CloudGuard Cloud Detection & Response

Intrusion Detection, Threat Hunting & Remediation

Successfully protecting against threats in the cloud requires behind-the-back vision and around-the-clock adaptability. Most organizations are relying on traditional SIEM solutions and analytics tools to understand their cloud activities. This method provides limited visibility and lacks security context.

Threats in the cloud range from data exfiltration to resource hijacking, denial of service and more. Often, these breaches are not discovered until after they occur, leaving security teams to manually search through logs to understand the impact and remediate. Streamlined data analysis, contextual visualization and threat intelligence is the only way to proactively address potential vulnerabilities and stop attacks in progress.

Invest in a Fully Integrated & Unified Solution

CloudGuard Cloud Detection and Response (CDR) works in harmony with CloudGuard CNAPP, achieving a deeper layer of security and insight with intrusion detection, threat hunting, and remediation. CloudGuard CDR provides SecOps and SOC teams with the necessary context, correlating information from cloud inventory and configuration, account activity, network traffic logs and additional threat feeds, such as Check Point ThreatCloud, IP reputation and geo databases to portray one complete and accurate picture.

USE CASES

- Automatically alert and remediate public cloud threats
- Reduce breach detection time
- Streamline network security operations
- Expedite incident investigation process
- Identify anomalous user behavior and network traffic by leveraging machine learning

KEY PRODUCT BENEFITS

- Integrates with Amazon AWS, Microsoft Azure, Google GCP, Alibaba Cloud and Kubernetes.
- Robust enrichment engine to make sense of cloud logs and minimize false positives
- Context-rich intuitive visualization and natural language querying
- Threat Cloud integration, world's largest IOC database
- Intrusion Detection automatic alerts
- CloudBots integration for automatic remediation

Automate Intrusion Detection & Threat Hunting

Anomaly Detection
Prevent security breaches and unauthorized activity before any vulnerabilities can be exploited. Leveraging AI and UEBA, CloudGuard continuously analyzes account activity and monitors network traffic for signs of anomalies and cyber threats.

Pre-Built Rules & Automated Alerts
Receive automatic alerts on rule infringement. Pre-built rules are comprised of industry best practices, in-depth cybersecurity research, MITRE ATT&CK framework and more. Using the GSL builder, customers can also define their own rules to monitor specific events, allowing for advanced customization and flexibility.

Gain Visibility & Simplify Incident Investigation

Turn enriched data into actionable insights! Retrieve historical data and perform advanced incident analysis to drive data-informed decisions. CloudGuard CDR Explorer is a visual exploration tool that interprets account activity and network traffic logs, and provides rich contextualized information.

Easily Identify Unwanted Traffic—Use the Traffic Explorer to view actual traffic between assets and the internet, quickly identifying suspicious traffic patterns, such as connection with malicious IPs.

Uncover Suspicious Activity—Understand at once, who did what action on which resource to detect potential threats, such as lateral movement, using the Activity Explorer.

Correlate Events—CloudGuard provides you with the tools to take the investigation further. Choose from an extensive set of predefined queries or craft custom ones using CloudGuard's expressive yet concise query language.

Quickly Respond to Incidents & Remediate

Eliminate Alert Fatigue—CloudGuard provides the tools to filter out false positives, speed up triage, and simplify incident analysis. Check Point's world-renowned team of experts continually analyze, expand and improve alerts.

Remediate On the Spot—Automatically revert risky configuration changes with CloudBots technology. CloudBots is a serverless framework allowing customers to trigger remediation with just one click! Create custom responses to any type of network alert or audit trail, running entirely within your environment.

Manage Across Multi-Cloud Environments

Organizations can easily manage the security of their public cloud environments at any scale across Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Alibaba Cloud and Kubernetes. CloudGuard CDR connects the dots between posture management, network traffic and identity activity, minimizing the time between alerts and confirmed incidents. While CSPM has a proactive approach of reducing any risk or misconfigurations, CDR can alert you of actual security incidents happening live across the cloud infrastructure.

Integrate Findings into Your SIEM

Integrating with all leading SIEM vendors, CloudGuard CDR feeds alerts, derived from enriched log traffic, in a highly contextualized JSON format.

Check Point CloudGuard provides unified cloud native security for all your assets and workloads, giving you the confidence to automate security, prevent threats, and manage posture—everywhere—across your multi-cloud environment. CloudGuard CDR is part of Check Point's CloudGuard Cloud Native Security, which also includes Cloud Posture Management, Workload Protection and Cloud Network Security.
Try CloudGuard today!

CloudGuard
CDR

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