

Security Agents Don't Belong In Your Cloud!

Published 08/18/2021

[Home](#) > [Industry Insights](#) > Security Agents Don't Belong In Your Cloud!

This blog was originally published by [Blue Hexagon](#) [here](#).

Written by [Saumitra Das](#), [Blue Hexagon](#).

COVID-19 has significantly accelerated migration to the cloud as organizations enable an increasingly remote workforce and adopt cloud-native services to serve increasingly online customers. Unfortunately, cyber attackers are also now increasingly targeting cloud infrastructure and even using remote worker device infections to laterally intrude into the enterprise cloud deployments.



Securing cloud real estate has become paramount specifically given the unique attack surface that the cloud presents. The software-defined nature and agile code release practices in the cloud make it:

- *Easier* to misconfigure and expose a wider attack surface
- *Harder* for security teams to keep tabs on constantly ephemeral cloud

Traditional approaches used for on-premises, like security agents, have significant limitations in the cloud. However, a new “agent-less” approach to cloud security has recently become possible due to cloud-native APIs now available from CSPs. This approach provides security in a fundamentally different way – taking advantage of the unique characteristics of the cloud while being best suited to the dynamic nature of the cloud.

This new agentless approach to cloud security uses cloud-native patterns such as:

- **Event triggers** (e.g. *AWS Cloudwatch*) to maintain security inspection as assets change over time
- **APIs** to enable or disable services and settings, notifications (e.g. *AWS SNS*) to enable remediation
- **Traffic mirroring** (e.g. *AWS Traffic Mirroring*, *GCP Packet Mirroring*, *Azure vTAP*) to get access to any network packet, in any region, from any host or service, programmatically.

A key defining characteristic of such an approach to cloud security is that security teams now do not need to tightly couple or interface with the typically much larger Developer and DevOps teams, to instantiate and maintain security posture. For example, they do not have to mandate the use of a third-party agent to go into every workload or developer VM and make sure the right version is always present, correctly configured, and updated after a workload is in production.

A security team should be able to deploy an agentless security solution with zero downtime or changes to existing or future workloads.

There are six key benefits of an agentless approach to security versus agents as further described in the rest of this blog post.

Zero Supply Chain Attacks



Latest from CSA



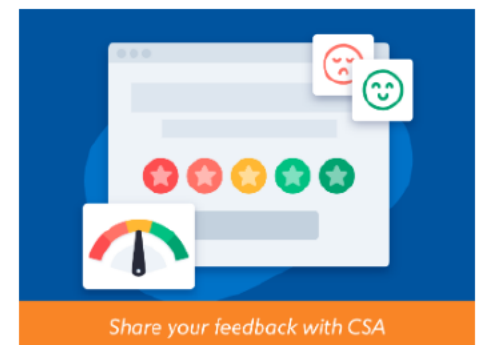
Help Shape the Next Top Threats Deep Dive



Participate in the Open Peer Review for Data Privacy Engineering



Explore Shadow Access and AI



Share your feedback with CSA



Orca Security Ltd.
Exhibit 2103
Wiz v. Orca
IPR2024-01109, -01190, -01191
Ex. 2103-001

A security team should be able to deploy an agentless security solution with zero downtime or changes to existing or future workloads.

There are six key benefits of an agentless approach to security versus agents as further described in the rest of this blog post.

Zero Supply Chain Attacks

The Solarwinds attack showed us how running privileged code from a third party can lead to attacks even in sophisticated organizations. Running third-party security agents that typically have high privilege rights alongside workloads, which have your IP and data, increases security risk dramatically. Using agents involves the risk of exposing your workloads and infrastructure to code that is being developed somewhere else without your visibility or control into their security posture. In contrast, an agentless solution can be completely isolated from your workloads and indeed even sequestered into its own virtual network or even account/project so that no lateral movement from the security solution is possible. This is a superior approach that eliminates the risk of supply chain attack to zero.

Zero Privilege Escalation and Tampering

In addition to the supply chain risk, agents have been known to have unpatched vulnerabilities themselves (Example 1, Example 2, Example 3) which could then be exploited by a threat actor and lead to privilege escalation. In the Solarwinds attack, agents were often tampered with and disabled in a very targeted way (<https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039a>). In contrast, cloud-native infrastructure mechanisms such as AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTAP cannot be disabled by an attacker in userspace or used to escalate privilege.

Zero Performance Impact

Agentless solutions have zero performance impact upon the systems they are inspecting, period! Agent-based solutions require additional configuration efforts to make sure memory and CPU resources are not affecting the workload performance itself.

Zero Downtime and Maintenance

Agentless solutions do not require any downtime on customer workloads for instantiation. They also do not require manual intervention for maintenance and updates because they operate from the outside. Agents need constant care and upkeep to keep up with vulnerabilities, OS platform changes, performance issues, version updates and much more. This requires the cloud operations or security teams to have to then go and update the agents on all the workloads in production.

