Check Point
SOFTWARE TECHNOLOGIES LTD

CloudGuard Intelligence

Cloud Intelligence and Threat Hunting

Insights

As companies migrate and expand their applications and services to multi-cloud environments at an unprecedented rate, despite the many benefits of multi-cloud, this also creates security problems. This is due to the fact that local deployments differ from those offered by cloud service providers such as Amazon Web Services or Microsoft Azure.

Visibility and incident investigation in multi-cloud environment is a growing challenge. Cloud forensics and investigation becomes costly and ineffective when there is too much security data to analyze; making it sometimes nearly impossible to elevate true security alerts from the irrelevant ones. The accumulation and interpretation of data collected during daily cloud operations prior to an incident play a critical role. This has a direct impact on security, as any such information may be relevant for subsequent investigations. Organizations migrating to the cloud must understand the importance of data analysis, contextual visualization and threat intelligence to protect sensitive data while preventing threats.

USE CASES

- Streamline Network Security Operations
- Reduce time of threat detection
- Detect and remediate cloud-oriented attacks and abnormal usage of cloud resources, network activities and logins
- Expedite and assist compliance validation

CloudGuard
Intelligence

KEY PRODUCT FEATURES & BENEFITS

- Easily integrate with Amazon AWS, Microsoft Azure, and Google GCP to unify your cloud native solution.
- Gain simplified visibility of the entire multi-cloud environment with our Unified Visual Exploration tool.
- Receive advanced analytics and forensics powered by ThreatCloud and machine learning.
- Enrich traffic logs with contextualized information that provides relevant alerts, quarantines threats and minimizes false positives.
- Expedite security investigation processes, detect activity anomalies and auto-remediate misconfiguration using CloudBots.
- Seamlessly integrate with SIEMs using our firehose connector in JSON format for more insights.

CloudGuard Intelligence

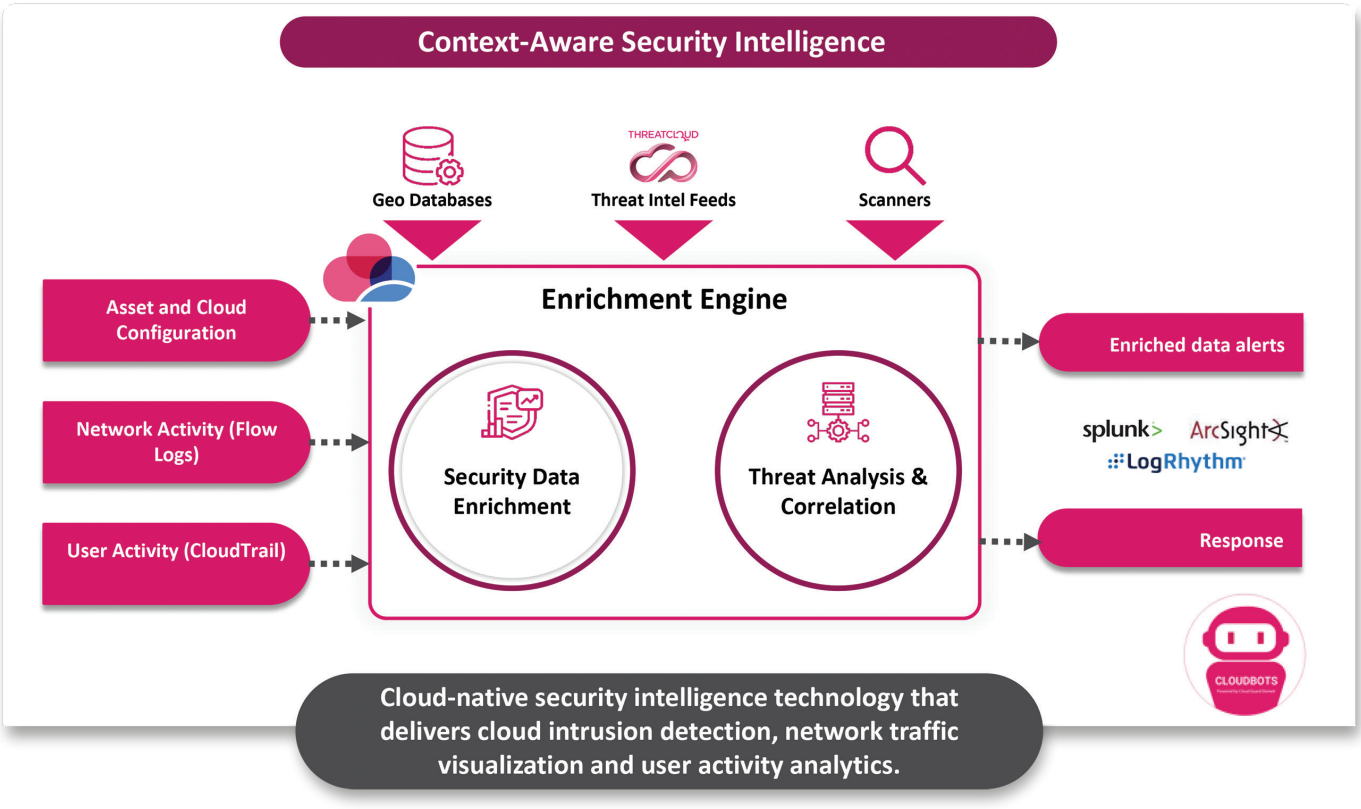
Advanced cloud security intelligence and threat hunting, delivering contextualized visualization of threats and real-time insights in multi-cloud environments for faster and more efficient incident response in multi-cloud environments.

