FireEye has long been perceived by the market as purely a breach detection system (BDS) vendor but is working to change this. Today, the vendor offers threat prevention (NX, EX, and FX appliances; HX appliances; MX appliance), forensics (PX and IA appliances, Mandiant Intelligent Response appliance [MIR], AX appliances) and threat analytics (Threat Analytics Platform, or TAP) products. FireEye subscription services (i.e., FireEye as a Service, Threat Intelligence) integrate with all FireEye products. The vendor has recently released enhancements to the FireEye Email Threat Prevention Platform and FireEye Advanced Threat Intelligence and has also updated hardware specifications for both of its endpoint security appliances (HX series).

### Portfolio

<table>
<thead>
<tr>
<th>DEPLOYMENT OPTIONS</th>
<th>Physical appliance, cloud service, managed service (utilizing local hardware)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRODUCT</strong></td>
<td><strong>Network Security</strong>&lt;br&gt;• NX 900 (10 Mbps)&lt;br&gt;• NX 1400 (20 Mbps)&lt;br&gt;• NX 2400 (50 Mbps)&lt;br&gt;• NX 4400/4420 (250 Mbps)&lt;br&gt;• NX 7400/7420 (1,000 Mbps)&lt;br&gt;• NX 7500 (1,000 Mbps)&lt;br&gt;• NX 9450 (2,000 Mbps)&lt;br&gt;• NX 10000 (4,000 Mbps)&lt;br&gt;• NX 10450 (4,000 Mbps)&lt;br&gt;<strong>Email Security</strong>&lt;br&gt;• EX 3400 (150,000 emails per day)&lt;br&gt;• EX 5400 (300,000 emails per day)&lt;br&gt;• EX 8400/8420 (600,000 emails per day)&lt;br&gt;<strong>Content Security</strong>&lt;br&gt;• FX 5400 (80,000 emails per day)&lt;br&gt;• FX 8400 (160,000 files per day)&lt;br&gt;<strong>Endpoint</strong>&lt;br&gt;• HX 4400/4400D&lt;br&gt;<strong>Mobile</strong>&lt;br&gt;• MX 900</td>
</tr>
</tbody>
</table>

*Models listed are available at time of publication.*

- The FireEye network (NX series), email (EX series), and content security (FX series) products inspect traffic on specific protocols.
- The FireEye Threat Prevention Platform feeds information to the FireEye Threat Intelligence service.
- FireEye as a Service is a managed security service that utilizes FireEye hardware.

### Total Cost of Ownership and Market Summary

- At US$460, the **TCO per Protected Mbps** for the EX 3400 and NX 4400 was higher than the average **TCO per Protected Mbps** for the 2015 NSS Labs BDS group test (US$169).
- The BDS market is expected to grow by 41 percent in 2016 and is projected to have a compound annual growth rate (CAGR) of 32 percent over the forecast period.
- A strong interest in post-incident forensics is driving the market.
**Recent Developments**

<table>
<thead>
<tr>
<th>May 2015</th>
<th>July 2015</th>
<th>August 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration with PFU Systems for network access control</td>
<td>Updates HX series endpoint appliances</td>
<td>Receives Caution rating in NSS Labs BDS v2.0 group test</td>
</tr>
</tbody>
</table>

**OCTOBER 2015**

**Buyer Considerations**

<table>
<thead>
<tr>
<th>FACTORS</th>
<th>OVERALL</th>
<th>SIX-MONTH TREND</th>
</tr>
</thead>
</table>
| Product Innovation | NEUTRAL | NO CHANGE | Apple Mac OS X virtual machine support, Apple iOS support for mobile product, and FireEye as a Service  
| | | | Founded in 2004 and often credited with defining breach detection market |
| Product Features | POSITIVE | POSITIVE | Rapidly expanding product capabilities (such as dedicated forensics tools, IPS functionality, endpoint, and mobile)  
| | | | Recent updates in embedded URL detection for FireEye EX series and Advanced Threat Intelligence (ATI)  
| | | | nPulse acquisition |
| Integrations and Third-Party Support | POSITIVE | NO CHANGE | Longtime player in breach detection market; respectable technical alliances (including Adallom, Check Point, ForeScout, ForgeRock, HP ArcSight, Imperva, LogRhythm, NXLog, Splunk, and Verdasys)  
| | | | Building portfolio through acquisition (e.g., Mandiant, nPulse) and organic growth (has launched an IPS) as it works to establish itself as comprehensive security vendor |
| TCO | NEUTRAL | NEGATIVE | FireEye platforms demonstrated a high TCO per Protected Mbps during NSS testing |

