Introduction to Cybersecurity: Security for Brokers and Traders

Richard Henderson, Director, Security Intelligence & Evangelism

Agenda

- About the speaker
- Changes in the Threat Landscape
- Threats specific to traders and brokers
- Background on Unified Threat Management, and how it helps
- What can YOU do? A series of recommendations
- Q&A

About Me!

Richard Henderson
Director, Security Intelligence & Evangelism

Fortinet Technologies, Inc.

Security Researcher, Evangelist, Author, Hacker

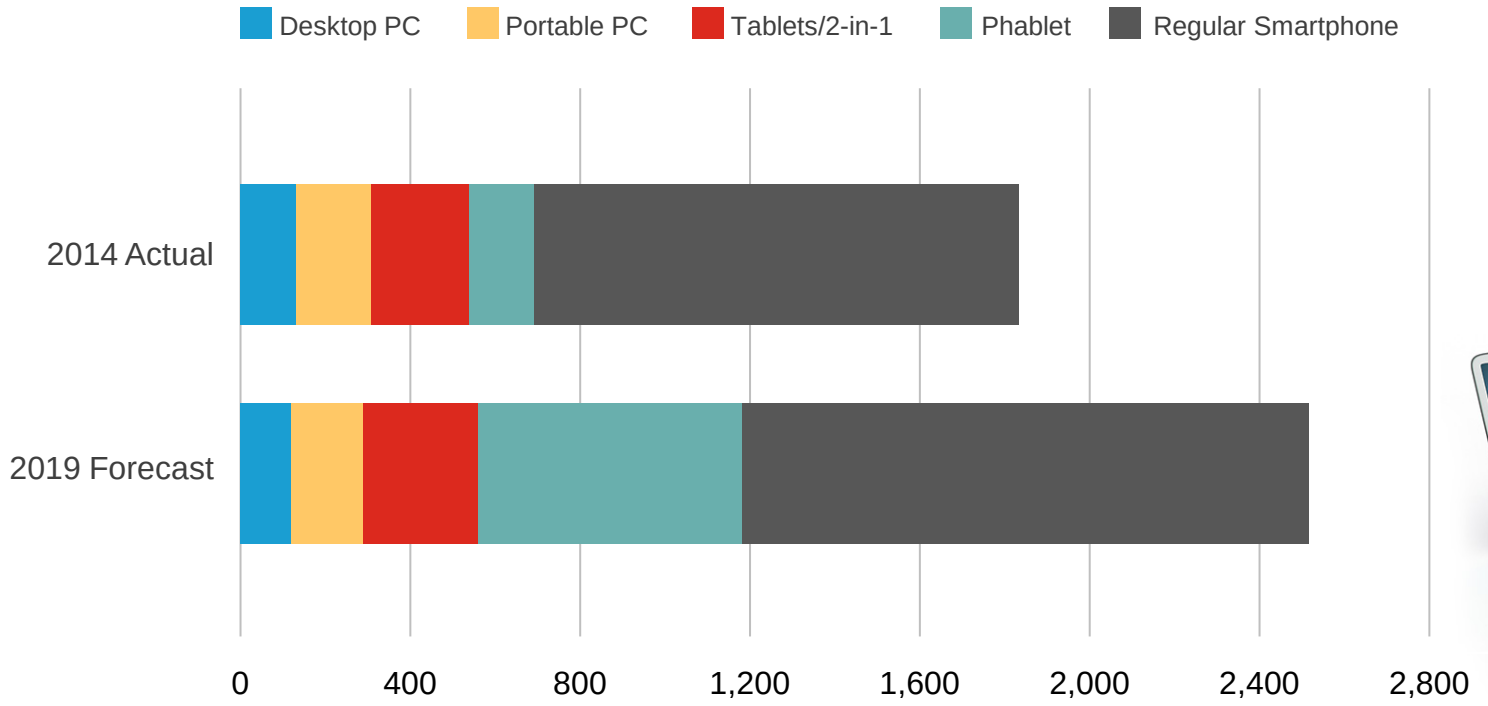
Cybersecurity in 2016

Changes in the Threat Landscape

FORTINET

Today's Technology Trends: Mobility/BYOD

WW Smart Connected Device Shipments, 2014 and 2019
(Million Units)

