

[Book a demo](#)

[Request a custom quote](#)

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our Privacy Policy.



Cloud environments are dynamic by nature. It's easier now than ever before to spin up new resources and add new technologies, which leads to a growing number of people and teams deploying in the cloud.

Ephemeral resources like serverless functions and containers can contribute to workloads being added and removed at blistering speeds. From a security perspective, these changes have made keeping up with the cloud all the more challenging. The dynamic nature of the cloud has strained some traditional security approaches to the breaking point. One component under scrutiny is the scanning agent.

Although agents still have an important role to play in cloud environments, they are best positioned as the last line of defense for threat detection. Agent-based scanning is not the most suitable for visibility, risk or compliance assessments.

What is agentless security?

Agentless security provides visibility into the threats in your environments, without requiring the installation of software-driven agents.

Under the agent-based model, each of your hosts must run a monitoring process that collects data from the host's environment and sends it to your security service. Agentless security removes this requirement by having the service collect data itself, using cloud provider APIs and metadata.

Agentless analysis approaches are based on two fundamental principles:

- Privileged access to customer's cloud environment via APIs
- Snapshot scanning

Privileged access assigned to the security vendor enables discovery of all resources and services used in the cloud environment. This information is then processed to determine the list of workloads to be scanned.

The workload scanner is responsible for analyzing workloads. It uses the information described above to create snapshots in the environment, mount them as read-only file systems, examine the VMs that are spun up from the snapshot to identify vulnerabilities, and finally delete them.

Agentless is easier to set up and maintain because you don't need to configure an agent on each of your hosts. This reduces friction and ensures effortless coverage of your cloud resources. Moreover, agentless security can directly reduce your attack surface by eliminating the risk posed by network-connected agent processes.

Agents are not enough: Why cloud security needs agentless deep scanning

[Read more](#)



Agentless security vs. agent-based security

Agentless and agent-based systems are both valid approaches for cloud security. There is no single right answer when deciding which to choose, as each comes with its own advantages and drawbacks.

Advantages of agent-based security

Agent-based security is generally seen as the traditional method. This is mainly because it's broadly understood and matches expectations of how security solutions should be administered. While the setup is more complex and laborious, it can *feel* familiar because it's predictable: You install the agent on your systems, authenticate to your cloud security service, and then watch the data flow in.

Here are some of the reasons why agents still find favor with security teams, along with some caveats as to why they are not the ideal choice for cloud.

Can fulfill an active role

Agents can do more than just siphon logs, metrics, and vulnerability alerts to your security platform. They're also capable of enforcing policies and making host config changes that improve security, such as by enabling firewalls or pruning unused applications.

However, all this comes at the cost of having to install the agent on each of your systems. The powerful on-device functionality is also a security risk: If the agent is compromised, then an attacker could abuse the agent's host access to apply their own changes.

Works across infrastructure types

Agents can be deployed to any compatible host, whether in the cloud, your own data center, or on employee devices, enabling standardization of your security tools.

Unfortunately, this also means there's a burden on IT teams to ensure agents are consistently configured. The challenge involved in scaling agents to support thousands of devices shouldn't be underestimated. If you're already running all your endpoints in the cloud, then it'll be simpler and safer to select an agentless service instead.

WIZ BLOG

Wiz's agentless approach to cloud-native vulnerability management

[Read more](#)



Doesn't require a central service

Agents can operate independently of the service they're controlled by, functioning autonomously within their given environment. This decentralizes your security model and makes it more resilient to incidents like network or platform outages.

Unfortunately, this is of limited practical utility. Effective cloud security management depends on “single pane of glass” visibility using a unified platform that lets you see every threat in your environment. Offline, disconnected, or individually managed agents don’t satisfy this requirement.

Disadvantages of agent-based security

While the advantages of agent-based security aren't without merit, agents also [present numerous drawbacks](#) that admins and security teams need to address.

Can cause coverage gaps

Agent-based security depends on the agent being installed and enabled on each device in your fleet. It's up to administrators and operators to implement processes that ensure this actually happens. If a new host is deployed without the agent, there is still the risk of the host being compromised.



The agent software requires maintenance to prevent it from becoming outdated or [misconfigured](#). These admin tasks are tedious and burdensome because they need to be replicated across all of your resources that use the agent.

