Importance of having a Integrated Security Fabric
Sandbox-Mail-Client-Web-Firewall-SIEM

David Leinberry - ATP Product Specialist - Fortinet
Brian Foote - ME Vets Home - Network Admin
Mike Mokos - ATP Engineer - Fortinet
Industry Information

- Estimated **$400 Billion** a year of Intellectual Property (IP) is Stolen: Lloyds of London, *Time* 1-2-17

- 300% + in Ransomware, W2 - CEO fraud, 460k comp infected - $5.3 Bill – KnowBe4/ MS / FBI 2/18

- 70% of Businesses Attacked Pay Ransomware; IBM study, 12-15-16

- The Average incursion: **186 days** without detection – Verizon Breach Report; 4/16

- **Phishing**/Social Engineering - still responsible for **90%** of data breaches
  last 10 years – BankInfoSecurity/Verizon, 3-6-17

- AV detection performance in decline; by 5% – Virus Bulletin 1/17

Gartner Group: “signature based detection will be a commodity, you need real time detection” like a sandbox. 3/14
AV detection rates in Decline - Virus Bulletin (VB) - December 2016

RAP averages quadrant
Jun - Dec 2015

RAP averages quadrant
Apr - Oct 2016

Chart includes only those products with two or more qualifying results during the period covered.

- **64,199 incidents**
- **2,260 breaches**
- **CEOs, CIOs and CISOs who resigned**

All organizations experienced a data breach, ranging from approx 2,600 to 100,000 compromised records.

---

**Sources:**
- Verizon April 2016 Data Breach Investigations Report,
- IBM / Ponemon Institute© Breach Report June 2017

---

### Incidents

<table>
<thead>
<tr>
<th>Industry</th>
<th>Total</th>
<th>Small</th>
<th>Large</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation (72)</td>
<td>90</td>
<td>140</td>
<td>79</td>
<td>143</td>
</tr>
<tr>
<td>Administration (56)</td>
<td>44</td>
<td>6</td>
<td>3</td>
<td>55</td>
</tr>
<tr>
<td>Agriculture (91)</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Construction (123)</td>
<td>9</td>
<td>0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Educational (61)</td>
<td>254</td>
<td>18</td>
<td>20</td>
<td>216</td>
</tr>
<tr>
<td>Entertainment (77)</td>
<td>2,707</td>
<td>18</td>
<td>1</td>
<td>2,688</td>
</tr>
<tr>
<td>Finance (62)</td>
<td>1,268</td>
<td>20</td>
<td>121</td>
<td>1,227</td>
</tr>
<tr>
<td>Healthcare (62)</td>
<td>146</td>
<td>21</td>
<td>25</td>
<td>90</td>
</tr>
<tr>
<td>Information (59)</td>
<td>1,028</td>
<td>18</td>
<td>28</td>
<td>792</td>
</tr>
<tr>
<td>Management (58)</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Manufacturing (31-33)</td>
<td>171</td>
<td>7</td>
<td>61</td>
<td>103</td>
</tr>
<tr>
<td>Mining (21)</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>Other Services (81)</td>
<td>17</td>
<td>6</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Professional (25)</td>
<td>916</td>
<td>34</td>
<td>9</td>
<td>883</td>
</tr>
<tr>
<td>Public (23)</td>
<td>47,337</td>
<td>6</td>
<td>44,973</td>
<td>258</td>
</tr>
<tr>
<td>Real Estate (69)</td>
<td>11</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Retail (44-45)</td>
<td>159</td>
<td>102</td>
<td>20</td>
<td>37</td>
</tr>
<tr>
<td>Trade (42)</td>
<td>18</td>
<td>0</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>Transportation (28-43)</td>
<td>31</td>
<td>1</td>
<td>6</td>
<td>24</td>
</tr>
<tr>
<td>Utilities (22)</td>
<td>24</td>
<td>0</td>
<td>3</td>
<td>21</td>
</tr>
<tr>
<td>Unknown</td>
<td>9,653</td>
<td>113</td>
<td>1</td>
<td>9,532</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>94,139</td>
<td>621</td>
<td>47,408</td>
<td>16,270</td>
</tr>
</tbody>
</table>

