DEPLOYMENT AND INTEGRATION SERVICES

# FireEye Endpoint Security

## OVERVIEW

Deployment and Integration Services for FireEye Endpoint Security ensure that your Endpoint Security deployment integrates with your security response processes, is easy to maintain and provides actionable threat data. The service is available in two jumpstart options:

- The **basic jumpstart** is for organizations that have recently purchased an Endpoint Security appliance and want to apply FireEye methodology to manage hosts, review alerts, prioritize responses and enhance workflows to more quickly contain attacks.
- The **advanced jumpstart** is designed for organizations that have recently purchased an Endpoint Security appliance and one or more Endpoint Security DMZ appliances and are interested in additional assistance for forensic analysis of triage packages.

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.

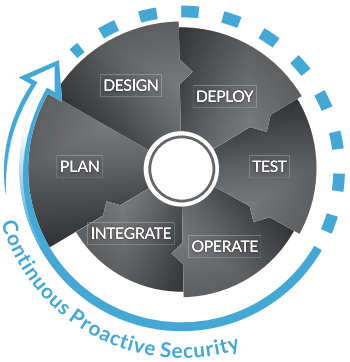
**Table 1. Jumpstarts.**

| | Basic | Advanced |
|---|---|---|
| **Endpoint Security architecture design, configuration, administration** | Yes | Yes |
| **Integration with Network Security and Email Security using FireEye Central Management** | Yes | Yes |
| **Agent deployment (number of profiles)** | 3–5 | Up to 15 |
| **Host set creation** | Yes | Yes |
| **Hit triage and workflow process setup** | Yes | Yes |
| **API and custom integration review** | Yes | Yes |
| **Endpoint Security core concepts knowledge transfer (IOCs, hit review and more)** | Up to 2 staff | Up to 7 staff |
| **Additional Redline forensic analysis** | | Yes |
| **Endpoint Security custom IOC creation** | | Yes |
| **Additional agent rollout assistance and scripting** | | Time permitting |
| **Installed solution documentation** | Yes | Yes |
| **Duration (consecutive days)** | Up to 3 | Up to 5 |

## HIGHLIGHTS

- **Efficient Deployment:** Accurate, best-practice configuration deployed by FireEye experts
- **Rapid Containment:** Provision of workflow process to ensure fast identification, triage and containment of threats to endpoint systems
- **Efficient Analysis:** Training that enables your staff to use FireEye tools such as Redline
- **Operational Readiness:** Integration with existing technology, including other FireEye technologies as well as SIEM and central logging systems

## DEPLOYMENT AND INTEGRATION




FireEye

This jumpstart enhances your Endpoint Security solution with FireEye expertise and methodologies on host management, alert review and analysis, activity prioritization, threat investigation and containment workflow processes.

Jumpstarts include Endpoint Security architecture design, configuration, and agent deployment. FireEye staff also validate the Endpoint Security installation and provide best practice recommendations for ongoing maintenance and management.

Your staff will learn how to:

- Locate FireEye updates, threat packages and support mechanisms
- Understand Endpoint Security architecture, setup and administration
- Use Endpoint Security agent, controller and interfaces
- Administer Endpoint Security appliances
- Upload information about new threats
- Integrate Endpoint Security with other security appliances
- Access support resources such as the FireEye Customer Support Portal, forums, blogs and customer communications

Endpoint Security operators will also learn how to manage hosts, review threat "hits," and collect and analyze triage packages. They will learn the workflow for containment requests, review and approvals. Finally, they will learn the various threat sources and how those threat sources influence the data returned to the Endpoint Security controller.

The knowledge transfer session covers the following topics:

- Host management
- Threat hit review
- Triage data collection and review using Redline
- Host containment requests, approval and removal
- FireEye, custom and automatic threat creation

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