Agentless Workload Posture

Frictionless, Instant, Deep Visibility

It's impossible to secure something that's out of sight and out of the security team's control, which is event more complex in today's cloud environment. Instead of relying on the DevOps team to deploy agents for in order to gain visibility into the cloud environment and security posture of workload assets, take advantage of new agentless models. Check Point CloudGuard can allow you to gain deep visibility through agentless deployments to understand what is happening within your cloud workloads without impacting performance, as well as complete visibility into OS security configuration issues, leaked credentials, malware on workloads, and more with continuous scanning.

Deep Workload Visibility With No Agents

It's time for security professionals to regain control of their cloud environments and CloudGuard offers exactly this with Agentless Workload Posture (AWP). AWP extends CloudGuard's agentless infrastructure visibility into workloads — scanning and identifying risks including misconfigurations, malware detection, vulnerabilities and secrets across all cloud workloads including Virtual Machines, Containers and Serverless Functions.

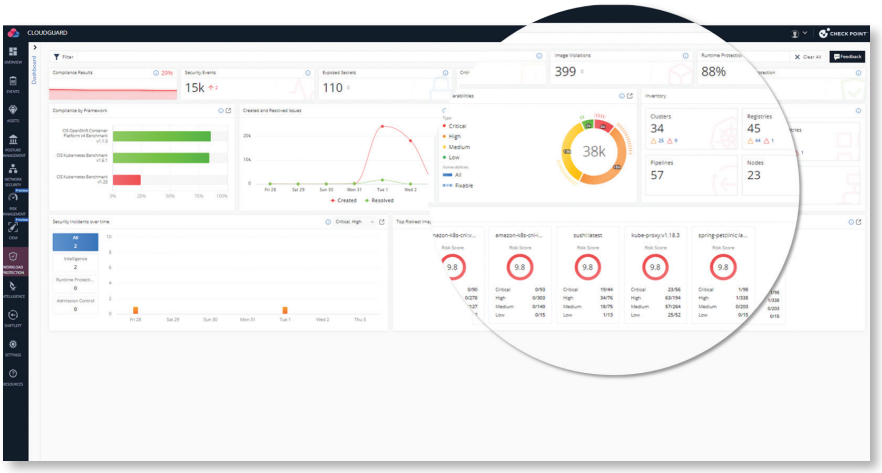
Check Point CloudGuard Provides Deep Visibility Into Cloud Workloads

With CloudGuard you can achieve instant visibility into running workloads including vulnerabilities, malware and exposed secrets. Since CloudGuard has an agentless model, you can maintain security posture quickly without impacting workload performance.

CloudGuard AWP technology provides:

- Immediate and low-cost visibility into workloads including VMs, Containers, and Functions at scale
- Detect & alert on risks such as misconfigurations, malware, vulnerabilities and secrets
- AWP findings feed into CloudGuard's contextual risk engine (ERM) and XDR platforms

AWP is seamlessly integrated into CloudGuard and provides deep insights with no performance impact on the live workloads, and without the need for DevOps teams to deploy agents. By eliminating the need for agents, security teams can get their cloud security up and running within a matter of hours.



Activate agentless security quickly and gain deep visibility into vulnerability information, secret and malware impacting security posture in the runtime environment — dive deep into the threat details and effective remediation.

Unified Security, Built to Reduce Risk in the Cloud

The AWP capabilities are part of the unified cloud native security tools provided in CloudGuard. Check Point understands that unification is a means to an end which is why our AWP feeds into the Effective Risk Management engine, which combines all of the outputs from the posture management, vulnerability & malware scanning and CIEM, to provide each risk with a score based on the business' architecture and priorities. CloudGuard then produces business-centric risk remediation prioritization for security teams, to ensure security optimization.

More Context, Actionable Security, Smarter Prevention

From **code to cloud**, Check Point CloudGuard delivers **automated** cloud native security, unified across your applications, workloads, and network to **manage risk, maintain posture, and prevent threats**, in context, at cloud speed and scale. CloudGuards prevention-first approach protects applications and workloads throughout the software development lifecyle, and includes an effective risk management engine, with automated remediation prioritization, to allow users to focus on the security risks that matter.
For more information on CloudGuard, visit **www.checkpoint.com/cloudguard**

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com