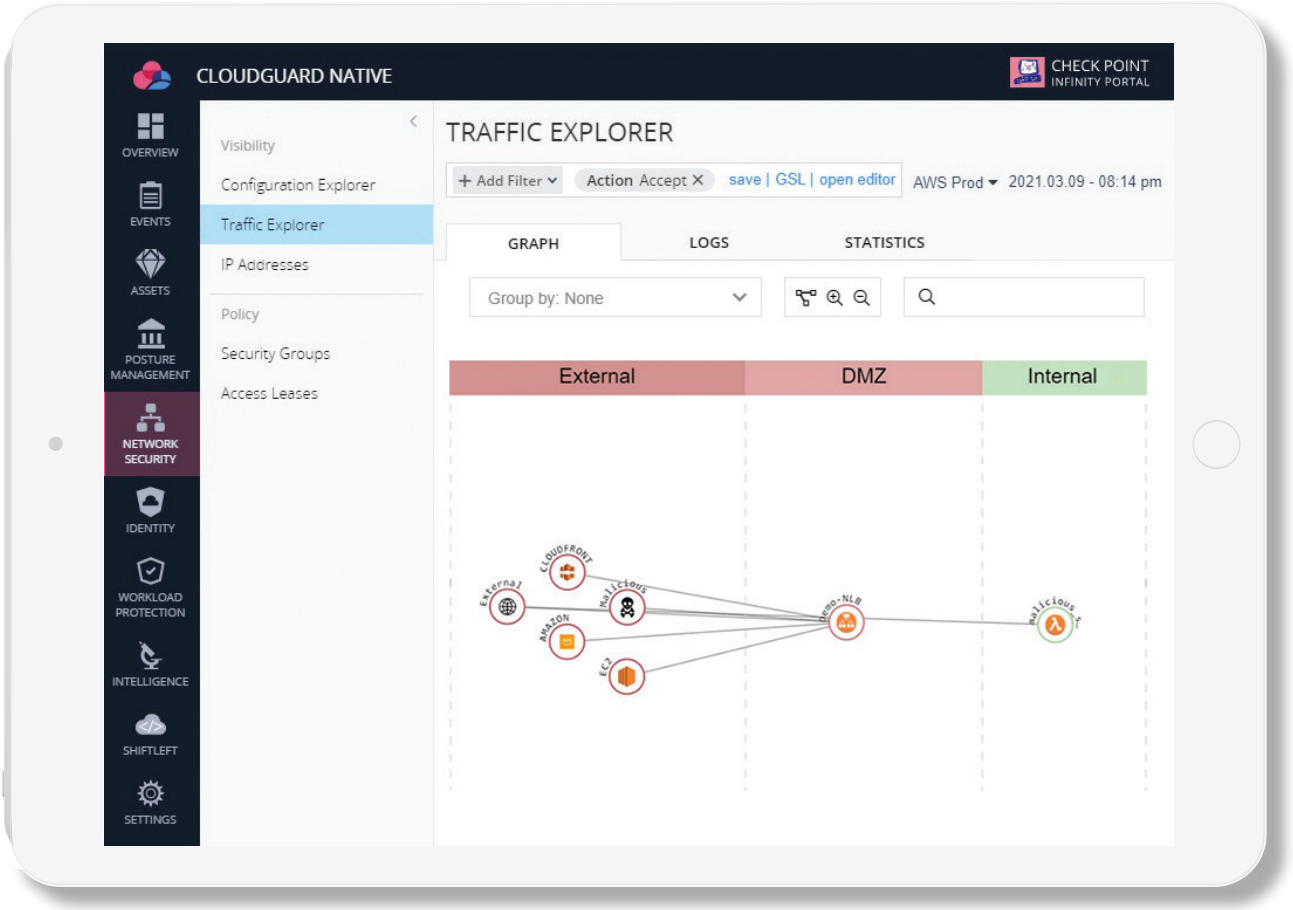
CloudGuard Intelligence is equipped with automated threat detection and traffic analysis (NTA), identifying and investigating security breaches as well as unauthorized activities. It also offers contextual and graphical visualization of network traffic and user activity. Advanced object-mapping algorithms use cloud inventory and configuration information as well as real-time monitoring data from a number of different sources across Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Kubernetes.