**COMPETITIVE FEATURES**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Multiple threat prevention appliances, each with dedicated functionality</th>
</tr>
</thead>
</table>
| Form Factor | NX, FX, HX, MX series: physical appliance (the NX 10450 and the NX 9450 are modular)  
| | EX series: physical appliance, cloud service |
| Deployment Mode | NX series: network inline and out of band; EX series: inline; FX series: out of band |
| Scanning | Focus on primary protocols: HTTP (NX series), SMTP (EX series), and CIFS and NFS-compatible file shares (FX series) |
| Sandbox Location | Local appliance: NX, EX, FX  
| | Cloud-based: FireEye Email Threat Prevention Cloud, Mobile Threat Prevention  
| | HX and MX utilize indicators of compromise for detection; neither has sandbox functionality |
| Customizable Sandbox | Supported, but requires support request from FireEye for implementation |
| Host Remediation | Not supported (FireEye HX series agent reports infections and isolates infected endpoints) |
### STRENGTHS

- In the 2015 NSS BDS group test, the EX 3400 and the NX 4400 passed all stability and reliability tests.
- The Network Threat Prevention Platform (NX series) can be used for traffic enforcement, and permits inline (block/monitor) and out-of-band (TCP reset/monitor) deployment modes.
- Three network scanning appliances (NX series) provide options for higher throughput (>1,000 Mbps) deployments.
- The Threat Prevention Platform can be used in monitor mode to communicate with third-party incident response products.
- The NX 7500 supports Apple Mac OS X sandboxes.
- The FireEye agents in the HX series and in the MIR appliance provide access to host-based forensic information.

### WEAKNESSES

- During the 2015 NSS BDS group test, the combined score for the EX 3400 and NX 4400 was below the test average for breach detection (they achieved a 59.4 percent breach detection rate) and for **TCO per Protected Mbps** (they demonstrated a **TCO per Protected Mbps** of US$460). The devices subsequently received a **Caution** rating. During the test, the devices:
  - Detected 69.1 percent of all HTTP malware, 30.6 percent of all email malware, and 81.3 percent of all exploits, which resulted in its overall breach detection rating of 59.4 percent
  - Detected 46.3 percent of all evasions

### OPPORTUNITIES

- FireEye as a Service will appeal to organizations looking to outsource their breach detection functions.
- The acquisition of forensics specialist Mandiant expands FireEye’s abilities regarding advanced threat behavior.
- The vendor’s expanding partner list (including most recently NXLog, ForgeRock, and Adallom) targets a broader customer base.
- FireEye is building a comprehensive suite of products that comprises scanning, forensics, and analytics capabilities.
- FireEye can leverage its large and expanding development team to remain competitive.

### THREATS

- The challenges associated with large-scale endpoint agent deployments – such as those in which the FireEye HX and MIR products may be installed – are much different than the challenges for network-based technology, which is the market with which FireEye is most familiar. Sales challenges (such as value presentation and proof-of-concept testing) and customer impact (for example, installation and management) must be considered, and FireEye lacks the experience of some traditional antivirus competitors that also offer breach detection products.
- Network scanning, email scanning, content scanning, and endpoint scanning tools are offered as discrete components of the Threat Protection Platform, and while these are integrated products and technologies, such a modular approach can increase maintenance costs. Scaling sandboxes, whether they are located on-premises or in the cloud, often introduces additional management and costs.
- Unless the HX series appliances and the MIR appliance are consolidated, customers desiring threat detection, validation, isolation, and comprehensive forensics will have to purchase both products.
At NSS, **Security Effectiveness** and throughput are critical metrics by which security devices are measured. NSS testing has shown:

- FireEye’s breach detection rate reached 59.4 percent overall, which was below the average of the 2015 NSS BDS group test.
- Vendor-claimed throughput aligned with NSS-tested throughput in 2014 and 2015.

During the 2015 NSS BDS group test, the EX-3400 and NX-4400:

- Detected 100.0 percent of sandbox evasions and virtual machine evasions
- Detected 63.8 percent of packer evasions
- Detected 10 percent of HTML obfuscation evasions
- Detected 4.2 percent of compressor evasions
- Detected 0 percent of layered evasions

### NSS Labs Group Test Results

<table>
<thead>
<tr>
<th>Product</th>
<th>NSS Methodology Version</th>
<th>NSS-Tested Throughput</th>
<th>Breach Detection</th>
<th>TCO per Protected Mbps ($US)</th>
<th>NSS Labs SVM Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX-3400 (v7.1.6) and NX-4400 (v7.5.3)</td>
<td>Breach Detection Systems v2.0</td>
<td>750 Mbps</td>
<td>59.4%</td>
<td>$460</td>
<td>Caution</td>
</tr>
<tr>
<td>FireEye MPS (v6.2)</td>
<td>Breach Detection Systems v1.5</td>
<td>667 Mbps</td>
<td>94.5%</td>
<td>$374</td>
<td>Caution</td>
</tr>
</tbody>
</table>

Test methodologies are found on the NSS Labs website at www.nsslabs.com.

NSS-tested throughput for the NSS Labs Breach Detection Systems Methodology v1.5 was capped at 1,000 Mbps, and may not reflect the true maximum capabilities of the tested product.

TCO per Protected Mbps corresponds to single sensor costs over a 3-year period.

---

© 2015 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, e-mailed or otherwise disseminated or transmitted without the express written consent of NSS Labs, Inc. ("us" or "we").

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. “You” or “your” means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.

2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.

3. **NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.**

4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.

5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.