Fortinet Advanced Threat Protection- Part 4
Closing Off The #1 Targeted Attack Vector- EMAIL
Agenda

- Brief Recap on Breaches and the Need for Advanced Threat Protection
- Gartner Secure Email Gateway (SEG) Requirements
- Overview of FortiMail (SEG)
- A Closer Look at FortiMail and FortiSandbox Together
- Final Thoughts
Brief Recap
The Problem: Breaches, Breaches and More Breaches

- **2014**: 79,790 security incidents
- **2015**: CEOs, CIOs and CISOs who resigned

All organizations should now assume that they are in a state of continuous compromise.

— Gartner, 2/14/14

Sources:
Verizon 2015 Data Breach Investigations Report, April 2015
This is Fortinet Advanced Threat Protection (ATP)

**Known Threats**
- Reduce Attack Surface
- Inspect & Block Known Threats

**Unknown Threats**
- Identify Unknown Threats
- Assess Behavior & Identify Trends

**Response**
- Identify scope
- Mitigate impact

---

**Prevent**
- FortiGate
  & everything that can enforce a security policy

**Detect**
- FortiSandbox
  & everything that is behavior based

**Mitigate**
- FortiGuard
  teams and automation

---

**Hand off:**
- **High risk items**
- **Creating a fix & update prevention**
- **Provide ratings & results**
How To Move From Detection/Response To Prevention?

- **Random Detection**: (average 229 days, prior to response)

- **Sandbox Only**: Detection & Response (days)

- **Sandbox + NGFW/WAF**: Detect & Respond (minutes)

- **Sandbox + SEG/EPP**: Prevention (0-second)
The $20bn Opportunity

- Endpoint ($4.6bn)
- WAF ($800m)
- NGFW/UTM ($8.5bn)
- Sandbox ($2bn)
- SEG ($2bn)
- SWG ($2bn)
Integrating a Secure Email Gateway with Sandbox

1. Email is a top vector of targeted attack
2. No one notices small email delay
3. It’s better to prevent than just detect
Sales Motion: Add SEG + Sandbox

- Director favored FireEye
- Fortinet won with:
  - Better detection
  - FortiGate/FortiMail integration
  - Flexible deployment options

DEAL INFORMATION

This was a highly competitive proof of concept where the Director of Security favored FireEye because he had used them in a previous job. What enabled us to win was our better detection rates, our integration with FortiGate and FortiMail, our highly competitive price and our flexible deployment options.

By introducing FortiMail into the opportunity it allowed us to expand the deal size, while providing automatic detection and mitigation of Phishing and SPAM, something that their Cisco Ironport solution was not doing effectively.

The fact that they already had FortiGate infrastructure was also crucial, as these devices automatically became sensors at all their ingress/egress points, eliminating the cost of purchasing new sensors at every location.
Global 500 financial firm, ~10,000 employees

FireEye kicked out for low-balling

Fortinet won with:
  » Mature solution, high effectiveness
  » Consolidated functions
  » Integration with Fortinet and partner products

DEAL INFORMATION

What’s particularly pleasing about this deal is that, although it’s not an existing FortiGate customer, being currently a Check Point & Cisco firewall house (for now), this deal wasn’t an upsell, rather the insertion point into the customer was created with FortiSandBox & FortiMail – and we now aim to upsell some FortiGates!

Over the past 12 months, the customer has been the target of sustained malware campaigns via e-mail – something they attribute to an increase in high profile sponsorships such as ...

They use McAfee E-mail Gateway which has missed many threats resulting in an average of 10 PCs per day becoming infected, risking sensitive information being stolen. The PCs had to be rebuilt which created a lot of disruption and bad internal PR for the IT team.

The team consulted with Gartner and their integration partners about their options, shortlisting 6 vendors they wished to explore further. HP Tipping Point was one, Check Point and Trend were not taken forward after their initial investigations as ______ found neither solution was mature enough. FireEye was ruled out after they were deemed to have low-balled their initial sizing, causing trust issues.

Features ______ likes about the Fortinet solution include 1) Easy integration with Splunk, 2) Capture rate, 3) The ability to scan file shares, 4) on-demand uploading of suspicious files, and 5) the ability to integrate with FortiGate and FortiClient in the future – opening up a new upsell opportunity for us.
Sales Motion: Net New NGFW+ SEG + Sandbox

- FireEye was dismissed due to the distributed environment.
- FortiGate + FortiSandbox stopped spearphishing
- FortiMail integration is first in 2016.

DEAL INFORMATION/WHY WE WON?

Customer recently underwent a network security refresh which included implementing FortiGates at both their core and branch locations. However, while they had a solid network security solution in place, we helped them to realize that they needed an additional layer to fill the gap that is advanced/targeted threats.

As a result of the need to meet their compliance goals (with the help of a security audit), this project ramped up very quickly. Fortinet had been engaged throughout, but FireEye was quickly brought in (and dismissed for that matter) to the conversations. FireEye was deemed not an option due to the distributed nature of their environment.