### Breaches

<table>
<thead>
<tr>
<th>Industry</th>
<th>Total</th>
<th>Small</th>
<th>Large</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation (72)</td>
<td>90</td>
<td>140</td>
<td>79</td>
<td>143</td>
</tr>
<tr>
<td>Administration (56)</td>
<td>44</td>
<td>6</td>
<td>3</td>
<td>55</td>
</tr>
<tr>
<td>Agriculture (91)</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Construction (123)</td>
<td>9</td>
<td>0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Educational (61)</td>
<td>254</td>
<td>18</td>
<td>20</td>
<td>216</td>
</tr>
<tr>
<td>Entertainment (77)</td>
<td>2,707</td>
<td>18</td>
<td>1</td>
<td>2,688</td>
</tr>
<tr>
<td>Finance (62)</td>
<td>1,268</td>
<td>20</td>
<td>121</td>
<td>1,227</td>
</tr>
<tr>
<td>Healthcare (62)</td>
<td>146</td>
<td>21</td>
<td>25</td>
<td>90</td>
</tr>
<tr>
<td>Information (59)</td>
<td>1,028</td>
<td>18</td>
<td>28</td>
<td>792</td>
</tr>
<tr>
<td>Management (58)</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Manufacturing (31-33)</td>
<td>171</td>
<td>7</td>
<td>61</td>
<td>103</td>
</tr>
<tr>
<td>Mining (21)</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>Other Services (81)</td>
<td>17</td>
<td>6</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Professional (25)</td>
<td>916</td>
<td>34</td>
<td>9</td>
<td>883</td>
</tr>
<tr>
<td>Public (23)</td>
<td>47,337</td>
<td>6</td>
<td>44,973</td>
<td>258</td>
</tr>
<tr>
<td>Real Estate (69)</td>
<td>11</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Retail (44-45)</td>
<td>159</td>
<td>102</td>
<td>20</td>
<td>37</td>
</tr>
<tr>
<td>Trade (42)</td>
<td>18</td>
<td>0</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>Transportation (28-43)</td>
<td>31</td>
<td>1</td>
<td>6</td>
<td>24</td>
</tr>
<tr>
<td>Utilities (22)</td>
<td>24</td>
<td>0</td>
<td>3</td>
<td>21</td>
</tr>
<tr>
<td>Unknown</td>
<td>9,653</td>
<td>113</td>
<td>1</td>
<td>9,532</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>94,139</td>
<td>621</td>
<td>47,408</td>
<td>16,270</td>
</tr>
</tbody>
</table>
Audience Poll #1

What do you think the average cost of a data breach was in 2017?

A. $411k
B. $3.62m
C. $1.2b
D. $162m
E. $141
Data Breach Cost Data Points

Data Breach Cost - Cost of Data Breach study conducted by Ponemon Institute
This year’s study reports the global average cost of a data breach is down 10 percent over previous years to **$3.62 million**.

The average cost for each lost or stolen record containing sensitive and confidential information also significantly decreased from $158 in 2016 to **$141** in this year’s study.

Target Says Credit Card Data Breach Cost It $162M In 2013-14

*Posted Feb 25, 2015 by Ingrid Lunden (@ingridlunden)*

What are you most concerned about losing as result of a cyber attack?

- Customer Data
- System Availability/Business Continuity
- Intellectual Property
- Employee Data
- Company Brand
Why a Sandbox?

- To provide a pristine & isolated environment that automatically tests potentially malicious software
  - FortiTrace executes the file just like a human would (double click)
  - FSA steps through the file, opens other programs as need to execute it (Office, Adobe, etc.)
  - If a GUI is opened we screen shot the malware install
  - Call back/C2 is tracked
  - A forensics report is created and email weekly to the pre-defined alias list
- After testing intelligence is applied in deciding to alert or block software and network behavior
- Multiple VM in a single appliance allows for multiple files and threats to be analyzed at once
- Integrated with multiple Fortinet Security Platforms: Firewall-Mail-Client-SIEM-Web
- Integration with all major SIEMs and Log Aggregation tools
FortiSandbox – 5 Steps to Enhance Security

- **Call Back Detection**: Quickly simulate intended activity – Fortinet patented CPRL
- **Full Virtual Sandbox**: Examine real-time, full lifecycle activity in the sandbox to get the threat to expose itself
- **Code Emulation**: OS independent & immune to evasion – high catch rate
- **Cloud File Query**: Check community intelligence & file reputation
- **AV Prefilter**: Apply top-rated anti-malware engine

- Identify the ultimate aim, call back & exfiltration
- Mitigate w/ analytics & FortiGuard updates

9
14 Types of Danger and some examples

- **Adware**
  - BitTorrent

- **Riskware**
  - smsreg

- **Botnet**
  - Fastflux

- **Hijack**
  - Trovi

- **Trojan**
  - CryptoLocker 40 Variants.
  - CyberheistNews 6-20-16:
    “Over 100+ different strains of Ransomware & the end is not in sight”.

