Advanced Threat Protection Framework:

What it is, why it's important and what to do with it

Doug Manger, Senior Security Engineer
dmanger@fortinet.com

FORTINET®

High Performance Network Security

Agenda

- Security Concepts
- Common elements of sophisticated attacks
- Key technologies and services recommended to address each element
- How they can all fit together as part of a cohesive security framework
- Additional learning resources
- Q&A

Security Concepts

1. **What is a Botnet and/or C&C?**
2. What is an “Advanced Persistent Threat”?
3. What is “Sandboxing”?
4. What is a Next Generation Firewall (NGFW)?
5. What is a security framework?
6. What are your security plans?

Question 1: What is a “Botnet” and/or “C&C”?

A “botnet” is network of computers that have been compromised with malware. Botnets are normally leveraged by command and control (C&C) servers to execute distributed attacks.

Examples:

- *Mariposa*
- *Conficker*
- *Zeus*
- *BredoLab*

Security Concepts

1. What is a Botnet and/or C&C?
2. **What is an "Advanced Persistent Threat"?**
3. What is "Sandboxing"?
4. What is a Next Generation Firewall (NGFW)?
5. What is a security framework?
6. What are your security plans?

Question 2: What is an “Advanced Persistent Threat”?

An “Advanced Persistent Threat” is a sophisticated, sustained, long-term attack/breach that remains undetected. An ATP is regularly executed against businesses and or nations for financial or political reasons. ATPs are of paramount concern for all organizations due to the grave impact they present.

Examples:

- *Heartbleed*
- *Shellshock*
- *Stuxnet*
- *Poodle*

Security Concepts

1. What is a Botnet and/or C&C?
2. What is an “Advanced Persistent Threat”?
3. **What is “Sandboxing”?**
4. What is a Next Generation Firewall (NGFW)?
5. What is a security framework?
6. What are your security plans?

Question 3: What is “Sandboxing”?

“Sandboxing” is the isolation and relegation of malware and/or other nefarious payloads in a virtualized operating system so as to limit/stop their propagation within an environment.

Sandbox components:

- *Isolated, Virtual Operating Systems*
- *Extensive threat detection engine*
- *Expedient, but thorough inspection*
- *Dedicated security services backend*
- *Cost-effective*

Security Concepts

1. What is a botnet and/or C&C?
2. What is an “Advanced Persistent Threat”?
3. What is “Sandboxing”?
4. **What is a Next Generation Firewall (NGFW)?**
5. What is a security framework?
6. What are your security plans?

Question 4: What is a “Next Generation Firewall” (NGFW)?

A “Next Generation Firewall” is a secure, multi-faceted network platform that adds a variety of filtering functions to the common firewall. This includes:

- Web Content Filtering
- Application Visibility/Control
- Intrusion Detection/Prevention
- Data Loss Prevention
- Anti-Virus/Spam
- Deep Inspection for SSL/SSH

Security Concepts

1. What is a botnet and/or C&C?
2. What is an “Advanced Persistent Threat”?
3. What is “Sandboxing”?
4. What is a Next Generation Firewall (NGFW)?
5. **What is a security framework?**
6. What are your security plans?

Question 5: What is a security framework?

A security framework is a layered management tool that defines the practices that are required for an organization maintain its highest possible level of security.

Components:

- *Access Control*
- *Threat Detection/Prevention*
- *Incident Response*
- *Continuous Monitoring*
- *Continuous Learning*

