DEPLOYMENT AND INTEGRATION SERVICES

FireEye Helix

OVERVIEW

Deployment and Integration Services for FireEye Helix allow you to seamlessly integrate FireEye Helix with our leading detection and protection technologies, our world-class threat intelligence and security consulting and your third-party security products. They ensure that your security operations platform investment connects and enhances all of your security solutions so your team can surface unseen threats and make expert decisions based on frontline intelligence.

Our professional methodology for deploying network, email, endpoint and log and analytics solutions in the FireEye Helix platform helps your organization quickly realize the benefits of FireEye Helix. FireEye Helix deployment and integration services install, configure and onboard a variety of Helix-enabled solutions, including physical or virtual on-premise sensors, endpoint agents and cloud-based controllers and analytics engines.

There are four tiers of services for FireEye Helix:

- The **basic jumpstart** is for organizations that have minimal data sources and want to accelerate implementation and integration with their existing security operations.
- The **standard jumpstart** is ideal for mid-tier organizations that have a moderate number of log sources and network points to monitor.
- The **advanced jumpstart** is for organizations that have larger or more complex networks, along with a larger set of data sources and deeper analytics requirements.
- For the most complex networks and analytics requirements, we offer **custom scoped engagements** to provide tailored services that include additional onboarding, tuning and custom dashboard creation.

FireEye professionals close every jumpstart with a detailed solution overview report that includes the test plan, configuration and architecture of the installed products and solution.

Jumpstart Process Inclusions

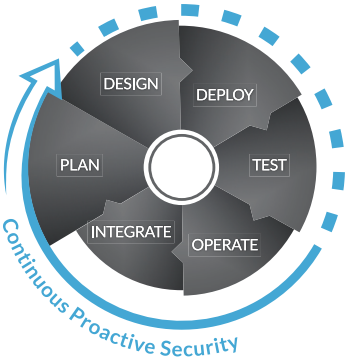
FireEye professionals work with you to develop a deployment process to successfully implement FireEye Helix. The process includes:

- Deliverables and estimated timelines for FireEye Helix components
- Deployment milestones
- Architecture review
- Onboarding of the FireEye Helix components
  - Instantiation and configuration of FireEye Helix cloud instances such as FireEye Helix dashboard, cloud Endpoint Security and cloud Central Management
  - Configuration of an Endpoint Security controller and deployment of endpoint agents, including host set creation, hit triage and workflow process setup
  - Configuration and deployment of virtual or physical Network Security sensors, including enterprise authentication configuration (e.g. LDAP, AAA) and network flow analysis
  - Configuration and deployment of log and analytics cloud collectors
  - Configuration of rules, lists and custom intelligence Integration of third-party data sources

HIGHLIGHTS

- **Efficient Deployment:** Accurate, best-practice platform configuration deployed by FireEye experts
- **Operational Readiness:** Seamless integration of FireEye cloud and on- premise products to ensure operational readiness
- **Tailored Deployment Process:** Step-by-step custom deployment management from kickoff documentation to final deliverables
- **Customer Enablement:** Helix workflow processes for detection, validation and remediation on the network and endpoints
- **Maximum Helix Value:** Guidance on data source selection, custom rule development and threat hunting enablement

DEPLOYMENT AND INTEGRATION



- Documentation
- Knowledge transfer for FireEye Helix platform components
  - Component setup and administration
  - FireEye Helix platform web and command line interfaces
  - Basic alert analysis and review, including alert severity and prioritization, OS change reports and contextual intelligence from the FireEye Threat Intelligence Portal
  - Host management, including host containment processes and agent upgrades
  - Threat hit review
  - Triage data collection and review using Redline
  - Effective search techniques to find threats
  - Event and case management in FireEye Helix
  - Custom rules, indicators and dashboards
  - FireEye, custom and automatic threat creation
  - Hunting for malicious activity with FireEye Helix

Table 1. FireEye Helix Deployment and Integration Jumpstarts.

	Basic	Standard	Advanced
Onsite visits	One visit, up to four days	One or two visits, up to four days each	Up to three visits, up to four days each
Deployment of Endpoint Security (HX series) agents	Pilot deployment	Pilot deployment; additional agents, time permitting	Pilot deployment; additional agents, time permitting
Deployment of FireEye network sensors	Up to 2	Up to 6	Up to 10
Deployment of cloud collectors	Up to 2	Up to 6	Up to 10
Database backup and restore processes for on-premise systems	Yes	Yes	Yes
System and alert notifications setup	Yes	Yes	Yes
Data source onboarding	Up to 5	Up to 5	Up to 10
Custom rules creation	Up to 5	Up to 5	Up to 15
Dashboards configuration and tuning	Yes	Yes	Yes
Hunting enablement			Yes
Rule efficacy analysis			Yes
Configuration validation	Yes	Yes	Yes
Knowledge transfer on Helix components	1 session, up to 3 staff	2 sessions, up to 5 staff	2 sessions, up to 8 staff

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300 / 877 FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. 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 has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye