SOLUTION BRIEF

FireEye

Security for AWS

Monitor and defend AWS applications

HIGHLIGHTS

- Gain real-time visibility into cloud infrastructure activity to monitor for threats and configuration issues.
- Detect credential misuse and understand actions taken across your AWS environments.
- Centralize monitoring and collection of Cloud Trail, S3 and ELB logs to accelerate security operations

Moving to Amazon Web Services (AWS) helps organizations alleviate many security concerns, but with the shared responsibility model, organizations are still responsible 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. FireEye Helix is a cloud-based security operations platform that allows organizations to take control of any incident from alert to fix. FireEye Helix integrates disparate security tools and augments them with next generation SIEM, security orchestration, and threat intelligence capabilities to capture the untapped potential of security investments.

AWS users should assess 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 FireEye Helix, your security operations can:

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

aws partner network

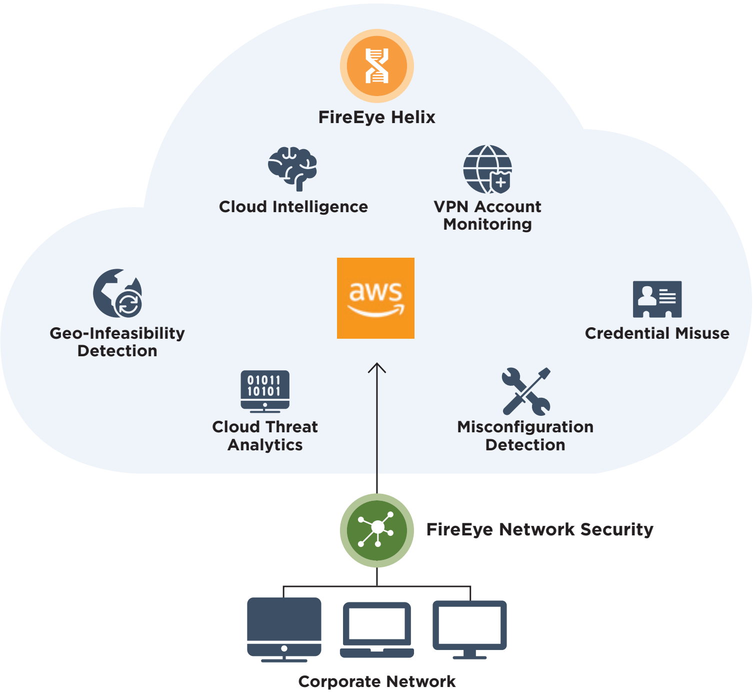
Advanced
Technology
Partner

What FireEye Solution Does:

Surface Unseen Threats with Visibility and Intelligence

Prevent Credential Abuse and Cloud Misconfiguration

Track Decentralized Assets



Cloud infrastructure security with FireEye.

Credential Misuse Detection

Identefies and alerts on compromised accounts

Geo-Infeasibility Detection

Detects whether observed logins are physically impossible given a geolocation

Cloud Configuration Rules, Analytics and Orchestration

Detects, automatically remediates and generates reports on cloud misconfigurations

Compromised VPN Account Detection

Identifies potential VPN-based threats by applying heuristics that rely on data center logins, geo-infeasibility and IP anomaly detection

Cloud Intelligence

Enhances Amazon GuardDuty alerts with contextual intelligence to facilitate efficient detection and response

Network Monitoring

Detects anomalous activity over WAN links to prevent lateral attacker movement between corporate networks and IaaS and PaaS clouds

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

FireEye®