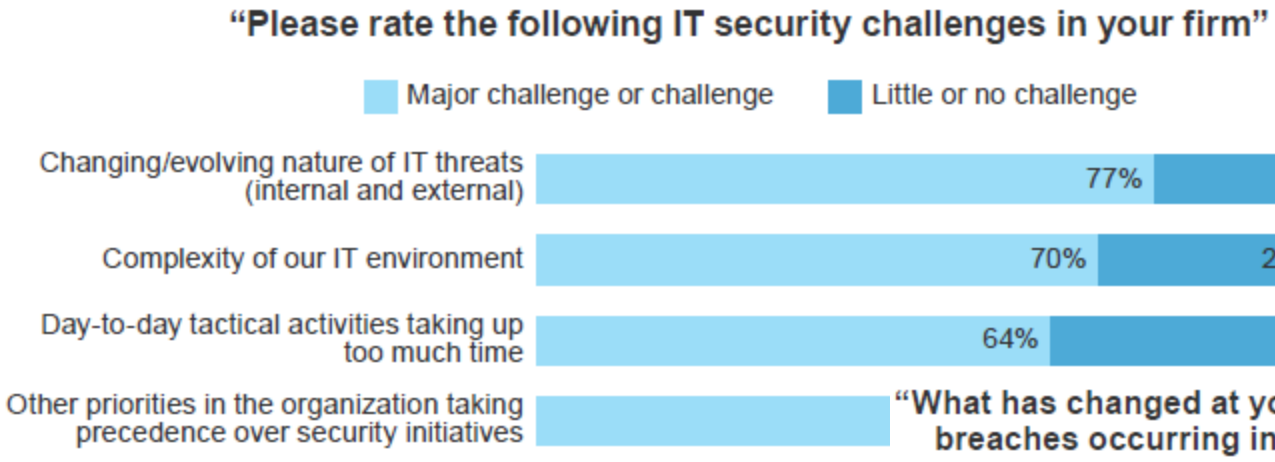
Security Concepts

1. What is a botnet and/or C&C?
2. What is an “Advanced Persistent Threat”?
3. What is “Sandboxing”?
4. What is a Next Generation Firewall (NGFW)?
5. What is a security framework?
6. **What are your security plans?**

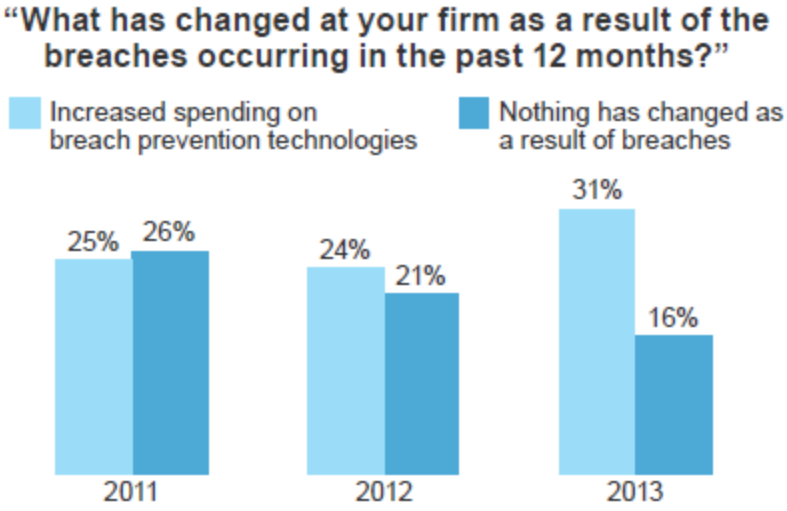
Question 6: Do you have an active project in the next 6 months to increase security from advanced malware/sophisticated threats?

- Yes, I have a firewall upgrade project to move to NGFW
- Yes, I have a new project to deploy a stand-alone “sandbox”
- Yes, I have another type of project designed to increase security
- No, but I do have such a project later this year
- Not at this time/unsure

Advanced Malware/Sophisticate Threats a Top Concern



Base: 282 network security professionals
Source: Forrsights Security Survey, Q2 2013, Forrester Research, Inc

