

How Agentless Approaches Sideline Cloud Workload Protection Strategies

Cloud Workload Protection



By **Keith Mokris**
February 23, 2021 at 12:00 PM
6 min. read



Unified security, especially for new architectures, is a concern among practitioners.

With cloud native architectures on the rise, including an 84% increase in container adoption over the last year, securing these new technologies is a top concern. At Prisma Cloud, we work with some of the most innovative companies in the world to secure cloud native workloads spanning hosts, containers and serverless functions. Against our track record of accurately assessing future cloud security needs, we wanted to show why over 1800 customers believe our architecture offers the most comprehensive and ideal approach for securing cloud workloads at scale.

Cloud Native Security

Unlike more traditional application delivery mechanisms, cloud native application architectures are dominated by two trends:

1. Immutable infrastructure practices where provisioning of servers, applications and networks is fixed and repeatable, so that the process does not suffer from incremental software upgrades, inconsistent deployments or human errors.
2. The use of microservices and ephemeral workloads that address the needs for auto-scaling, but result in a continuously changing application footprint.

Addressing security in these environments requires an approach focused on applying controls as early as possible in the application lifecycle, coupled with detailed monitoring and protection at runtime that can adapt to the rapidly changing nature of applications.

Agentless Solutions Fall Short: Common Scenarios

Recently, new agentless or “side-scanning” solutions have emerged claiming to provide a lightweight design that delivers security for cloud native workloads. Unfortunately, this lightweight architecture only delivers rudimentary security capabilities, mostly useful for compliance. These solutions fail to take advantage of immutable infrastructure principles and only offer a “point-in-time” view, or “snapshot” of what’s running at any given time. They cannot capture the dynamic evolution of workloads or provide runtime attack prevention and policy enforcement. Here we present a few scenarios that demonstrate this shortcoming.

Scenario 1: Real-Time, Continuous Vulnerability Management and Compliance

Agentless solutions are engineered to provide basic visibility into vulnerabilities and misconfigurations based on scanning from the outside-in. While this may provide some level of insight, they are not continuous, real-time solutions.

For example, in container environments, at least 50% of containers have a lifespan of less than 5 minutes. This frequent change is due to the high-release velocity of today’s DevOps teams – especially with containerized and Kubernetes environments. An agentless approach that only takes a snapshot of the infrastructure every 30 minutes will miss most runtime activity of these workloads (or about 50% of the operations). It is thus insufficient for validating and measuring the security posture of cloud

Document title: How Agentless Approaches Sideline Cloud Workload Protection Strategies

Capture URL: <https://web.archive.org/web/20210727053930/https://www.paloaltonetworks.com/blog/prisma-cloud/agentless-approaches-sideline-cloud-workload-...>

Capture timestamp (UTC): Wed, 19 Mar 2025 12:08:36 GMT

Estimated post date: 07/27/2021 5:39:30 AM

Page 1 of 4

Orca Security Ltd.
Exhibit 2106
Wiz v. Orca
IPR2024-01109, -01190, -01191
Ex. 2106-001

infrastructure. This frequent change leads to the high release velocity of today's DevOps teams – especially with containerized and Kubernetes environments. An agentless approach that only takes a snapshot of the infrastructure every 30 minutes will miss most runtime activity of these workloads (or about 50% of the operations). It is thus insufficient for validating and measuring the security posture of cloud native systems. Additionally, agentless solutions lack the ability to prevent misconfigurations or enforce vulnerability and compliance policies that arise in these changes.

Scenario 2: Continuous Integration and Continuous Delivery Security

Since immutable infrastructure techniques are the main way to manage cloud native application delivery, integrating security with the continuous integration (CI) and continuous delivery (CD) workflow is a core requirement. DevOps and security teams need to see real-time vulnerability results in both native tooling and centralized dashboards before deployments are made.

Agentless solutions currently do not provide visibility or enforcement for DevOps teams during CI/CD phases. Security issues discovered after deployment cannot be correlated to the application definitions that created them in the first place. Today, many organizations have hundreds or thousands of such container images stored in one or several container registries – agentless solutions would be unable to provide continuous visibility or control over them.

Scenario 3: Runtime Protection

To secure cloud native applications, organizations need to deliver scalable security across file system, process and network activity; enforce runtime policy; surface real-time audit data; and capture forensic data for analysis.

