

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

In this post, we're going to dive into the role and limitations of security agents in the cloud, and put forth a different approach for cloud infrastructure security: agentless deep scanning.



Josh Dreyfuss

September 28, 2021

6 minute read



Cloud environments are characterized by their dynamic nature. It's easier than ever before to spin up new resources and add new technologies, which leads to an ever-increasing number of people and teams deploying in the cloud. Ephemeral resources like serverless functions and containers mean that workloads are being added and removed at blistering speeds.

From the security perspective however, 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. The latest one is agents.

In this post, we're going to dive into the role and limitations of security agents in the cloud, and put forth a different approach for cloud infrastructure security: agentless deep scanning.

The role of agents in a cloud world

It is time to rethink the role of agents in the cloud. While they still play an important purpose in

Orca Security Ltd.
Exhibit 2138
Wiz v. Orca
IPR2024-01109, -01190, -01191
Ex. 2138-001

in this post, we're going to dive into the role and limitations of security agents in the cloud, and put forth a different approach for cloud infrastructure security: agentless deep scanning.

The role of agents in a cloud world

It is time to rethink the role of agents in the cloud. While they still play an important purpose in a cloud world, agents are best served as a last line of defense for threat protection and EDR.

There are multiple limitations and challenges for security teams when it comes to using agents in cloud environments that make them ill-suited for security usage beyond runtime and EDR however. Agents are not the best option for visibility, or risk and compliance assessment. Let's take a look at why that is.

Incomplete coverage

One of the largest challenges for securing the cloud with agent-based solutions is coverage. Agents only work on machines they're deployed on, and it's difficult for security teams to get those agents implemented across the cloud environment. DevOps teams are the ones that need to actually deploy the agents across resources, and with ownership spread across many teams, security teams face a monumental task both in getting visibility into every resource in the cloud so they know where they need to put the agents, and in getting the right developer across teams to actually install their agent. This creates a situation where security teams aren't even aware of what they're not covering.

Finding the right owner only matters for resources you can install agents on at all. There are several types of resources that agents aren't able to handle, such as ephemeral resources that only exist for a few minutes, or marketplace images that cannot be modified. Additionally, agents aren't able to scan machines that are stopped or paused, leading to gaps in coverage.

With these challenges, it is extremely common for organizations to end up with less than 50% of their cloud environment covered by agents. This makes agents better suited to serve a role as an additional layer of defense for the most critical resources, rather than attempting to cover the entire cloud with them.

Difficult to maintain and manage

Once an agent is installed, that's not the end of the story. Agents need to be maintained and managed just like any other piece of software. Agents evolve, and each new version of the agent has to be tested and validated before it's rolled out to the environment, which adds strain on security and DevOps teams.

On the flip side, cloud resources also evolve, so security teams must make sure that the agents they have out there support the latest kernel updates. The risk here is the potential to crash a resource or application if there's misalignment, or for the agent to become a security risk itself if it is not patched. Some vendors have **built-in protections** to ensure that an agent won't crash a resource if it doesn't recognize the kernel, but even if using an agent with such functionality, the capabilities of the tool will be reduced.

if it is not patched. Some vendors have **built-in protections** to ensure that an agent won't crash a resource if it doesn't recognize the kernel, but even if using an agent with such functionality, the capabilities of the tool will be reduced.

Keeping agents updated and staying on top of the impact of resource changes on agents is a full time juggling job for security teams, and one where it's easy for a ball to drop and impact cloud security posture.

Impacts the cloud environment

Finding the owner of a resource is a challenge, but on top of that, even when security teams identify the right owner, often times there's internal resistance to adding additional agents for security purposes. This is because agents have an impact on the cloud environment.

Each agent consumes computing resources, which impacts the performance of cloud workloads. There are costs to compute and memory with every agent, and they add up. As more agents are added, workloads become more expensive and less performant.

Beyond the resource impact, there is a more pernicious potential impact to adding agents: introducing new security risks. **OMIGOD was a reminder** that agents, even from reputable companies, can be installed with high privileges and come with vulnerabilities ranging from Local Privilege Escalation (LPE) to unauthenticated Remote Code Execution (RCE).

Table of contents

The role of agents in a cloud world

Incomplete coverage

Difficult to maintain and manage

Impacts the cloud environment

The rise of cloud-native approaches: agentless deep scanning

It's time to move beyond agents in cloud security

New checklist:

How to Identify and Remediate OMIGOD

Get step-by-step guidance on how to identify and remediate OMIGOD, the new Azure OMI vulnerability

Download now

OMIGOD Identification and Remediation Checklist

WIZ

The rise of cloud-native approaches: agentless deep scanning

The cloud has opened up new approaches for security leveraging the specific technologies and benefits of the cloud. One such approach is called "agentless deep scanning." Agentless deep scanning is a cloud-native way of scanning workloads. It works by leveraging Cloud API connections to take in all the relevant security data about workloads. Because of the availability of Cloud APIs and the visibility they open up, it is now possible to get full stack visibility in the cloud without agents – something that is not possible on-prem. This broad

The cloud has opened up new approaches for security leveraging the specific technologies and benefits of the cloud. One such approach is called “agentless deep scanning.” Agentless deep scanning is a cloud-native way of scanning workloads. It works by leveraging Cloud API connections to take in all the relevant security data about workloads. Because of the availability of Cloud APIs and the visibility they open up, it is now possible to get full stack visibility in the cloud without agents – something that is not possible on-prem. This broad visibility in combination with the context available at the cloud-level, as opposed to the machine-level context of agents, makes it possible to identify toxic combinations of flaws that lead to actual risks. This has a range of benefits.