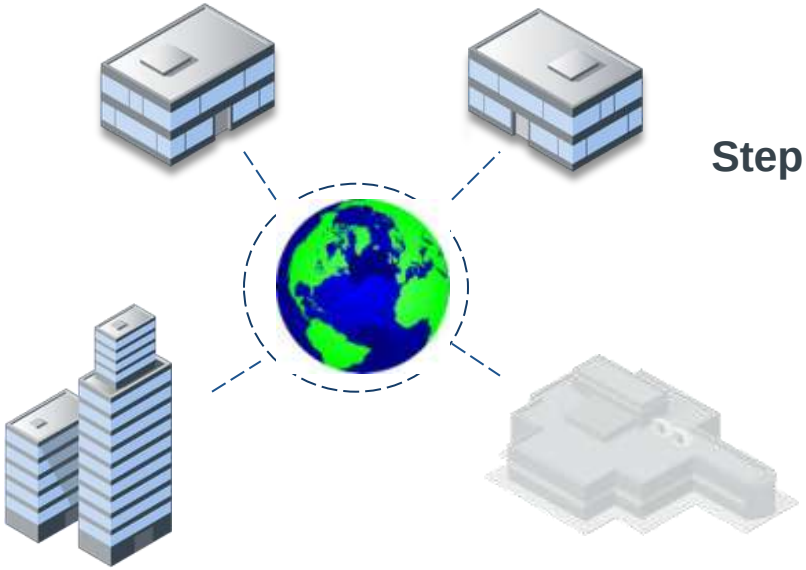


Base: varied counts of network security professionals
Source: Forrsights Security Survey, Q2 2013, Forrester Research, Inc

Microsoft Security Advisory 2963983- IE Vulnerability

Cybercriminal

Step 1: email links to malicious page
page exploits vulnerability to run code

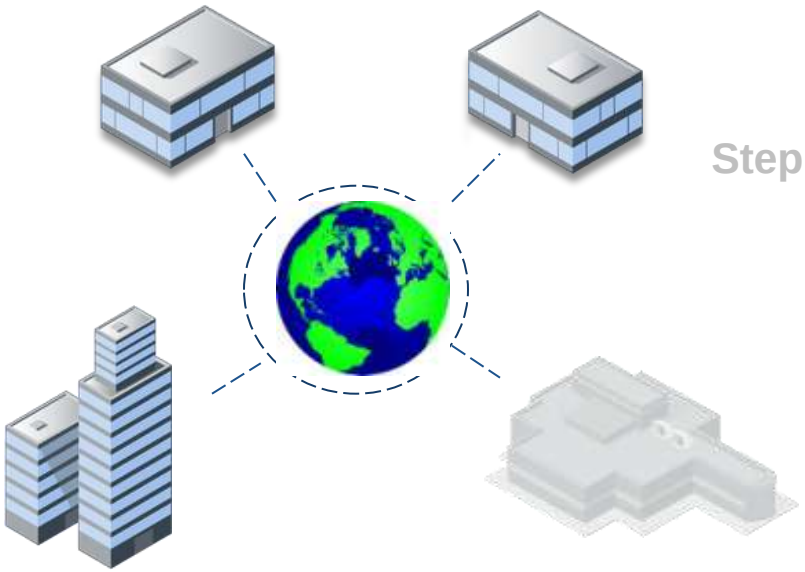


Step 2: code reaches out to download URL
file enters network and installs

Microsoft Advisory 2963983- Security Recommendations

Cybercriminal

Step 1: email links to malicious page
page exploits vulnerability to run code



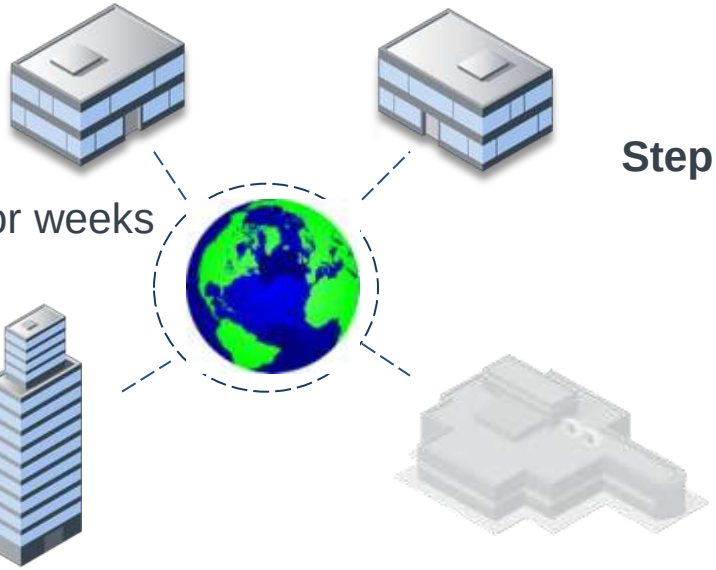
Step 2: code reaches out to download URL
file enters network and installs

- Don't use IE/Flash
- Turn on MSFT EMET
- Update IPS to prevent exploit
- Update web filter to block site
- Patch when available

