Overview

FireEye Flexible Defense is a rapidly deployable cyber defense and response solution powered by the same industry-leading, award-winning tools used by Mandiant incident responders every day to protect and respond to the world’s most advanced persistent threats (APTs).

This solution integrates three critical FireEye technologies and applies machine learning to help detect malicious activity that might have previously been missed. By incorporating the FireEye platform, and integrating with third-party tools, this solution provides full-scale cyber operations in all types of environments.

Use-cases include

- Defensive Cyber Operations (DCO)
- Site Assessments & Validation
- Incident Response
- Network Forensics
- Host-Based Forensics
- Malware Analysis / Reverse Engineering

Example Sizing and Configurations.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>22.0”x14.0”x9.0”</td>
</tr>
<tr>
<td>Weight:</td>
<td>&lt;45 lbs</td>
</tr>
<tr>
<td>CPU</td>
<td>Up to 28 (Intel) / 64 AMD Cores per CPU</td>
</tr>
<tr>
<td>Storage</td>
<td>Up to 720TB</td>
</tr>
<tr>
<td>RAM</td>
<td>Up to 2TB</td>
</tr>
</tbody>
</table>
FireEye Helix

FireEye Helix is a security operations platform that makes it simple to deliver advanced security to any organization. It surfaces unseen threats and empowers expert decisions with frontline intelligence to take back control of your defenses and capture the untapped potential of your security investments. Available with any FireEye solution, FireEye Helix works as a seamless and scalable foundation to connect and enhance all your security solutions, including non-FireEye products. Designed by security experts, for security experts, FireEye Helix empowers security teams to efficiently conduct primary functions, such as alert management, search, analysis, investigations and reporting.

FireEye Network Security and Forensics

FireEye Network Security and Forensics is an effective cyber threat protection solution that helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic. The FireEye Network Forensics solution pairs the industry’s fastest lossless network data capture and retrieval solution with centralized analysis and visualization. FireEye Network Security uses multiple analysis techniques to detect attacks with high accuracy and a low rate of false alerts:

- The Multi-Vector Virtual Execution™ (MVX) engine detects zero-day, multi-flow, and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops the infection and compromise phases of the cyber attack kill chain by identifying never-before-seen exploits and malware.
- Intelligence-Driven Analysis engines detect and block obfuscated, targeted, and other customized attacks with contextual, rule-based analyses based on real-time insights gathered from the frontlines, including millions of verdicts from the MVX engine, thousands of hours of incident response experience gathered by FireEye Mandiant and the work of hundreds of threat researchers.

FireEye Endpoint Security

Even with the best protection, breaches are inevitable. To ensure a substantive response that minimizes business disruption, FireEye Endpoint Security provides tools to:

- Search for and investigate known and unknown threats on tens of thousands of endpoints in minutes
- Identify and detail vectors an attack used to infiltrate an endpoint
- Determine whether an attack occurred (and persists) on a specific endpoint and where it spread
- Establish timeline and duration of endpoint compromises and follow the incident
- Clearly identify which endpoints and systems need containment to prevent further compromise

To learn more about FireEye, visit: www.FireEye.com