Making sense of security data has never been more challenging. Malicious users, compromised accounts and cloud infrastructure vulnerabilities add complexity to the challenge of finding threats and remediating compromises. Organizations need automated, machine learning-driven detection that empowers security teams to find threats faster.

FireEye Helix integrates your security tools and augments them with next generation SIEM, orchestration and threat intelligence capabilities to capture the untapped potential of security investments. The security analytics built into FireEye Helix enables security operations teams to prevent, detect, and respond to threats faster.

**BENEFITS**

- **Identify threats faster:** Shorten the time it takes your analysts to find threats by helping them identify abnormal patterns.
- **Detect advanced, non-malware based attacks:** Identify complex attacks that leverage stolen credentials or misconfiguration vulnerabilities with UEBA and configuration monitoring.
- **Prevent insider threats and lateral network movement:** Track user behavior and network traffic patterns to identify attackers before they can exfiltrate data.

**Figure 1.** Operational interface for immediate situational awareness.
User, Entity and Behavioral (UEBA) Analytics
Track users accessing data across your environment, detect behavioral anomalies, and identify insider threats.

Cloud Analytics
Proactively identify and automatically prevent AWS and Azure cloud misconfigurations.

Machine Learning
Build detection rules to identify threats unique to your environment using machine learning and dynamic modelling.

Credential Abuse and Compromised Account Detection
Monitor all your connected devices and networks. Detect abnormal access behavior or to prevent covert attacker access.

Lateral Network Movement Detection
Analyze inbound and outbound network traffic patterns, port scanning attempts and VPN access.

Security Augmentation
Enhance your native cloud security products and have greater access control and visibility with an integrated interface.

HOW TO GET THE FIREEYE HELIX PLATFORM
FireEye Helix is available standalone or with the purchase of FireEye’s subscription-based solutions. It works across all FireEye technologies and helps integrate your installed base of non-FireEye security products. As your organization grows and changes, FireEye solutions can be reconfigured, added or upgraded without disrupting organizational operations.

To learn more about FireEye Helix, visit: www.FireEye.com/helix

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. H-EXT-BF-US-EN-000263-01