Target Data Breach

Cybercriminal

Step 1: steal vendor credentials to access network



Step 2: access PoS to install code

Step 5: continue for weeks

Step 4: stage and deliver to ftp

Step 3: seek out other data, including “guest” db

Target Data Breach- Security Recommendations

Cybercriminal

Step 1: steal vendor credentials to access network

- Require 2FA

Step 2: access PoS to install code

Step 5: continue for weeks

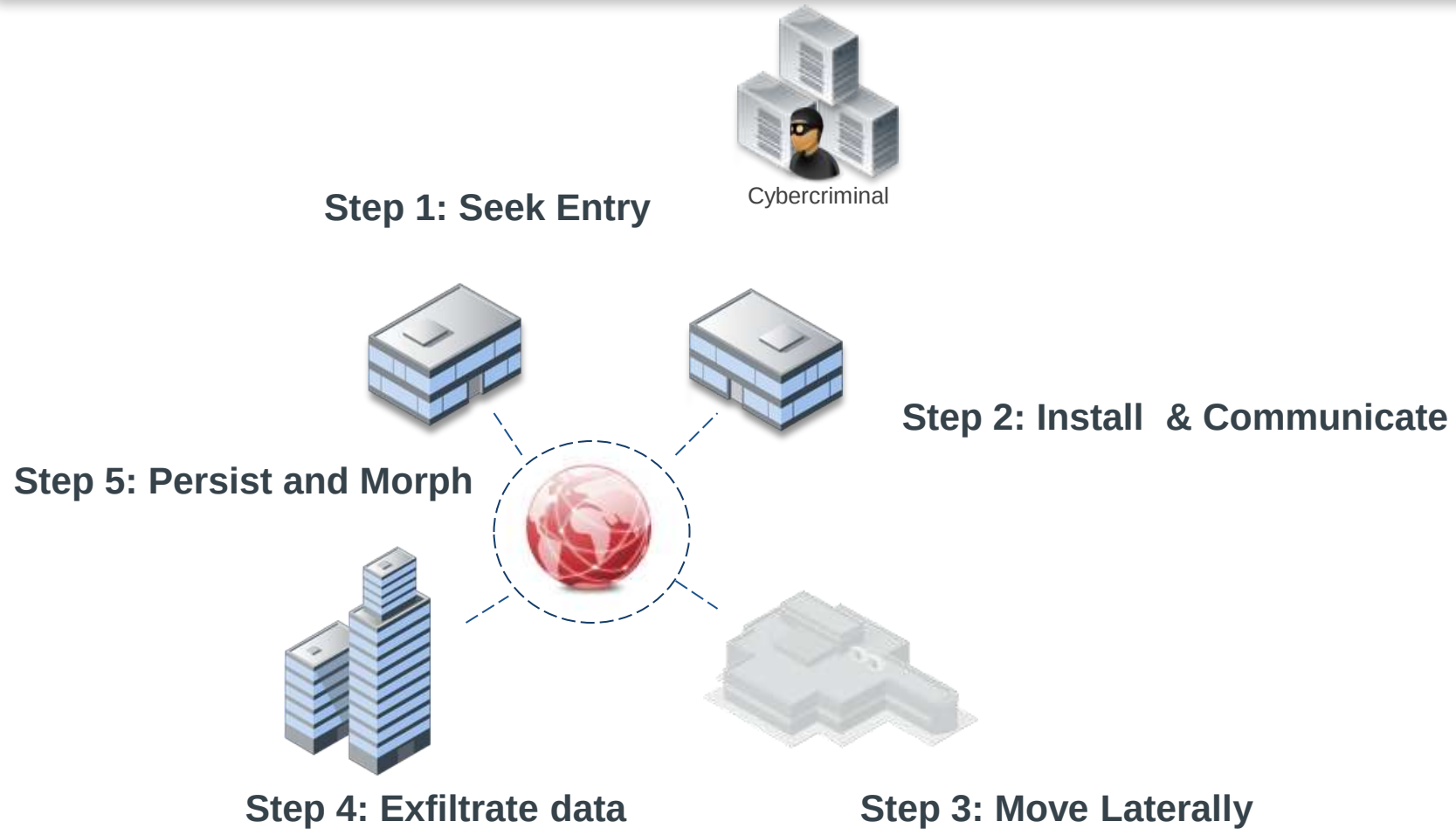
- DLP
- C&C blocking
- Advisories

- Deeper inspection/ Advanced detection

Step 4: stage and deliver to ftp

Step 3: seek out other data, including “guest” db

At a fundamental level, there are key commonalities

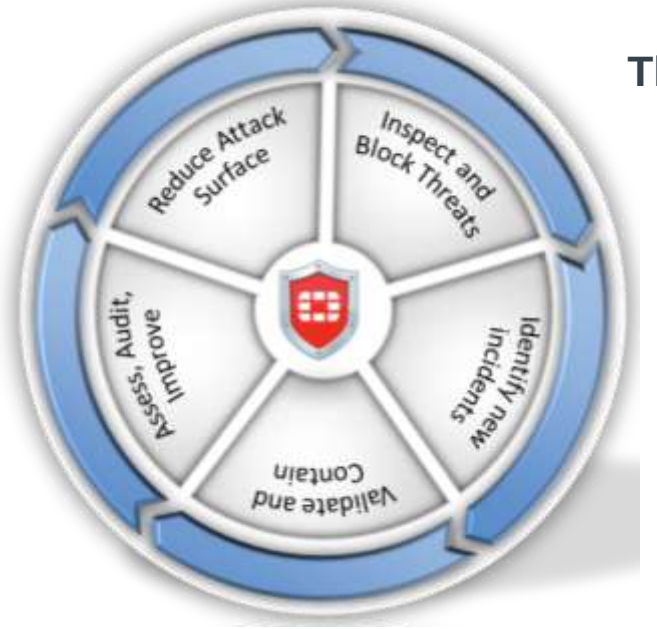


Fortinet Recommends a Cohesive Approach

Cybercriminal

