FireEye Helix

World-class detection and intelligence for security operations

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.

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.
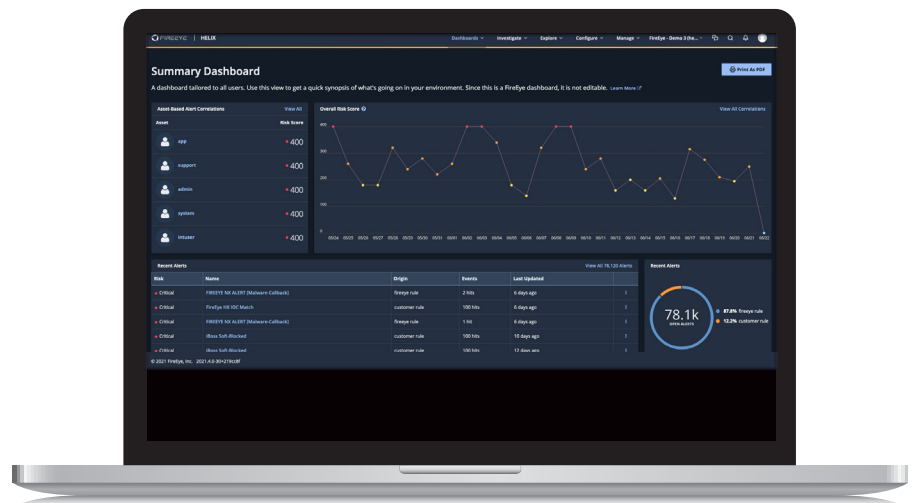

Figure 1. Operational interface for immediate situational awareness.

What FireEye Helix Does

Detect security incidents by correlating data from multiple tools

Make informed and efficient decisions with contextual threat intelligence

Centralize security data and infrastructure

Threat Intelligence
Detect, enrich, explore and learn about the latest intelligence threats.

Security Orchestration and Automation (SOAR)
Automate response with pre-built playbooks created by frontline practitioners.

Workflow Management
Organize, assign, collaborate and action steps through the investigative process through automated and manual workflows.

Next-Generation SIEM
Improve threat and vulnerability detection with advanced user behavioral analytics.

User and Entity Behavior Analytics (UEBA)
Correlate alerts with machine learning to identify activities that suggest a high risk of insider threats, lateral movement or final-stage attacks.

Compliance Reporting
Use and customize dashboards and widgets to visually aggregate, present and explore the most important information.

How to Get the FireEye Helix Platform

FireEye Helix is available with the purchase of any FireEye subscription-based solution. It works across all FireEye technologies and integrates 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, 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