SOLUTION BRIEF

FireEye

Security for the Cloud

Monitor and defend hybrid infrastructure

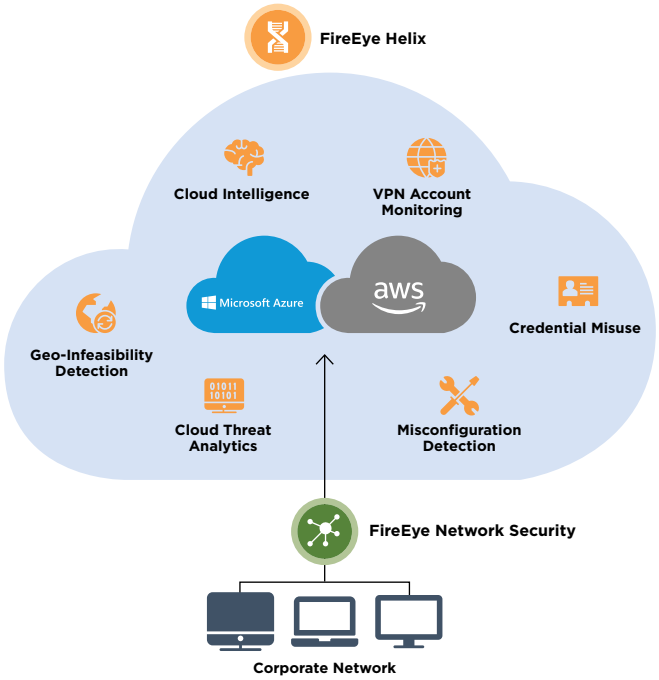
HIGHLIGHTS

- Gain real-time visibility into cloud infrastructure vulnerabilities and threats
- Detect and prevent credential abuse and inadvertent misconfiguration that can lead to a cloud breach
- Centralize monitoring and collection of Cloud Trail, S3 and ELB logs to simplify security operations

As organizations move business operations to the cloud, they face a host of security challenges. Poorly configured authentication, sloppy key management and unsecured APIs are just a few of the ways threat actors gain access to cloud infrastructures. They can then hijack applications and move undetected through the cloud, obtaining credentials and exfiltrating confidential data. The cloud is as vulnerable to attack as on-premise technology, but few organizations have the tools necessary to protect it.

Providers of infrastructure as a service (IaaS) and platform as a service (PaaS) employ a shared responsibility model of security that leaves customers responsible for protecting their own data in the cloud. To defend cloud infrastructure, organizations need to protect user credentials, proactively identify vulnerabilities and centralize security monitoring.

Such advanced security is achievable. FireEye Helix is a security operations platform that uses centralized visibility, configuration monitoring and user behavior analytics to detect advanced attacks in the cloud.



Cloud infrastructure security with FireEye.

What the FireEye Solution Does:

Surface Unseen Threats with Visibility and Intelligence

Prevent Credential Abuse and Cloud Misconfiguration

Track Decentralized Assets

Credential Misuse Detection

Identifes 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

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FireEye