Access Control

Threat Prevention



Continuous Monitoring

Threat Detection

Incident Response

Applying the Framework- IE Vulnerability

Continuous Monitoring

Incident Response

Threat Prevention

Access Control

- Stay abreast of the threat landscape
- Don’t use IE/Flash
- Turn on MSFT EMET
- Update IPS to prevent exploit
- Update web filter to block site
- Patch when available

Applying the Framework- Target Corporation Data Breach

Access Control

Threat Prevention

Threat Detection

Incident Response

Continuous Monitoring

- Require 2FA
- Perform deeper inspection
- Block C&C
- Deploy DLP
- Perform advanced detection
- Be prepared to respond
- Monitor advisories/landscape

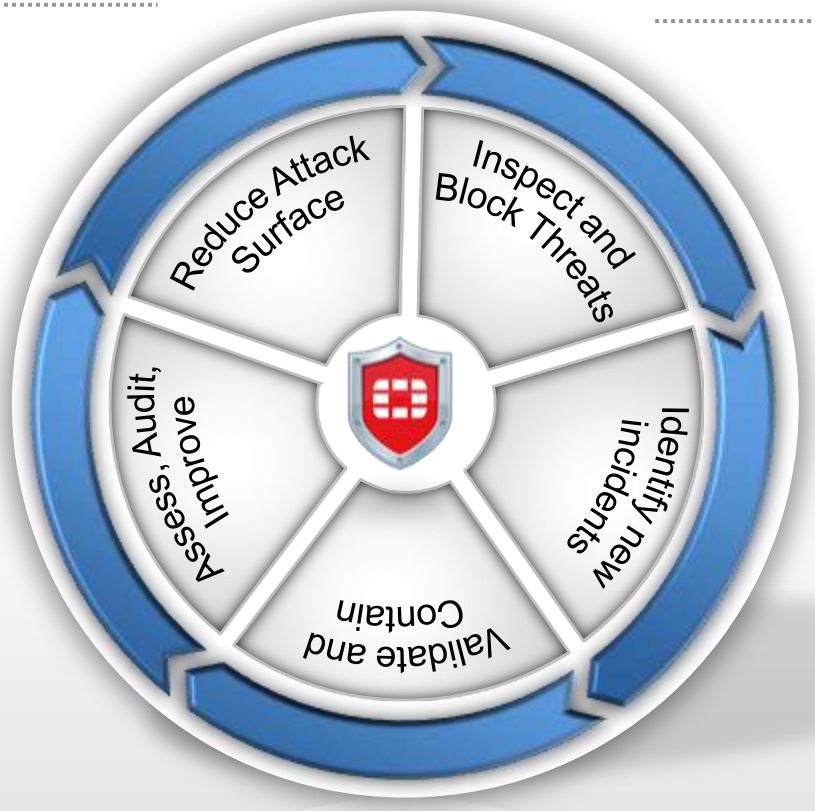
Fortinet's Advanced Threat Protection Framework

