Cloud Intelligence & Threat Hunting for the Public Cloud

Product Benefits

- **Bullseye Threat Prevention**: detect cloud anomalies to remediate at once, and quarantine threats utilizing the world's largest threat intelligence feed
- **Security for all IaaS and PaaS cloud assets**: gain full visibility and security posture awareness for ephemeral assets like: AWS Lambda, NAT Gateways, load balancers, and more
- **Context-Rich Visualization**: Make sense of cloud big data with fascinating visualization, intuitive querying, intrusion alerts, and notifications on policy violations

Use Cases

- Alert & quarantine public cloud threats
- Expedite security investigation processes
- Enrich 3rd party SIEM solutions with critical data on ephemeral assets and security postures

Product Features

- Robust logs enrichment engine
- Cloud intrusion alerts
- Visual exploration tool
- Firehose connector into 3rd party SIEM
- Threat Cloud and CloudBots integration
- A turnkey solution that integrates with your cloud infrastructures

CLOUD SECURITY DOES NOT ALWAYS MAKE SENSE

Gartner projects that in 2019 the worldwide public cloud services market will grow by 17.5 percent, to a total of $214.3 billion.

With the shift to the cloud, businesses are also shifting their responsibility; relying on traditional SIEM solutions and analytics tools to understand their cloud activities. But analyzing cloud big data is no easy task, and existing solutions provide only limited visibility and no context to shed light on malicious cloud activity.

It's time to put cloud security in context.

TRANSFORMING LOGS INTO SECURITY LOGIC

CloudGuard provides cloud-native threat protection and security intelligence for the public cloud. CloudGuard enriches cloud logs with context, transforms them into readable security logic, and enables security teams to take cloud security to the next level.

Using CloudGuard businesses can:

- See every data flow and audit trail in today's elastic cloud environments
- Make sense of cloud data and activities to expedite investigation processes

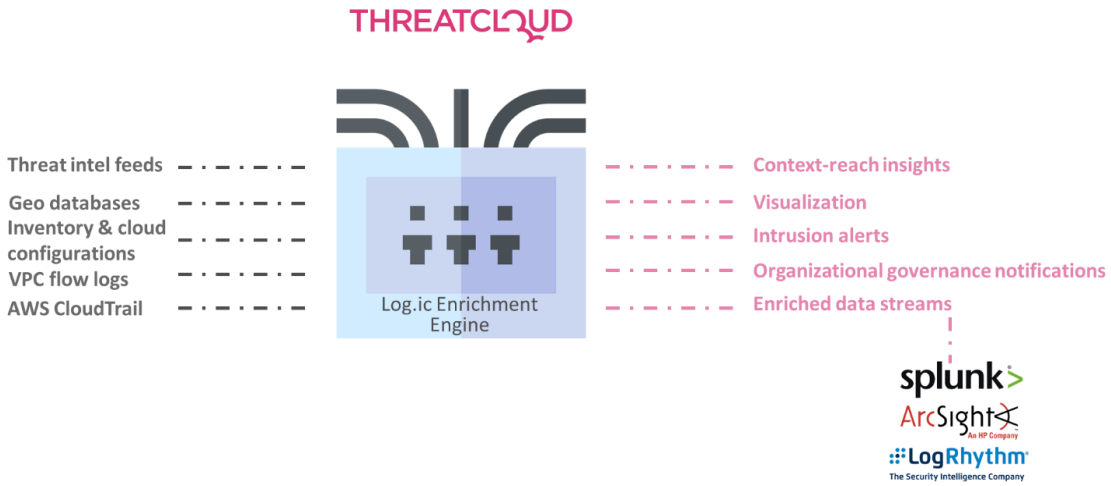
CLOUD SECURITY WILL NEVER LOOK THE SAME

CloudGuard delivers cloud intrusion detection, network traffic visualization and user activity analytics. Its object-mapping algorithms combine cloud inventory and configuration information with real-time monitoring data from a variety of sources including VPC Flow Logs, CloudTrail, Amazon GuardDuty, AWS Inspector, as well as Check Point's Threat Cloud feeds, IP reputation and geo databases.

The outcome is rich contextualized information that is used within the CloudGuard platform for enhanced visualization, querying, intrusion alerts and notifications of policy violations. It can also be piped to third-party SIEM solutions, anywhere.

With robust threat detection at core, CloudGuard CloudBots technology also extends remediation capabilities indefinitely – allowing you to create custom response to any type of network alert, audit trail, or any other.

CloudGuard is the only platform that attributes network traffic to cloud-native ephemeral services such as Amazon Lambda functions as well as other cloud-native platform components (RDS, Redshift, ELB, ALB, ECS) to provide a complete view and understanding of your cloud infrastructure across time.



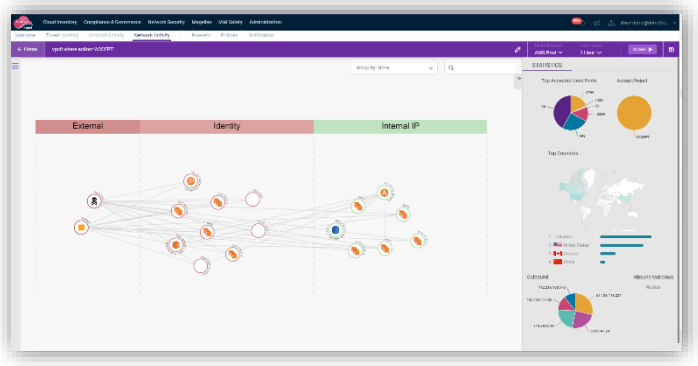
DETECT AND PREVENT CLOUD ANOMALIES USING AI, ALERT AND QUARANTINE THREATS WITH CHECK POINT'S THREAT CLOUD

CloudGuard for Cloud Intelligence and Threat Hunting uses security best practices of signature detection, built-in rules, threat intelligence feeds and existing traffic flow to create a baseline of your network and user activity. It also uses AI and anomaly detection algorithms to spot potentially unauthorized or malicious activity within your cloud environments, including serverless applications. CloudGuard can provide real-time policy violation and intrusion detection alerts based on user-defined criteria to the security admin team.

- **Feeding off of the world's largest IOC database**: CloudGuard leverages Check Point's ThreatCloud to enrich logs with intelligence from various feeds, including:
  - 750M+ malicious hashes, sites and C&C addresses
  - 11M behavioral signatures
  - 2.5M daily detections
  - Dozens of external feeds
- **Auto-remediation with CloudBots**: CloudBots is a serverless framework that triggers a remediation function with a single click deployment, running entirely within your environment. Add CloudBots to create custom response to any type of network alert, audit trail, or other, and remediate threats at once with CloudGuard.

EXPEDITE INVESTIGATION PROCESSES WITH BIG DATA ANALYTICS

CloudGuard includes a visual exploration tool that allows you to analyze the network activity and traffic traversing in and out of your cloud environment. You can choose from an extensive set of predefined queries or craft custom ones using CloudGuard's expressive yet concise query language. The Explorer visualization feature lets you see every element and traffic in your VPC at a glance, and from there, zoom into the relevant entity or connection. Use CloudGuard's rich contextualized visualization to fire: Deep investigation, Incident response, and Threat Hunting.



ENRICH YOUR SIEM TO SEE THE CLOUD

CloudGuard Log.ic's firehose connector feeds the enriched log traffic in a highly contextualized JSON format to various SIEM products for further investigation. Pipe into Splunk, ArcSight, LogRythm and more, to nurture with critical data on ephemeral assets and security posture awareness.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan 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; 650-628-2117 | Fax: 650-654-4233 | www.checkpoint.com