

Deployment and Integration Services

OVERVIEW

FireEye offers comprehensive deployment and integration services to ensure the proper configuration of FireEye technology, streamline workflow between systems and address user knowledge gaps. The result is a more efficient security infrastructure that can respond more quickly to cyber threats and better protect your organization.

Introduction

Organizations continue to increase spending on security products, but the number of incidents continues to climb. While it's true that advanced attacker tactics can be highly sophisticated, compromises also happen when security products are not properly configured or integrated and IT security teams aren't fully trained and enabled.

In the rush to bring new security technologies online, organizations often overlook or postpone optimization strategies, resulting in an overload of alerts, an inability to prioritize critical events, high manual error rates and slow response times.

FireEye deployment and integration services provide your organization with a professional team of consultants trained

to implement and validate your FireEye technology investments and integrate FireEye solutions into your broader security infrastructure. The result: peace of mind, reduced risk and continuous improvement through skills development.

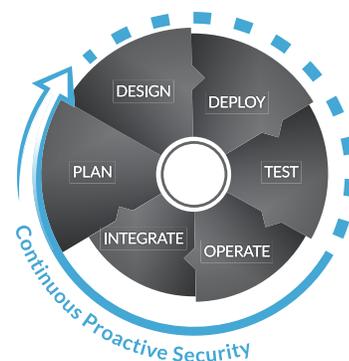
FireEye deployment and integration services offer:

- A dedicated team of trained and certified FireEye consultants
- Orchestration and workflow optimization expertise
- Experience with hundreds of FireEye product deployments in a variety of unique environments and architectures
- Broad industry and government experience
- Long-standing client services relationships
- Priority escalation to Mandiant Incident Response and FireEye engineering teams
- Worldwide presence with regionally located consultants
- Consistent testing and deployment methodologies

HIGHLIGHTS

- **Integration of products across security infrastructure:** Workflows optimized through automation, providing improved efficiency and response times
- **Customization and tuning:** Indicators, alerts and scripts relevant to your organizational practices
- **Backup, recovery and system health monitoring:** Proactive management, risk mitigation and disaster readiness
- **Skills development and best practices:** Multi-level reporting, triage, live analysis and containment

DEPLOYMENT AND INTEGRATION



All of the trends we're seeing lead to one conclusion: **It is more critical to focus on all aspects of your security posture** (people, processes and technology) than ever before.

- Mandiant M-Trends 2016 Report

Service Offerings

The FireEye Deployment and Integration Services team provides comprehensive service offerings for FireEye endpoint, network, and cloud solutions. FireEye also provides specialized integration services to automate

workflows between FireEye solutions and other security products with FireEye Security Orchestrator using out-of-the-box plugins for most common security tools and the ability to build custom plugins and courses of action for your unique use cases.

Endpoint Platforms	Network Platforms	Cloud and Integration Services
Basic Jumpstart Services <ul style="list-style-type: none"> • Foundation implementation and configuration • Basic architectural review and design • Agent roll-out, testing and verification • Hit triage and workflow process setup • Integration with FireEye network products • Knowledge transfer and documentation: Containment, triage and live response 	Basic Jumpstart Services <ul style="list-style-type: none"> • Foundation architectural review and design • Appliance configuration and detection testing • System and guest image updates • Enterprise authentication authorization and access control • Integration with FireEye endpoint products • Knowledge transfer and documentation: Alert notification and reporting 	FireEye Security Orchestrator Jumpstart Services <ul style="list-style-type: none"> • Orchestration architecture, configuration and administration • Use case definition • Courses of action (CoA) builds • Plugin installation and development • CoA cyber playbook review • Knowledge transfer and documentation: CoA development and product integrations
Advanced Jumpstart Services <ul style="list-style-type: none"> • Automated backup and restore • API and custom integration review • Endpoint Security custom IOCs • System health monitoring • Redline forensic analysis • Rollout assistance and scripting for additional agents • Enterprise searches and tuning 	Advanced Jumpstart Services <ul style="list-style-type: none"> • Database backup and restore • System health monitoring • Configurable integrations (e.g. SIEM, Syslog) • Advanced architectural scenarios, and lab testing, such as high availability and MVX separation 	FireEye TAP and Helix Jumpstart Services <ul style="list-style-type: none"> • Customized data source workshop • Deployment of Communication Brokers and Cloud Collectors • Data source on-boarding • Rules, lists, custom intel configuration • Dashboard tuning and configuration • Hunting enablement • Use case documentation and verification • Configuration validation • Rule efficiency analysis
Best Practice Services <ul style="list-style-type: none"> • Analysis best-practices workshops: Incident detection and response workflow integration • Knowledge transfer and documentation: Containment, basic memory acquisition, and analysis and tuning procedures 	Best Practice Services <ul style="list-style-type: none"> • Analysis best-practice workshops: Incident detection and response workflow integration • Knowledge transfer and documentation: Malware detection, analysis and response procedures 	FireEye as a Service Jumpstart Services <ul style="list-style-type: none"> • Solution architecture design and planning • Deployment and configuration of FireEye on-premise and cloud components • Connectivity enablement • Onboarding and transition services • Knowledge transfer and documentation: FireEye and customer partnership

Enterprise Services Packages

Enterprise services can be applied to endpoint, network, cloud and orchestration services. They may include:

- Comprehensive project management
- Advanced architecture design and implementation
- Development, coordination, implementation and documentation of comprehensive testing processes
- Analysis best practices, health check services and FireEye as a Service onboarding

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.

© 2017 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. DS.DIS.EN-US.082017