Access Control

-Firewall
-2 Factor Authentication
-Vulnerability Management

Continuous Monitoring

-Reporting
-Threat research
-SIEM/Log Mgt/Intelligence
Service partners



Threat Prevention

-IPS, App Control
- Deep Flow Antimalware
-Email/Web Filter
- Antibot

Threat Detection

-Sandbox
-Network behavoral analysis
-Client reputation
-Botnet reporting

Incident Response

-Security Services - Device Quarantine - Security Updates

Which of the following technologies would you add first?

- Strong authentication to the network
- More threat prevention in more places
- New threat detection at key spots
- New incident response tools/services
- More monitoring/intelligence tools/services

Recap/Q&A

- Sophisticated attacks are beating traditional defenses
- While there are many effective new tools to help address these threats, Fortinet cautions there is no one “silver bullet”
- Rather, organizations are encouraged to establish a cohesive approach, combining technologies within an extensible framework

Q&A/Additional Resources

- IE Vulnerability
  http://blog.fortinet.com/post/first-end-of-support-windows-xp-internet-explorer-vulnerability-discovered
- Target Data Breach
  http://www.fortinet.com/webinars/target-data-breach-what-we-can-all-learn-it.html
- Fortinet Advanced Threat Protection Framework
  http://www.fortinet.com/solutions/advanced-threat-protection.html

A Global Leader in Network Security

Global presence and customer base

- Customers: **210,000+**
- Units shipped: **1.7+ Million**
- Offices: **30+** worldwide

Platform Advantage built on key innovations

- FortiGuard: industry-leading threat **research**
- FortiOS: tightly **integrated** network + security OS
- FortiASIC: **custom** ASIC-based architecture
- Market-leading technology: 177 **patents**, 146 pending

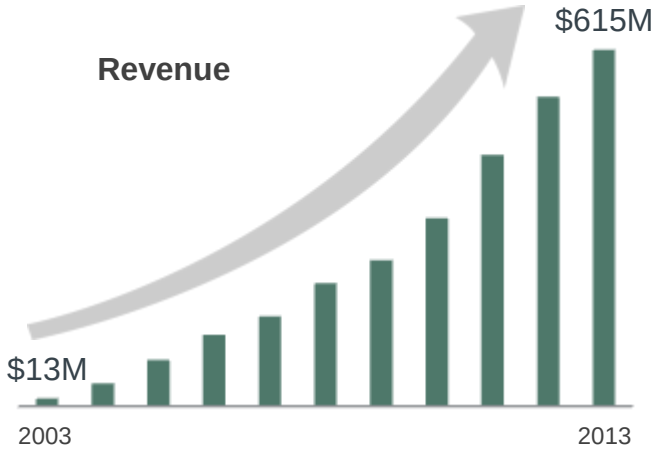
Founded **2000,** 1st product shipped **2002,** IPO **2009**

