Co by vás mělo potkat na cestách za kybernetickou bezpečností

Milan Habrecht, Security account manager, Cisco Systems
ISSS Hradec Králové, 3.4.2017
Effective Security

simple  |  open  |  automated
The Results Speak for Themselves

~6.5 hours
Median time to detection with Cisco security

>100 days
Industry median time to detection

Source: Cisco Midyear Cybersecurity Report, 2016
Difference between a paperweight and a NGFW?

Threat Intelligence

- **Cisco Security Intelligence**
  - Global Visibility
  - Global Footprint

- **120TB** Security Intelligence
- **150,000** Micro-applications
- **13B** Web Requests
- **5B** Daily Email Connections
- **1.6M** Deployed Devices
- **93B** Daily Email Messages
- **150M** Deployed Endpoints
- **1,000** Applications
- **19.7B** Threats Blocked
- **35%** Enterprise Email
- **3-5 min** Updates
- **4.5B** Daily Email Blocks
- **1.1M** Sandbox Reports
- **75,000** FireAMP Updates
- **6,000** New Clam AV Sigs
- **14M** Deployed Access Gateway
- **13B** Web Requests
- **93B** Daily Email Messages
- **150M** Deployed Endpoints
- **1,000** Applications
- **19.7B** Threats Blocked
- **35%** Enterprise Email
- **3-5 min** Updates
- **4.5B** Daily Email Blocks
- **1.1M** Sandbox Reports
- **75,000** FireAMP Updates
- **6,000** New Clam AV Sigs
- **14M** Deployed Access Gateway

**Sandbox Reports**
NSS Labs Aug 2016 Breach Detection System Results (Cisco Firepower + AMP)

<table>
<thead>
<tr>
<th>Product</th>
<th>Detected &lt; 1 min</th>
<th>Detected &lt; 3 min</th>
<th>Detected &lt; 5 min</th>
<th>Detected &lt; 10 min</th>
<th>Detected &lt; 30 min</th>
<th>Detected &lt; 1440 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Software 13500</td>
<td>44.4%</td>
<td>75.9%</td>
<td>86.6%</td>
<td>97.4%</td>
<td>97.9%</td>
<td>99.4%</td>
</tr>
<tr>
<td><strong>Cisco Firepower 8120</strong></td>
<td><strong>67.0%</strong></td>
<td><strong>91.8%</strong></td>
<td><strong>96.3%</strong></td>
<td><strong>96.6%</strong></td>
<td><strong>97.1%</strong></td>
<td><strong>100.0%</strong></td>
</tr>
<tr>
<td>FireEye NX 10450 and EX 8420</td>
<td>0.6%</td>
<td>2.9%</td>
<td>6.5%</td>
<td>15.2%</td>
<td>85.8%</td>
<td>96.8%</td>
</tr>
<tr>
<td>Fortinet FortiGate 5000D</td>
<td>48.9%</td>
<td>88.7%</td>
<td>91.0%</td>
<td>95.6%</td>
<td>98.5%</td>
<td>99.4%</td>
</tr>
<tr>
<td>Fortinet FortiSandbox-3000D</td>
<td>46.2%</td>
<td>84.2%</td>
<td>88.4%</td>
<td>91.3%</td>
<td>93.1%</td>
<td>99.0%</td>
</tr>
<tr>
<td>Lastline Enterprise</td>
<td>5.5%</td>
<td>31.3%</td>
<td>47.8%</td>
<td>85.0%</td>
<td>96.9%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Palo Alto Networks 5020 – Inline Mode</td>
<td>7.3%</td>
<td>17.9%</td>
<td>27.6%</td>
<td>43.1%</td>
<td>76.4%</td>
<td>98.9%</td>
</tr>
<tr>
<td>Palo Alto Networks 5020 – Tap Mode</td>
<td>6.5%</td>
<td>17.1%</td>
<td>27.0%</td>
<td>42.5%</td>
<td>75.4%</td>
<td>90.1%</td>
</tr>
<tr>
<td>Trend Micro Deep Discovery 4000</td>
<td>3.6%</td>
<td>26.7%</td>
<td>66.2%</td>
<td>90.1%</td>
<td>94.0%</td>
<td>99.8%</td>
</tr>
</tbody>
</table>

Figure 5 — Breach Detection over Time (II)
## Competitive Threat Intelligence Comparison

<table>
<thead>
<tr>
<th></th>
<th>Palo Alto Networks (AutoFocus)</th>
<th>Check Point (ThreatCloud)</th>
<th>Fortinet (FortiGuard)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unique Malware Samples/Daily</strong></td>
<td>1.5M per day</td>
<td>10s of Thousands per day</td>
<td>10s of Thousands per day</td>
</tr>
<tr>
<td><strong>Email Messages Analyzed/Daily</strong></td>
<td>93B per day (86% are SPAM)</td>
<td>none</td>
<td>Not reported</td>
</tr>
<tr>
<td><strong>Total Threats Blocked Daily</strong></td>
<td>19.6B per day</td>
<td>Not reported: Likely 1000s</td>
<td>700K per day</td>
</tr>
<tr>
<td><strong>Categorized Web Blocks</strong></td>
<td>4.3B per day</td>
<td>Millions per day</td>
<td>Not reported</td>
</tr>
<tr>
<td><strong>Threat Data Processed</strong></td>
<td>120TB/day - 3.6PB per month (CWS)</td>
<td>Not reported</td>
<td>Not reported</td>
</tr>
<tr>
<td><strong>Contributing Users/Sensors</strong></td>
<td>150M (AC/AMP)/1.6M (IPS)</td>
<td>1000s</td>
<td>1000s of Gateways</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Free with Product</td>
<td>$35K per Seat</td>
<td>Free with Product</td>
</tr>
</tbody>
</table>
Our Integrated Approach is Unique
Our Architecture is Game-Changing
Cisco Security is Leapfrogging the Market

Simple, Effective, Integrated & Open Security
Thank you.