- Worm
- Backdoor
- Rootkit
- Dropper
- Downloader
- Injector
- Attacker
- Stealer
- Infector
FortiSandbox Protocol Details

1. Protocol support
   - **FortiGate Integrated:** HTTP, SMTP, POP3, IMAP, MAPI, FTP, SMB, IM and SSL encrypted equivalents
   - **Stand-alone:** HTTP, FTP, POP3, IMAP, SMTP, SMB
   - **FortiMail Integrated:** SMTP
   - **FortiClient Integrated:** All

2. File type support
   - **AV Prefilter:** all
   - **Full Sandbox:** as follows
     - Archived: .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj
     - Executable: PE, .dll, .scr
     - File: PDF, Office, SWF, Google APKs
     - URLs

3. Operating Environment
   - **Code emulation:** OS-independent
   - **Sandbox:** Windows 7, 8, 10, Android, IE, Adobe, Office 2007, 2010, 2016
   - **Mac OS – OSX in the cloud**
   - **Custom VM**
Flexible Deployment Modes

Flexible Deployment Options
- Offers most suitable implementation depends on requirements and infrastructure
- Allow protection of investment by allowing different deployment modes as requirement changes
- Full automatic Mitigation and blocking with the addition of FortiMail, FortiWeb and soon FortiGate
All Input Methods Supported Simultaneously

- **Devices / Client**
  - Files/URLs submitted by Fortinet products

- **Sniffer / TAP**
  - File extraction from monitored traffic

- **On-Demand**
  - Files or URLs manually submitted in GUI

- **File Shares – NFS / CIFS**
  - Files are examined on a network share

- **Adaptors / ICAP**
  - Files submitted by other security vendors
Breaking the Kill Chain of Advanced Threats

- Spam
- Malicious Link
- Exploit
- Malware
- Bot Commands & Stolen Data

Anti-spam

Web Filtering

Intrusion Prevention

Antivirus

App Control/ IP Reputation

Spam
Malicious Link
Exploit
Malware
Bot Commands & Stolen Data

Command & Control Center

Malicious Email
Malicious Web Site
URL
Breaking the Kill Chain of Advanced Threats

- Spam
- Malicious Link
- Exploit
- Malware
- Bot Commands & Stolen Data
- Anti-spam
- Web Filtering
- Intrusion Prevention
- Antivirus
- App Control/ IP Reputation
- Spam
- Malicious Link
- Exploit
- Malware
- Bot Commands & Stolen Data
- sandbox
- Malicious Email
- Malicious Web Site
- Command & Control Center
How Does It All Work?

- **FortiGuard Labs**
  - Security Updates

- **FortiSandbox**
  - Real-time intelligence updates
  - Intelligence Sharing

- **FortiGate/FortiMail/FortiWeb**
  - Block Objects
  - Quarantine Devices/Block Traffic

- **FortiClient**
  - Forensics and Response
  - Device/File Quarantine

1. File Submission/Result
2a. Block Objects
2b. Quarantine Devices/Block Traffic
3a. Real-time intelligence updates
3b. Intelligence Sharing
4. Security Updates
1. File Submission/Result
Solutions tested:
- Fortinet - 2000E appliance
- Check Point – NGTX App R7730
- Lastline – v7.25
- Trend Micro – Model 4000 v12.0
- Cisco – FirePower 8120 v6

Below average detection:
- FireEye – NX 10450, v7.9.2
- FireEye – EX 8400 v7.9.2
- FireEye – Net Sec 6500NXES
Number of vendors that publish their Zero Day Rates? 2!