Zero Darkspace In Cloud Real Estate

Customers tell me that agent-based approaches are only able to cover up to 50% of the cloud real estate even after several months of deployment. There are five fundamental reasons for this lack of visibility and consequently lack of security inspection:

- Deploying agents require disruptive changes to existing workloads which take time and in some cases may never happen
- Maintaining and updating agents is a time-consuming effort for multiple stakeholders
- Managed cloud-native services (Databases, Elasticsearch, Analytics) and serverless computing are increasingly being adopted and do not allow for agent installation
- Agents frequently have issues with running on different operating systems or different versions of a given operating system
- Third-party appliances are frequently deployed as black-boxes inside cloud infrastructure and they cannot have security agents installed on them to monitor behavior

Indeed, many agent-based security deployments have failed to secure the enterprise cloud instances, resulting in costly data breach and business disruption.

~Zero Friction between SecOps and Dev/DevOps

Deploying agents requires security teams to coordinate and make sure all containers and VMs – across all operating systems, in all regions, in all accounts and availability zones – are running the required



resulting in costly data breach and business disruption.

~Zero Friction between SecOps and Dev/DevOps

Deploying agents requires security teams to coordinate and make sure all containers and VMs – across all operating systems, in all regions, in all accounts and availability zones – are running the required security agents. This requires onerous continuous coordination between security teams and Dev/DevOps for whom agility in code release and time-to-deployment is the primary concern. To exacerbate this issue, security teams are outnumbered by multiple orders of magnitude by developers and DevOps personnel. Finally, as agents need to be updated or new workloads are created, this requires continuous coordination effort, and lead to potential gaps and delays.

Read other interesting blogs by Blue Hexagon at <https://bluehexagon.ai/blog/>.

DevSecOps

Enhancing cloud security strategy

Transitioning to the cloud



Share this content on your favorite social network today!

Level up with Cloud Infrastructure Security Training



Related Articles:



A.I in Cybersecurity: Revolutionizing Threat Detection and Response

Published: 03/14/2025



AI Agents: Human or Non-Human?

Published: 03/13/2025



Why Unified Data Security is Essential for Modern Enterprises

Published: 03/11/2025



Are You Asking the Right Questions About AI?

Published: 03/07/2025



© 2009–2025 Cloud Security Alliance.
All rights reserved.

Corporate Membership

Cloud Customers
Cloud Solution Providers

Join as an Individual

Circle Community Forum
Chapters
Working Groups

Research

Download Publications
View Working Groups
View All Topics

Find a...

Cloud Consultant
Cloud Service Provider
Trusted Cloud Provider

Certificates

CCSK
CCAK
CCZT

Events

Americas
EMEA
APAC

Education

Blog
Virtual Events & Webinars
Training
Cloud 101

Popular Resources

Security Guidance
CCM
CAIQ

About CSA

Contact Us
Press Releases
Affiliates
Press Coverage
Quality Policy

Our Team

Board of Directors
Management & Staff
Careers

Legal

Privacy Notice
Terms & Conditions

Cloud Security Glossary

exacerbate this issue, security teams are outnumbered by multiple orders of magnitude by developers and DevOps personnel. Finally, as agents need to be updated or new workloads are created, this requires continuous coordination effort, and lead to potential gaps and delays.

Read other interesting blogs by Blue Hexagon at <https://bluehexagon.ai/blog/>.

DevSecOps



Share this content on your favorite social network today!

Enhancing cloud security strategy

Transitioning to the cloud

Level up with Cloud Infrastructure Security Training



Related Articles:



A.I in Cybersecurity: Revolutionizing Threat Detection and Response

Published: 03/14/2025



AI Agents: Human or Non-Human?

Published: 03/13/2025



Why Unified Data Security is Essential for Modern Enterprises

Published: 03/11/2025



Are You Asking the Right Questions About AI?

Published: 03/07/2025



© 2009-2025 Cloud Security Alliance.
All rights reserved.

Corporate Membership

Cloud Customers
Cloud Solution Providers

Join as an Individual

Circle Community Forum
Chapters
Working Groups

Research

Download Publications
View Working Groups
View All Topics

Find a...

Cloud Consultant
Cloud Service Provider
Trusted Cloud Provider

Certificates

CCSK
CCAK
CCZT

Events

Americas
EMEA
APAC

Education

Blog
Virtual Events & Webinars
Training
Cloud 101

Popular Resources

Security Guidance
CCM
CAIQ
STAR
GDPR

About CSA

Contact Us
Press Releases
Affiliates
Press Coverage
Quality Policy

Our Team

Board of Directors
Management & Staff
Careers

Legal

Privacy Notice
Terms & Conditions

Cloud Security Glossary



Support