INSIGHTS
High fidelity Cloud Security Posture Management that provides visibility, control, and compliance across all cloud assets.

SOLUTION
CloudGuard High Fidelity Security Posture Management allows enterprises to easily manage the security and compliance of their public cloud environments at any scale across Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Kubernetes. CloudGuard visualizes and assesses security posture, detects misconfigurations, models and actively enforces gold standard policies, and protects against attacks and insider threats. Through enriched cloud security intelligence for cloud intrusion detection, CloudGuard ensures compliance with regulatory requirements and security best practices. Organizations use CloudGuard for faster and more effective cloud security operations, pain-free compliance and governance, and rugged DevOps practices.

KEY USE CASES
Security Operations: Visualize assets, assess security posture, fix misconfigurations and threats, manage the cloud firewall, and enforce security from a single source of network authority.

Privileged Identity Protection: Protect against compromised credentials and identity theft using a cloud’s native IAM capabilities to safeguard access to actions that can have a big impact.

Compliance and Governance: Manage the compliance lifecycle for standards such as PCI DSS, from automated data aggregation and assessment to remediation and reporting.
Cloud Security Intelligence: CloudGuard Log.ic is a cloudnative security intelligence technology that delivers cloud intrusion detection, network traffic visualization and user activity analytics.

Workload Protection: Seamlessly integrate protections and controls into your CI/CD tools, like CloudFormation and Terraform, and evaluate security posture pre-deployment—scaling across hundreds of thousands of cloud assets.

AGENTLESS, CLOUD-NATIVE ARCHITECTURE FOR TODAY’S CLOUD
CloudGuard uses the native security controls provided by public clouds to protect all cloud resources, including built-in services such as AWS RDS, GCP compute engine instances, and Azure LBs, meeting the needs of modern public clouds that agent-based solutions cannot address. CloudGuard for Cloud Security Posture Management allows you to protect multiple cloud environments by combining cloud-agnostic policy automation with cloud-native security capabilities. You can specify policies once across multiple clouds, and the system uses underlying cloud controls to implement the policy on each cloud.

HIGH FIDELITY POSTURE MANAGEMENT
CloudGuard for Cloud Security Posture Management provides enriched vulnerability management findings to better identify, prioritize, and auto-remediate events based on public exposure—minimizing risk. Prevent critical cloud security misconfigurations and keep up with evolving posture management security and compliance best practices, including auto-remediation. Comply with regulatory and industry standards, such as HIPAA, CIS BENCHMARKS, NIST CSF/800-53, PCI-DSS, with the most contextual cloud security across, 70+ native cloud services.

FASTER TIME-TO-VALUE
With no software to install and no agents to manage, you can secure your environment with CloudGuard in under five minutes. You never have to worry about software updates and scaling problems. CloudGuard for Cloud Security Posture Management integrates with your AWS accounts leveraging innovative cross-account trust policy to gather security information, rather than sharing keys and credentials.

REMEDIATE IN PLACE – FIND IT, FIX IT
Based on learned function context, CloudGuard provides dynamic protection along with automatic protection from the time of invocation. CloudGuard’s Function Self Protection (FSP) detects, alerts, and stops application layer attacks such as the Serverless OWASP Top 10 and anomalous activity independent of the attack trigger.

PLATFORM INTEGRATIONS FOR ALERTING & FORENSICS
CloudGuard is not just a monitoring solution. In addition to powerful visualization capabilities that allow you to review security posture in real-time to discover any vulnerabilities, compromised workloads, open ports or misconfigurations, CloudGuard also allows administrators to take the necessary actions to rapidly mitigate risk through remediation from a single platform. No more patchwork of tools needed for monitoring, remediation, or enforcement, thus bringing agility to the security and compliance life-cycle.