Fortinet is one of only two companies in the security space that publish their true Zero Day detection rates!

http://fortiguard.com/zeroday - FG - labs zero day detection rate up to 541 in the last 12 years. 5/18

https://www.fireeye.com/current-threats/recent-zero-day-attacks.html - FireEye Zero Day detection rates up to 30 in the last 5 years

You may want to ask why and bring that up to the customer and or the other security vendors.
FortiClient
Ensures protection against application level of denial of service attacks
Secures against malicious websites, undesirable applications, client targeting attacks and malware along with Secure Remote Access
Centralized policy management and offers a single pane of glass for your security configuration, logging and reporting

FortiAnalyzer, FortiManager
FortiWeb
Prevents web application attacks against your critical web assets
FortiSwitch
Secures Access Switching and Increases productivity for next generation applications through faster network access speeds

FortiWeb
Servers
Prevents web application attacks against your critical web assets

FortiMail
Secures against email threats and prevents SPAM and virus attacks from reaching your users

FortiGate
Secures against malicious websites, undesirable applications, client targeting attacks, and malware

FortiDDoS
Ensures protection against application level of denial of service attacks

FortiADC
Ensures WAN link redundancy and provides inbound GSLB

FortiSandbox
Detonates malware and detects zero-day and advanced attacks.
Prevents organization from making the news.

FortiAuthenticator
Identifies users wherever they are, and enforces strong authentication

FortiToken
Provides secure, scalable wireless access to your users leveraging native firewalling on FortiOS

FortiSIEM
Integrated Security, Performance, and Availability Monitoring in One Application

FortiGuard
Our FortiGuard Labs’ global research team continuously monitors the evolving threat landscape. More than 300+ researchers provide around the clock coverage to ensure your network stays protected. They deliver rapid product updates and detailed security knowledge to provide protection from the latest threats.
What does a SIEM do?

Consolidate, Correlate, Analyze

(SIEM) Security Incident and Event Management
  Log Management
    real time & historic queries
  Reporting
  Compliance

(PAM) Performance & Availability Monitoring
  Devices: Routers, switches, firewalls, servers, storage
  Cloud: Applications, hosted servers
  Enterprise Applications
  Users: LDAP, Active Directory
  Metrics: Up/Down, Utilization, throughput, statistical baselines, more...
  Configuration
  Change
  Compliance

Cross – domain - Analytics, Forensics, Correlation
Current Market – IT Network Challenges

**Physical Infrastructure**
- Physical Switches
- Physical Servers

**Virtual Infrastructure**
- Virtual Networks
- Virtual Servers

**Cloud Infrastructure**
- Public Cloud
- Private Cloud
- Hybrid Cloud

**Mobility/BYOD**
- Thousands of Devices
- Hundreds of Apps
- Deployed Generating Billions of Events per day and PBs of Data

Hybrid Cloud
FortiSIEM Architecture: Enterprise / MSP – Multi-Tenancy

Supervisor

CMDB
SVN / Config
Report Server (Visual Analytics)

Worker(s)

Cluster

NFS
Event Storage

Supervisor

Collector(s)

Customer 1

Firewalls, Routers, Storage, Servers, Apps

Customer 2

Firewalls, Routers, Storage, Servers, Apps

Main Data Ctr. / HQ
Public / Private / Hybrid

Remote Network(s)
Public / Private / Hybrid
Database scalability limited due to Oracle database stack, plus the fact that a separate log management appliance is required.

- Extremely expensive to buy and maintain
- Scalability — unable to handle high log volume
- Clunky hierarchical log collection architecture — cannot analyze all logs from one place
- Windows appliance — not cloud ready
- Low end standalone SIEM product offering built through acquisition
- Purchase of many add-on products required for same level of functionality

**Competitive Analysis — Why we win**
Fortinet

- Founded: 2000
- IPO: 2009
- $1.5B Cash
- 30%+ Growth
- Headquarters: Sunnyvale, CA
- 100+ Offices Worldwide
- 5,000+ Employees
- 340,000+ Customers
- 460+ Patents
- 243+ Pending
- Over 3.6 Million Devices Shipped
- #1 Unit Share Worldwide (IDC)
- 542 Zero Days detected in last 12 years
- Market Leading Technology

Fortinet is a leader in next-generation security solutions, providing comprehensive protection across the enterprise network. Fortinet’s suite of products and services is designed to meet the needs of today’s complex and dynamic security landscape. With a focus on innovation and industry-leading technology, Fortinet is dedicated to helping organizations protect against cyber threats and ensure business continuity.
Security Services and Technologies

- Antivirus
- Application Control
- Anti-spam
- IPS
- Web App Filtering
- Vulnerability Management
- IP Reputation
- Mobile Security
- NEW Firewall
- VPN
- Application Control
- IPS
- Web Filtering
- Anti-malware
- WAN Acceleration
- Data Leakage Protection
- Wi-Fi Controller
- Advanced Threat Protection