Transforming Logs into Security Logic

CloudGuard analyzes and enriches the cloud account's traffic metadata and logs with context, transforming them into readable security logic. Integration with the Check Point Threat Cloud allows CloudGuard to alert on a variety of suspicious connections, such as outbound and inbound traffic to malicious actors.

CloudGuard enrichment process provides enhanced investigation capabilities, for example, querying all traffic by asset type, such as EC2, Lambda. It also provides advanced analysis of unique attack techniques, network anomaly detection that alerts based on the asset's behavior, and abnormal traffic such as malformed DNS traffic.





Comprehensive Visibility and Expedite Investigation Using Big Data Analytics

CloudGuard can give near real-time views of the cloud's activity as well as the ability to investigate and analyze past activity. Real time alerts are configured for specific events or event types that occur in the cloud environment, so that the user will be aware and able to respond immediately. Utilizing the most up to date machine learning technology, CloudGuard detects new attacks and suspicious activities, such as login from abnormal locations, asset network changes, and usage of access key from an abnormal location.

CloudGuard gives the customer the ability to see every data flow and audit logs in today's elastic cloud environments. It bases its analysis on two main information pillars — account's 24/7 activity (APIs and user activities) and network connections of the environment. CloudGuard combines cloud inventory and configuration information with real-time monitoring data from a variety of sources, as well as current threat intelligence feeds, IP reputation, and geolocation databases. This results in enhanced visualization that distinguishes suspicious traffic from legitimate traffic. Intrusions detection, alerting, and investigation capabilities across AWS, Azure, GCP and Kubernetes are part of the solution.

Seamless Integration and Security Intelligence Boost to SIEM

CloudGuard Intelligence firehose connector feeds the enriched log traffic in a highly contextualized JSON format to various SIEMs, such as Splunk, ArcSight, LogRythm for further investigation. As shown in the diagram above, CloudGuard utilizes identify and perform a comprehensive investigation of security threats, enriching the logs ingested, and delivering more actionable insights into SIEM solutions.

Visit https://www.checkpoint.com/products/cloud-intelligence-threat-hunting to learn more about CloudGuard Intelligence, request a demo, and signup for a free-trial.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com