SOLUTION BRIEF

Security for AWS

Monitor and defend AWS applications

Overview

Moving to Amazon Web Services (AWS) helps organizations alleviate common security concerns, but with the shared responsibility model, many are still accountable for ensuring the security of their data and apps. AWS security services, such as GuardDuty, Macie, and Inspector are important building blocks for securing your AWS accounts. However, to protect against advanced threats, organizations need to integrate their security and apply the right expertise and processes. They also need to protect user credentials, proactively identify vulnerabilities, and centralize security monitoring.

Such advanced security is achievable. Trellix Helix is a cloud-based security operations platform that allows organizations to take control of any incident from alert to fix. Helix integrates disparate security tools and augments them with next generation security information and event management (SIEM), security orchestration, and threat intelligence capabilities to capture the untapped potential of security investments.

AWS users should know their security maturity level:

- **Basic:** Essential security controls are implemented manually, and infrastructure is not proactively monitored.
- **Intermediate:** Additional security controls from AWS are implemented, but their operation is for compliance only, with little interaction from security operations. Investigations are rare and time consuming.
- **Advanced:** Security controls are centralized, and security operations uses extensive automation to conduct regular, comprehensive investigations on raised alerts.

With AWS and Helix, your security operations can:

- Audit and flag suspicious data access
- Know who is logged in, what actions they took, and whether this behavior was normal
- Detect when instances are started and if they're authorized
- Centralize audit logging for compliance purposes
- Provide full context around alerts to expedite triage

Key highlights

- Gain real-time visibility into cloud infrastructure activity to monitor threats and configuration issues.
- Detect credential misuse and understand actions taken across your AWS environments.
- Centralize monitoring and collection of AWS CloudTrail, Amazon Simple Storage Service, and elastic load balancing logs to accelerate security operations.

What the Trellix solution does:

- Surface unseen threats with visibility and intelligence
- Prevent credential abuse and cloud misconfiguration
- Track decentralized assets

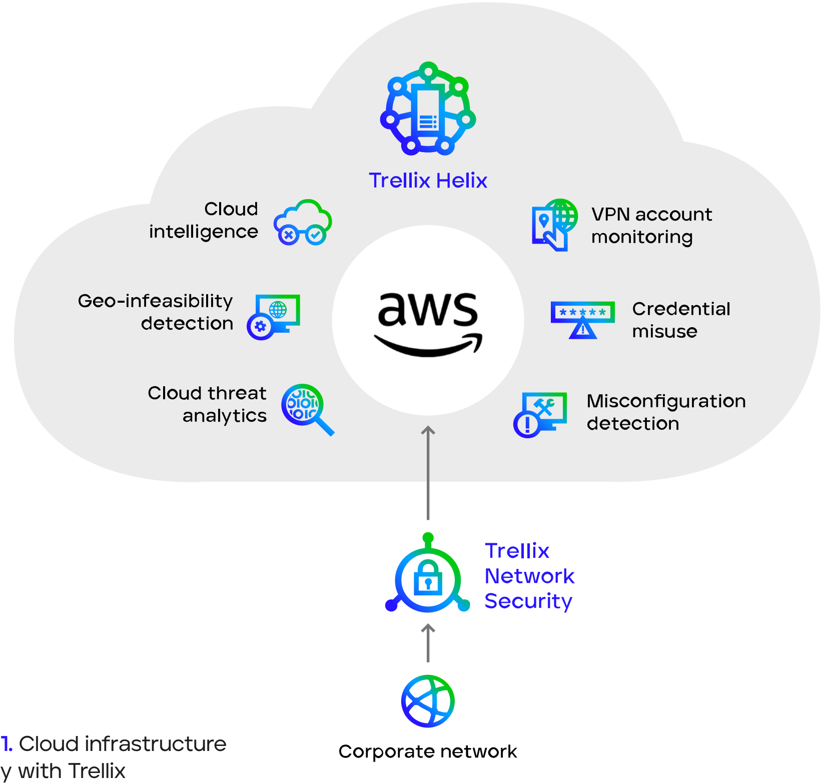

Figure 1. Cloud infrastructure security with Trellix

Credential misuse detection	Geo-infeasibility detection	Cloud configuration rules, analytics, and orchestration
Identifies and alerts you about compromised accounts	Detects whether observed logins are physically impossible given a geolocation	Detects, automatically remediates, and generates reports on cloud misconfigurations
Compromised VPN account detection	**Cloud intelligence**	**Network monitoring**
Identifies potential VPN-based threats by applying heuristics that rely on data center logins, geo-infeasibility, and IP anomaly detection	Enhances Amazon GuardDuty alerts with contextual intelligence to facilitate efficient detection and response	Detects anomalous activity over WAN links to prevent lateral attacker movement between corporate networks and infrastructure as a service and platform as a service clouds

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

Trellix

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.