Legacy security information and event management (SIEM) solutions aggregate event data, manage alerts and apply analytics to detect threats. But modern security teams demand more to help manage and automate security operations, enable faster and more effective investigations and detect advanced threats across on-premises and cloud infrastructures.

FireEye Helix offers all those capabilities and more. Available with any FireEye solution, FireEye Helix integrates with your security tools and augments them with next generation SIEM, orchestration and threat intelligence capabilities to capture the untapped potential of security investments.  

**Benefits**

- **Find true threats**: Detect threats faster with contextual intelligence and machine learning.
- **Efficiency and simplified management**: Accelerate response with alert context and dedicated investigative tools.
- **Get the most from your security stack**: Integrate and analyze data from your existing security stack to maximize your investment.

---

**Figure 1.** FireEye technologies working with a security information and event management solution.
## ADDITIONAL CAPABILITIES

### User, Entity and Behavioral (UEBA) Analytics

Track users and devices across your environment. Detect behavioral anomalies and identify insider threats, lateral attacker movement and data exfiltration.

### Cloud Analytics

Identify vulnerabilities in your cloud environments by monitoring for misconfigurations and automatically prevent them from being exploited by attackers.

### Integrated Threat Intelligence

Detect threats using rules derived from our insight into attacker tactics, techniques and procedures (TTP)s and known indicators of compromise (IOC)s.

### Compliance and Alert Reporting

Simplifies PCI and HIPAA compliance reporting with data dashboards to retain and organize event information and monitor privileged user access.

### Managed Rules

Receive near real-time updates from dedicated analysts to ensure your organization is protected from the latest attacker techniques.

### Workflow and Case Management

Collect alert data and assigns risk level for easy prioritization. Provide SOC teams with response and collaboration tools.

### Guided Investigations

Leads users through prepopulated investigative methods and a series of "next step" searches that provide useful context to the investigation for the responder to pursue.

### Expertise on Demand

Gain expert insight into any threat or event at the click of a button. Augment your security team’s capabilities and accuracy.

---

**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](http://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-000264-01