Full coverage across cloud providers and resources

With agentless deep scanning, security teams are able to tackle the problems of incomplete coverage. Agentless approaches only require a single connector per cloud or Kubernetes environment, and are able to capture all the important data about workloads, including ephemeral and offline resources, within those environments. No need to identify and install anything on any individual resource. Since the agentless approach leverages the cloud providers’ visibility itself, it is able to provide 100% coverage.

Rich context from the entire environment

Beyond cloud resources themselves, agentless approaches are also able to capture crucial context from the cloud environment that is necessary for identifying real risks. Important cloud metadata that goes beyond the boundaries of individual resources has a huge impact on identifying and prioritizing critical risks. For example, via the connectors, agentless approaches can capture information about identities across principals and resources to see the risks of exposed secrets, or networking information at the cloud level to identify network exposure paths for specific resources.

No impact on the environment

Agentless scans take snapshots of resources with each scan, so there are no changes made to the resources themselves, like with an agent-based approach. Any updates made to the agentless scanner will not require security teams to take maintenance actions on their resources, creating no impact on the environment.

The volume snapshot approach of agentless deep scanning ensures that there’s no impact to performance in an environment, as the connectors are only reading data via APIs and scanning out of band, not relying on the cloud environment’s compute resources to run. This allows agentless deep scanning approaches to achieve a level of comprehensiveness in terms of coverage and features that is not possible with agent-based approaches due to the tradeoff between performance and impact to the environment.

WIZ ACADEMY

Agentless vs. Agent-Based

WIZ ACADEMY

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

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.



[Read more >](#)

It's time to move beyond agents in cloud security

The cloud is too dynamic and ephemeral to keep up a strong security posture solely by relying on having agents on every resource. It's like trying to drain a river with a bucket. For each bit you do capture, so much more has raced past you. The only way forward is to find an approach that lets security teams get visibility into every resource in the ever-changing cloud -- whether they're static, ephemeral, or offline -- and doesn't impact the cloud environment, and lets agents play the role of the last line of defense on critical resources.

If they want DevOps teams to work with them, security teams cannot afford to introduce new risks or impact performance and resource utilization with their solutions. Cloud-native approaches let security teams roll out a solution quickly without onerous asks on DevOps that gives them the coverage and context across the entire cloud they need to identify and prioritize real risks. With agents in place on critical resources as a last line of defense, this lets security teams create a solid security foundation for the cloud world.



Tags [#Product](#)

Continue reading



Continue reading



5 reasons endpoint security agents are not enough

 Rotem Lipowitch
February 3, 2022

In this post, we discuss five security limitations of endpoint security agents and also explain how adding agentless solutions...



Wiz named a 2023 AWS EMEA Marketplace Partner of the Year

 Wiz Team
November 28, 2023

AWS has named Wiz a Marketplace Partner of the Year, recognizing our practice of helping customers drive innovation while...



Secret-based cloud supply-chain attacks: Case study and lessons for security teams

 Alon Schindel, Shir Tamari
December 13, 2022

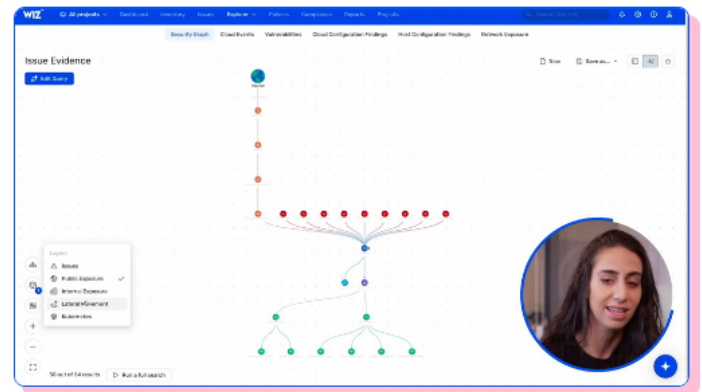
CI/CD pipelines, as an essential part of the software development process, are an attractive target to malicious actors. Based...

[GET A PERSONALIZED DEMO](#)

Ready to see Wiz in action?

“Wiz provides a single pane of glass to see what is going on in our cloud environments.”

 Adam Fletcher
Chief Security Officer



[Get a demo >](#)



PLATFORM

Wiz CNAPP

LEARN

Customer stories

COMPANY

About Wiz

Ready to see Wiz in action?

“Wiz provides a single pane of glass to see what is going on in our cloud environments.”

Blackstone

Adam Fletcher
Chief Security Officer



Get a demo >



PLATFORM

- Wiz CNAPP
- Wiz Code
- Wiz Cloud
- Wiz Defend
- Integrations
- Environments
- Documentation

LEARN

- Customer stories
- Train Your Team For Cloud
- Blog
- CloudSec Academy
- Resources Center
- Cloud threat landscape
- Cloud Security Assessment

COMPANY

- About Wiz
- Join the team
- Newsroom
- Events
- Contact us
- Trust Center
- Our partners

 English (US) ▾

