



## DATA SHEET

# FireEye Helix

## Simplify, integrate and automate your security operations



FireEye Helix is a comprehensive detection and response platform designed to simplify, integrate and automate security operations. FireEye understands cyber attacks better than anyone else and applies that knowledge to remove complexity from security. Our intelligence-led approach blends innovative security technologies, nation-grade FireEye Threat Intelligence and world-renowned expertise from FireEye Mandiant into FireEye Helix — our end-to-end security operations and response platform.

The security operations experience today is disjointed, with alerts generated across dozens of low fidelity products and management consoles without the benefit of contextual intelligence or automation and orchestration. This causes IT and security leaders to spend more time on inefficient manual processes and infrastructure management, leaving the organization less secure.

Designed by security experts, for security experts, FireEye Helix helps organizations operationalize their security programs and enables security teams to move from detecting a threat to defeating it quickly at a low total cost of ownership. They can gain clear insight into whether resources are effectively allocated and whether their security posture has improved.

FireEye Helix is based on a revolutionary platform that brings together the FireEye product portfolio with event data from non-FireEye components of an IT and security infrastructure. From this centralized platform, security

teams can overlay FireEye Threat Intelligence to triage buried threats and perform rich analytics to detect lateral movement, data exfiltration, account abuse and user behavior anomalies. All the while, they build the context to automate, prioritize and accelerate response activity. These capabilities are delivered through unified dashboards, guided search and reporting modules that enable users to quickly pivot from detection to investigation to response across every infrastructure component.

### Benefits

#### Raise your visibility

FireEye Helix features our award-winning MVX™ engine that drives network and endpoint threat detection. It intelligently collects and combines network metadata and alerts from across the security infrastructure and delivers them to a unified console. And it overlays FireEye Threat intelligence, rules and analytics to give your organization unparalleled situational awareness to stay a step ahead of attacks.

#### Accelerate response and minimize the impact of a breach

You need the right information at exactly the right time to stop threats. Helix gives analysts validated alerts with contextual analyses and the ability to rapidly shift from detection to remediation whether on the network or an endpoint. This helps to resolve attacks quickly and effectively and provides rich dashboards and reports for compliance audits and management briefings.

FireEye Helix accelerates and simplifies the end-to-end threat detection and response process by bringing together your existing technology investments and incident handling processes into automated workflows that deliver real-time responses, reduce risk exposure and maintain process consistency across a security program. Each deployment comes with pre-built playbooks that codify years of FireEye experience battling the world’s most consequential breaches. These playbooks hone your processes to effectively detect, investigate and respond to threats.

**Enhance existing security investments and reduce operational costs**

Many organizations have security tools that are disconnected and require slower manual processing that is prone to errors. FireEye Helix integrates and enhances existing security tools with automated correlation, pre-built playbooks and FireEye Threat Intelligence context to help you prioritize the alerts that matter the most and investigate and respond to threats faster than ever.

**Flexibly scale your operations**

Organizations change and grow over time and FireEye Helix is built to evolve right alongside them. It uses the elasticity of the cloud to quickly scale consumption and deployment and can always incorporate the latest available tools and technologies for the best possible cyber defense. FireEye Helix works on premise and in private, public and hybrid cloud environments.

**Achieve compliance**

For many organizations, reporting on compliance is often tasked to the security team because they have access and visibility into compliance-related activity and the expertise to secure critical systems. FireEye Helix contains pre-configured dashboards to provide visibility into your compliance program and a scheduled search capability to collect raw data over time. It helps your team satisfy audit requests quickly so they can focus on protecting your network.

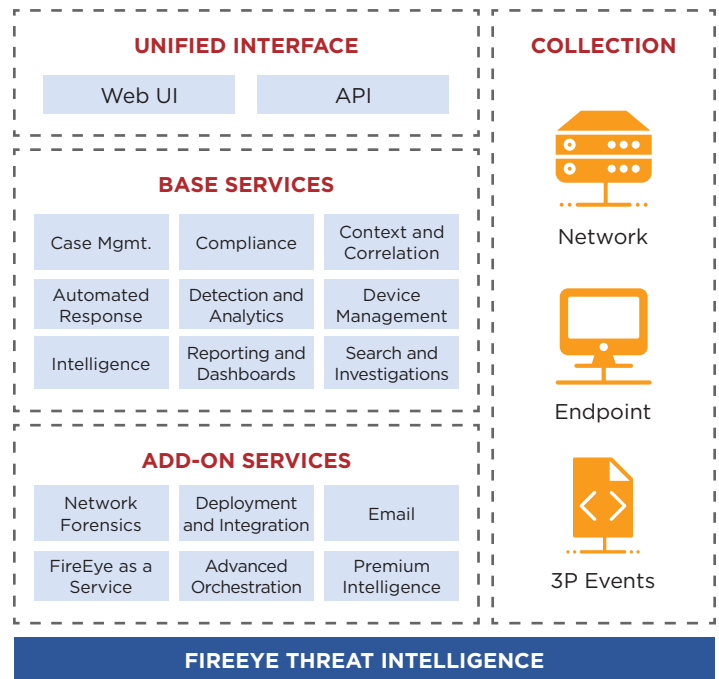
**FireEye Helix architecture**

With flexible deployment options, any organization can customize FireEye Helix to fit their security program’s requirements and existing architecture. An annual subscription includes organization-wide entitlement for:

- Cloud-based unified console with integrated FireEye Threat intelligence orchestration and analytics
- Network security smart nodes
- Endpoint agents

This can be further enhanced with optional FireEye Threat Intelligence components, integrated email security, increased customization of security orchestration, more pre-built playbooks and FireEye as a Service.

Figure 1. Helix at a glance.



To learn more about FireEye, visit: [www.FireEye.com](http://www.FireEye.com)

**FireEye, Inc.**

601 McCarthy Blvd. Milpitas, CA 95035  
408.321.6300/877.FIREEYE (347.3393)  
info@FireEye.com

©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-DS-US-EN-000050-04

**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.