WIZ BLOG

Wiz introduces agentless solution for detecting host and application misconfigurations

[Read more](#)



Can reduce system performance

Agents are usually designed to be lightweight, but they're still another process that's running on your hosts. Constantly analyzing threats and relaying data to the server can lower system performance and lead to increased resource consumption. Agent activity can even push your cloud compute nodes into higher-priced deployment tiers, causing unplanned cost increases that lead to budget overruns.

Risk of vendor lock-in

It's difficult to switch between agent-based security solutions because you need to remove the old agents, then install the new ones. This is a daunting task for organizations that have hundreds or thousands of endpoints, and they will more likely feel locked into their current vendor.

Can create security problems

Agents are there to protect security, but any problems with the agent process can actually pose a security threat. Agents are by nature privileged, networked processes that continually run on your hosts. A successful compromise is likely to expose sensitive system information, and multiple CVEs [have been reported](#) for security agents in recent years.

Challenging to scale efficiently

For all the reasons mentioned above, agent-based security is usually difficult to scale. Security should be automatic and nonintrusive; agents require manual deployment of extra software in your environments, so they fail to satisfy these criteria.

Advantages of agentless security

Agentless security solves most of the problems associated with agents.

Instead of running an agent in each of your environments, agentless services sit *outside* your resources. They collate security information by monitoring data

provided by cloud APIs and infrastructure services. This model presents several compelling advantages for security teams and administrators.

Simple, automatic coverage

Agentless platforms automatically monitor the resources in your cloud provider accounts. By connecting to cloud APIs, they can discover new resources as they're created, without requiring manual installation of an agent process. This maximizes security coverage from day one, improving the visibility of security issues.

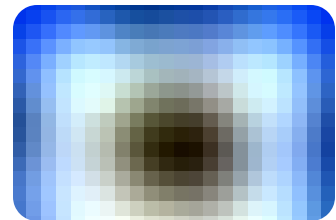
Excellent scalability

As you don't have to worry about deploying agents, agentless security is much more scalable. You can freely add, remove, and replace resources as required. There's no extra burden on administrators, whether you're monitoring 10 endpoints or 10,000.

WIZ BLOG

5 reasons endpoint security agents are not enough

[Read more](#)



No performance impact on your workloads

The absence of any agent processes running on your hosts means there's no performance impact on your workloads. At scale, small reductions in CPU utilization can have a big effect on overall resource capacity and associated costs. No processes also means no security impact.

No vendor lock-in

Eliminating agents lets you move between services more easily. Agentless is nonintrusive so you don't need to worry about cleaning up your environments after you switch. You can even use multiple services simultaneously for even better coverage or to help you trial available platforms.

Zero maintenance

Agentless security is maintenance-free. Not having to update agents lets your security teams focus on analyzing and mitigating detected threats. The platform will continually improve as the provider implements new features.

Disadvantages of agentless security

Agentless security solutions provide clear benefits over the agent-based approach, although it's not entirely without its pitfalls. Several factors could cause dissatisfaction with an agentless solution.

Requires cloud APIs

Agentless solutions can generally only monitor resources in your cloud accounts. This means they might not be as good a fit for organizations with hybrid cloud workflows that include some on-premises resources. But if you've already fully transitioned to the cloud, then agentless can match or even exceed the coverage achieved with agents. Not only does it allow you visibility into individual resources but also the bigger picture across your entire cloud.

No runtime protection

As agentless services don't run directly alongside your workloads, **they can't actively protect your hosts by making configuration changes or quarantining suspicious packages.** Despite this, agentless can still provide detailed visibility into runtime issues using a hybrid approach.

For example, [Wiz's agentless solution features eBPF sensors](#), Linux kernel modules that provide real-time monitoring of system calls, file changes, and anomalous activity within Kubernetes clusters without requiring an actual agent. This combines the best of both the agent-based and agentless models.

Summary: Agentless vs. agent-based security

Overall, agentless security is simpler, provides improved visibility, and is more scalable and maintainable than agent-based solutions. Although agents can still have advantages in specific situations, such as when you need low-level runtime protection, agentless is the option that's better suited to modern cloud operations.

The table below provides a quick reference for key factors to help you decide between the two.