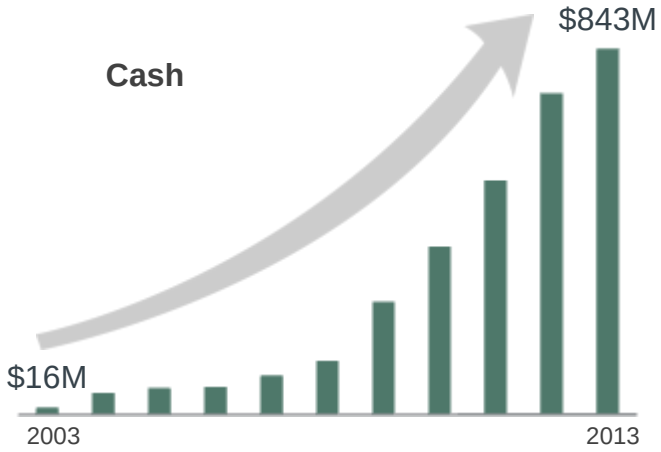
HQ: Sunnyvale, California

Employees: **2700+** worldwide

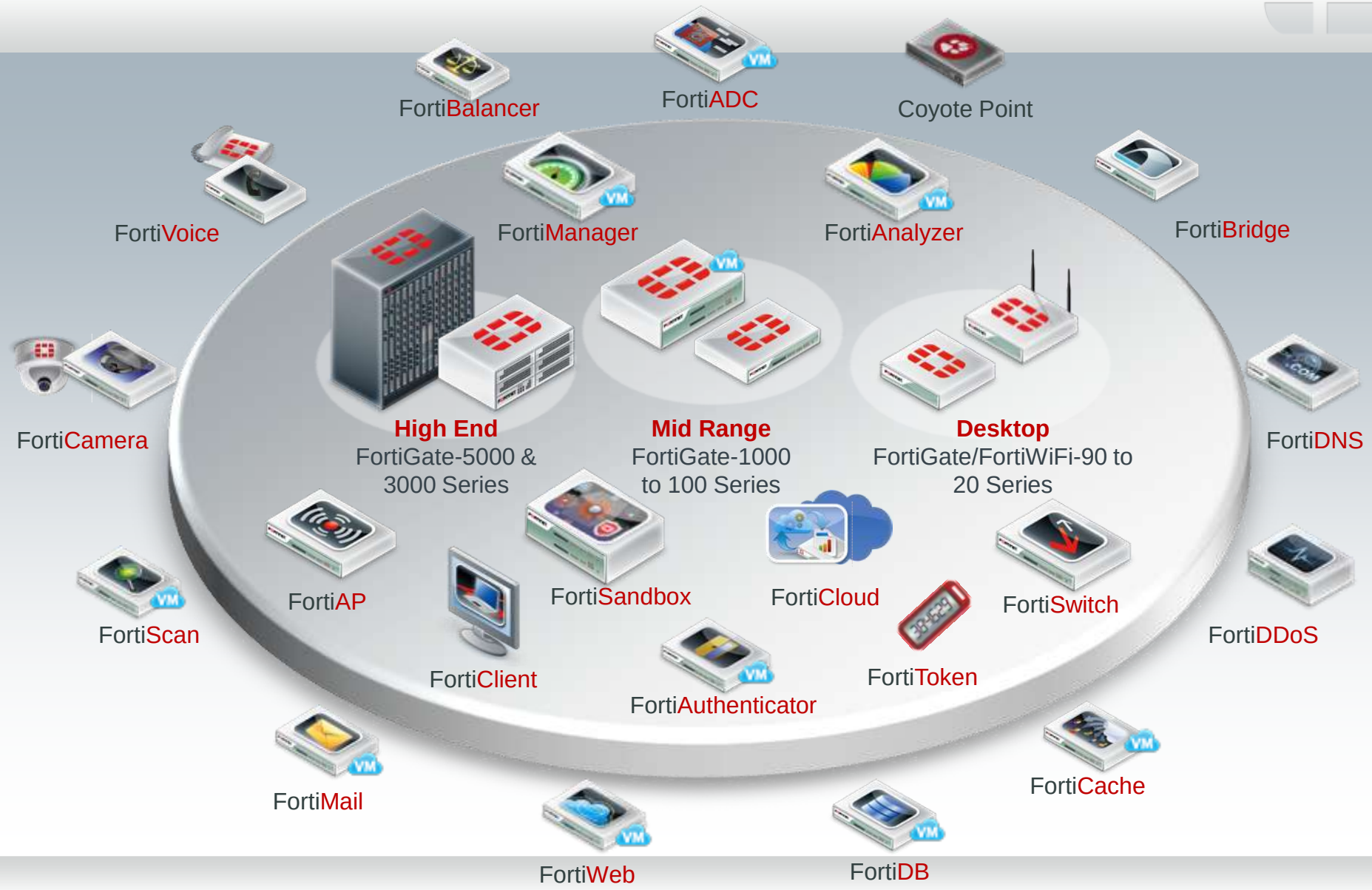
Consistent growth, **gaining** market share

Strong positive cash flow, **profitable**





End-to-End Security Solutions



High Performance Network Security

FORTINET

Thank you!

Doug Manger, CISSP
Senior Security Engineer

dmanger@fortinet.com