Two days after making the purchase, the FortiSandbox helped stop a nasty spear-phishing attack that their e-mail solution let into the environment. As a result, customer immediately recognized that this solution is starting to generate ROI for them. ..... The FortiMail/FortiSandbox integration is already one of the first projects for 2016.
Gartner Secure Email Gateway Requirements
Email Security Requirements

- Email handling
  - MTA, rate control, address rewriting...

- Threat protection
  - Anti-spam, anti-malware, anti-phishing
  - Optional sandboxing

- Data protection
  - DLP, encryption, fingerprinting, workflow
  - Optional Email archiving

- Administration
  - Role-based administration
  - Central quarantine/end user digest
  - Optional newsletter handling

- More for service providers
  - White label, end user self-service…
Email Security Requirements

- Email handling
  - MTA, rate control, address rewriting...

- Threat protection
  - Anti-spam, anti-malware, anti-phishing
  - Optional sandboxing

- Data protection
  - DLP, encryption, fingerprinting, workflow
  - Optional Email archiving

- Administration
  - Role-based administration
  - Central quarantine/end user digest
  - Optional newsletter handling

- More for service providers
  - White label, end user self-service...

The penetration rate of commercial SEG solutions is close to 100% of enterprises...Ancillary services, such as targeted attack prevention, data loss prevention and encryption, are the main drivers of growth, while traditional spam and virus-filtering subscription costs are flat to slightly down.”

—Gartner
Overview of FortiMail Secure Email Gateway
FortiMail - Top rated. High performance. All-in-one.

- A consolidated solution to prevent threats and data loss in a single high performance appliance for all segments
  - Top-rated threat protection
  - Integrated data protection
  - Enterprise class/service provider management
  - High performance physical/virtual appliances
  - Powered by FortiGuard Labs

Independent Validation

FortiGuard Threat Research
#1 Highly accurate and effective antispam “cocktail”

Connection Level Filtering:
Discard spam as early as possible for greatest performance.

Header Filtering:
Verify valid destination.
Support for latest RFCs.

Full Content Filtering:
Examine message body, including attachments, images, text, etc.
#2- Powerful Antimalware, more than signature matching

**File Sample**

- Signature Match (CPRL/Checksum)
- Decryption/unpacker System
- Behavior Analysis
- Code Emulator

**Anti-malware**
- One-to-many signature matching
- Heuristic engine
- Unpacker/decryption
- Code emulation

**Take Action Based on Profiles**

File discarded, option to Quarantine and event logged
Key Driver: Integration with NSS Recommended sandbox

- Hold for and act upon result
- Block previously unknown attacks
- Leverage granular policy controls
Key Driver: Integrated Data Protection

- **Data loss prevention**
  - Preset dictionaries for easy policy creation
  - Smart identifiers for high accuracy
  - Covers HIPAA, GLBA, SOX, PCI and more

- **TLS & S/MIME Encryption**

- **Identity Based Encryption**
  - No additional license required
  - No encryption key exchange, minimal key management

- **Sender or policy-based trigger**
#3: Low administration quarantine and end user controls

- **Central quarantine**
  - Easy administration
  - Can be consolidated across devices

- **Self-service personal quarantine digest**
  - Sender and subject
  - Release or delete links

- **Automatic tagging and delivery**
  - Newsletter and junk categories
  - Client filters to appropriate folder
Integrated email archiving

- Per mailbox policy based archiving:
  - Sender/recipient
  - Subject/body/attachment filename keywords
- IMAP archive access
- Remote archival support

Comply with regulatory obligations
#4: Managed Security Service Provider-ready

- **MSSP Service Framework**
  - FortiMail White Labelling
  - Multi Domain support with per domain quotas
  - Mass provisioning for lower OPEX
  - Delegated administration
  - User self service

**Mail Security Service Provider in a box!**
FortiGuard-powered security services

- Global FortiGuard Labs
  - 200+ threat researchers
  - Automated analysis of millions of messages per day
  - Proactively discovers zero day threats and tracks global botnets

Security experts working for you 24x7!
### FortiMail Physical and Virtual Appliances

<table>
<thead>
<tr>
<th>Email Routing (Msgs/hr)*</th>
<th>FML-60D</th>
<th>FML-200D</th>
<th>FML-400C</th>
<th>FML-1000D</th>
<th>FML-3000D</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>150k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>680k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1,200k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AS+AV Perf. (Msgs/hr)*</th>
<th>FML-VM00</th>
<th>FML-VM01</th>
<th>FML-VM02</th>
<th>FML-VM04</th>
<th>FML-VM08</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>120k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>500k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1,000k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: Performance numbers are for physical appliances only. Domain capacity is common for physical and virtual appliances.
FortiMail- FortiSandbox Demonstration
Additional Resources

- Partner Portal: https://partners.fortinet.com/FortiPartnerPortal/fortipp/login.jsp
- NSE Training: http://www.fortinet.com/training/certifications/
Final Thoughts

- Top-rated Spam, Virus, Phishing Protection
- Top-rated Integrated Sandbox
- Integrated Data Protection
- Available in all Form Factors
- Part of a Broader ATP solution
Thank you.