Feature	Agent-based security	Agentless security
Deployment method	Agent process running on every resource	Single cloud platform
Deployment speed	Slow; requires admins to install the agent	Instant, after initial setup
Scalability	Limited; requires agent to be manually installed and maintained on every resource	Highly scalable; new cloud resources automatically discovered
Flexibility	Harder to change configuration; risk of vendor lock-in	Highly flexible to changing requirements
Effect on security	Risk that agents will be compromised	No effect on workload security (data consumed from existing APIs)
Maintenance requirements	Agents must be updated and secured	Maintenance managed by the service provider

Feature	Agent-based security	Agentless security
Best used for	Legacy on-premises and hybrid cloud services that aren't supported by agentless services	All cloud resources

WIZ ACADEMY

What is CSPM? [How CSPM Tools Work]

Read more



Wiz's approach to agentless security

Wiz's Cloud Security Posture Management (CSPM) platform is an [agentless solution](#) built for easy deployments and non-intrusive, comprehensive coverage of your servers, virtual machines, applications, and other cloud assets.

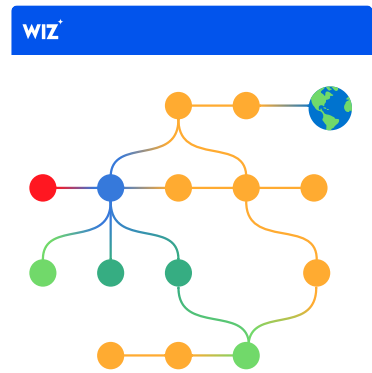
Wiz supports a flexible system of [custom rules](#) that lets you detect misconfigurations and security vulnerabilities at the cloud and host level—[no agents required](#). You can respond to all detected problems within the Wiz application, giving you a single pane of glass to control your cloud security.

Want complete, agentless security coverage for your cloud resources? [Book your Wiz demo](#) today.

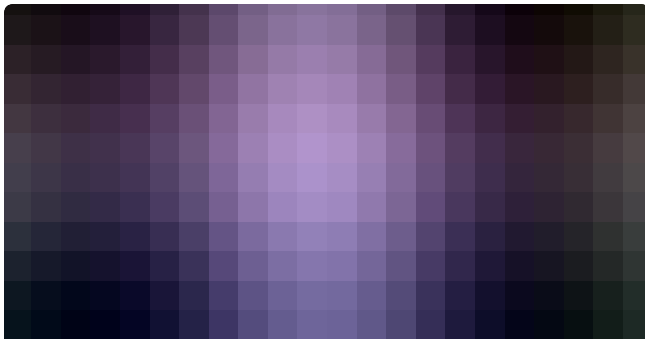
Uncover vulnerabilities in the cloud without deploying agents

See why CISOs at the fastest growing companies choose Wiz to secure their cloud environments.

 [Get a demo](#)



Continue reading

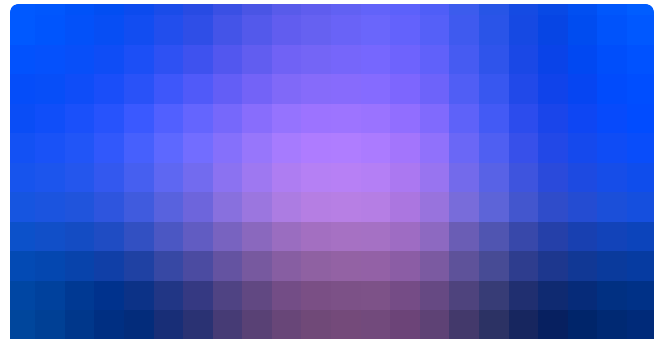


What is a Prompt Injection Attack?



Shaked Rotlevi
August 2, 2024

Prompt injection attacks are an AI security threat where an attacker manipulates the input prompt in natural language...

