Introduction
Cyber security has never been more challenging. Almost daily, new threats expose companies’ vulnerabilities, forcing them to purchase more products and hire more talent. Such reactive approaches lead to escalating complexity — yet another vulnerability attackers can take advantage of. Security operations — big or small — require a holistic, foundational approach. FireEye Helix helps organizations build that foundation.

FireEye Helix is a SaaS security operations platform that allows organizations to take control of any incident from detection to response. Available with any FireEye solution, 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. Designed by security experts, for security experts, it empowers security teams to efficiently conduct primary functions, such as alert management, search, analysis, investigations and reporting.

HIGHLIGHTS

- **Detect advanced threats:** Integrate over 600 FireEye and non-FireEye security tools and overlay contextual threat intelligence, and behavioral analytics to deliver unparalleled situational awareness.
- **Minimize the impact of an incident:** Accelerate response with security orchestration and workflow automation informed by frontline experience.
- **Gain visibility across all threat vectors and deployment types:** Whether on premise or in the cloud, centralize security data and infrastructure with next-generation SIEM for complete visibility into threats and vulnerabilities.

Figure 1. Operational interface for immediate situational awareness.
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.