Agentless solutions fail to deliver visibility and protection for these activities, or collect data for forensic analysis. If an attacker were able to get a foothold on a workload or container, these solutions would be unable to prevent new processes, unwanted file system activity or lateral movement. If malware or remote code execution were leveraged in an attack, agentless solutions would be unable to provide prevention. The same is true of their inability to stop attacks where an actor opens or closes a port, where web application firewall capabilities would be required for full stack security.

Cloud Native Workload Protection: Prisma Cloud Architecture

The Prisma Cloud platform has been designed to meet the cloud native security requirements described above. Prisma Cloud combines a strong “Shift Left” security paradigm that includes Infrastructure-as-Code and image container analysis, which prevents security vulnerabilities from being deployed in the first phase, with a robust runtime monitoring and protection mechanism that captures the exact behavior of constantly changing applications.

Our runtime capabilities span both cloud deployment and configuration as well as runtime workload protection. Runtime security is addressed head-on by a unified agent framework that protects the most popular cloud VMs / hosts, containerized or Kubernetes applications and serverless applications.

Illustrating our unified agent framework

Prisma Cloud Defender, our agent, supports all the leading cloud native workload and application architecture used by organizations today. For example, common Defender deployments include a container agent, Kubernetes DaemonSet or even app-embedded Defender to protect your application anywhere it is deployed. Whether you're protecting a Linux VM, a Kubernetes application on Red Hat OpenShift, a containerized application on AWS Fargate or a serverless function on AWS Lambda, Defender can be deployed to protect the application at runtime.

Defender also provides powerful, integrated Web Application and API Security capabilities without any additional deployment efforts – delivering defense-in-depth that no other solution on the market can match.

Additionally, Defender delivers full lifecycle vulnerability and compliance management into CI/CD workflows and container registries. Prisma Cloud is able to enforce policies to prevent an AMI, container image or function from being built and deployed.

Conclusion

Security teams need to deliver full stack security at the incredible scale of cloud native architectures. Simultaneously, they can't accept trade offs from their security solutions. With Prisma Cloud, we're securing some of the largest cloud native deployments in the world, ensuring every workload is protected both at runtime and across the application lifecycle.

To learn more about the requirements for cloud workload protection, [download the Gartner Market Guide for Cloud Workload Protection Platforms](#).

Get updates!

Sign up to receive the latest news

Enter your email



By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).

Popular Resources

[Blog](#)

[Careers](#)

[Communities](#)

[Content Library](#)

[Cyberpedia](#)

[Event Center](#)

[Investors](#)

Legal Notices

[Privacy](#)

[Trust Center](#)

[Terms of Use](#)

[Documents](#)

Account

[Manage Subscriptions](#)

[Report a Vulnerability](#)



Prisma Cloud Defender, our agent, supports all the leading cloud native workload and application architecture used by organizations today. For example, common Defender deployments include a container agent, Kubernetes DaemonSet or even app-embedded Defender to protect your application anywhere it is deployed. Whether you're protecting a Linux VM, a Kubernetes application on Red Hat OpenShift, a containerized application on AWS Fargate or a serverless function on AWS Lambda, Defender can be deployed to protect the application at runtime.

Defender also provides powerful, integrated Web Application and API Security capabilities without any additional deployment efforts – delivering defense-in-depth that no other solution on the market can match.

Additionally, Defender delivers full lifecycle vulnerability and compliance management into CI/CD workflows and container registries. Prisma Cloud is able to enforce policies to prevent an AML, container image or function from being built and deployed.

Conclusion

Security teams need to deliver full stack security at the incredible scale of cloud native architectures. Simultaneously, they can't accept trade offs from their security solutions. With Prisma Cloud, we're securing some of the largest cloud native deployments in the world, ensuring every workload is protected both at runtime and across the application lifecycle.

To learn more about the requirements for cloud workload protection, [download the Gartner Market Guide for Cloud Workload Protection Platforms](#).

Get updates!

Sign up to receive the latest news

Enter your email



By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).

Popular Resources

[Blog](#)

[Careers](#)

[Communities](#)

[Content Library](#)

[Cyberpedia](#)

[Event Center](#)

[Investors](#)

[Tech Docs](#)

[Unit 42](#)

[Sitemap](#)

Legal Notices

[Privacy](#)

[Trust Center](#)

[Terms of Use](#)

[Documents](#)

Account

[Manage Subscriptions](#)

[Report a Vulnerability](#)