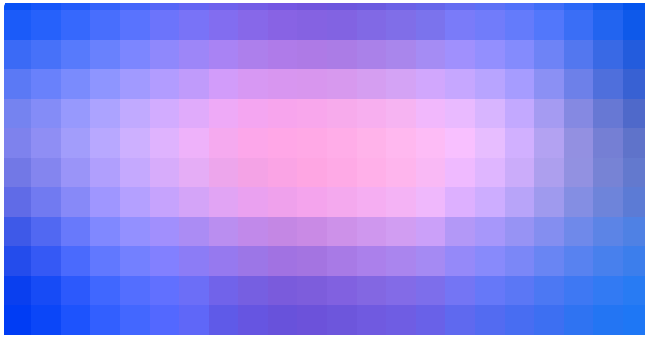


Helm Charts in Kubernetes: A security review



Nicolas Ehrman
August 1, 2024

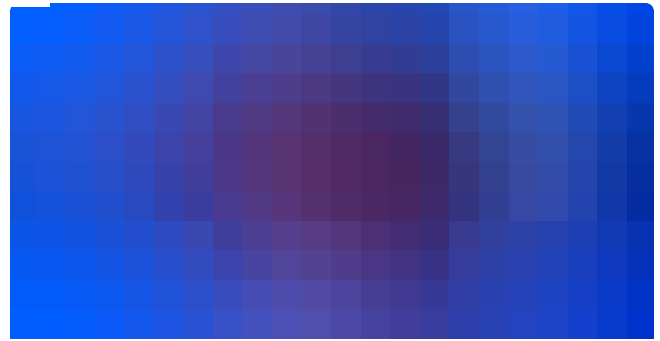
Helm Charts streamline the deployment of applications by providing a packaging format that includes all necessary...



What is Cloud Visibility? + Best Practices

Wiz Experts Team
July 31, 2024

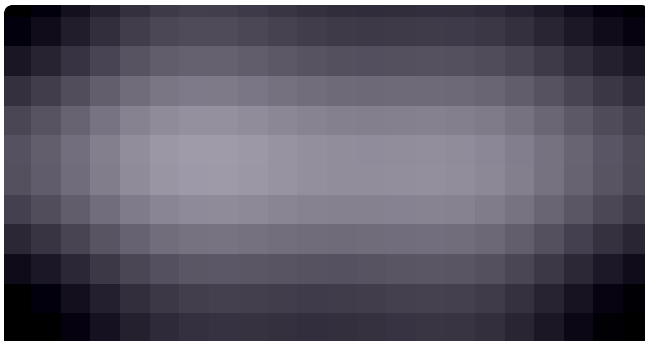
As cloud adoption grows, the only way to mitigate risks and access the full spectrum of cloud capabilities is to prioritize...



Dissecting the Steps of the Incident Response Process

Wiz Experts Team
July 26, 2024

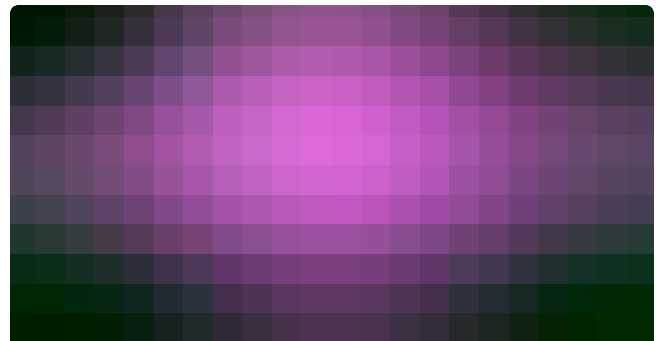
Incident response is a critical aspect of enterprise cybersecurity that involves identifying and responding to...



Unpacking the Security Operations Center (SOC)

Wiz Experts Team
July 23, 2024

Security operations centers (SOCs) are centralized facilities and functions within an enterprise's IT ecosystem that monitor...



What is a Container Engine?



Nicolas Ehrman
July 20, 2024

A container engine is a software tool that automates the process of running applications in isolated, lightweight...

PRODUCT

CSPM

Vulnerability management

Container & Kubernetes
security

CDR

IaC scanning

CIEM

Ensure compliance

CNAPP

DSPM

CWPP

AI-SPM

Code Security

Supply Chain Security

BLOG

Blog

LEARN

Customer stories

Our partners

CloudSec academy

Cloud Risk Assessment

Documentation

COMPANY

About Wiz

Join the team

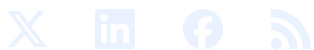
Newsroom

Events

Contact us

Trust Center

English (US)



[Status](#) [Privacy Policy](#) [Your California Privacy Rights](#) [Terms of Use](#)

[Do Not Sell or Share My Personal Information](#)

© 2024 Wiz, Inc.