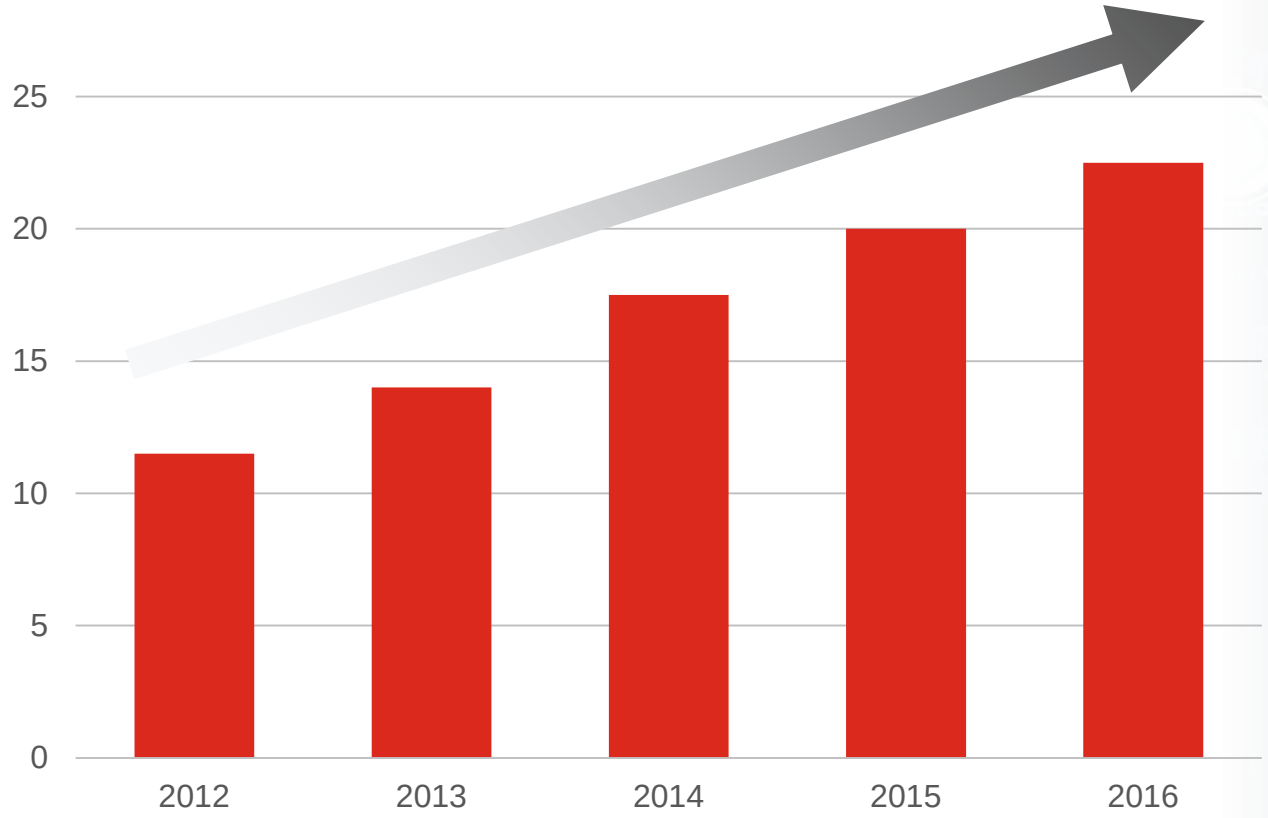


Source: IDC WW Quarterly Smart Connected Device Tracker, March 2015

Today's Technology Trends: Wireless Access

Wireless Access Points and Controllers

(Million Units)



Today's Technology Trends: Cloud Services

Top Functions Used or Being Implemented in the Cloud

Source: Osterman Research. SMB IT/Security Priorities and Preferences Survey. January 2016.

Fortinet Cyber Threat Assessment

Threat Landscape Report

32.14 Million
Attempted Attack Events

71 Malware
Variants Detected

- Botnets traditionally utilize two key vectors for infection: email attachments and compromised web content. However, we are starting to see indications of new strategies for infection that utilize instant messaging platforms to compromise user systems.
- 5,230 instances of the Conficker botnet topped the list of threats, followed by the Nemucod Trojan at 4,220 instances and the Zeroaccess botnet taking the third spot with 3,210 instances.
- Botnets like these typically employ Trojans to compromise systems and then download additional payloads. As an example, Nemucod is notable for its use in campaigns to distribute new highly sophisticated and extremely lucrative ransomware, including Teslacrypt and Cryptolocker.

Source: http://www.fortinet.com/sites/default/files/whitepapers/Executive-Summary-CTAP.pdf

Fortinet Cyber Threat Assessment

Threat Landscape Report

Application Vulnerability Exploits- SMB

Severity	Threat Name	Type	Count
5	MS.DCERPC.NETAPI32.Buffer.Overflow	Buffer Errors	233
5	OpenBSD.IPv6.Fragment.Buffer.Overflow	Buffer Errors	61
5	OpenSSL.Heartbleed.Attack	Information Disclosure	42
5	Joomla.Core.Sessioin.Remote.Code.Execution		40
5	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	18
5	MS.OLE.VBScript.CMD.REDIM.Array.Unbounded. Memory.Corruption	Buffer Errors	6
5	MS.IE.Object.SLayloutRun.Memory.Corruption	Buffer Errors	4
5	Blackhole.Exploit.Kit	Anomaly	2
5	OpenSSL.TLS.Heartbeat.Information.Disclosure	Buffer Errors	2
5	DotkaChef.Exploit.Kit	Anomaly	1

Application Vulnerability Exploits- Enterprise

Severity	Threat Name	Type	Count
5	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	487
5	Mozilla.Element.Style.RelativeToStatic	Other	78
5	OpenSSL.Heartbleed.Attack	Information Disclosure	12
5	Zpanel.pChart.Information.Disclosure		3
5	Angler.Exploit.Kit	Anomaly	2
5	Joomla.Core.Session.Remote.Code.Execution		2
5	OpenSSL.TLS.Heartbeat.Information.Disclosure	Buffer Errors	1
5	Apache.Commons.Collection.InvokerTransformer. Code.Execution		1
5	MS.OLE.VBScript.CMD.REDIM.Array.Unbounded. Memory.Corruption	Buffer Errors	1
5	Obfuscated.Flash.Exploit	Buffer Errors	1

Fortinet Cyber Threat Assessment

Threat Landscape Report (SMB only)

MS10-002: Get it while it's hot!

by Derek Manky | January 21, 2010 | Category: Security Research

Share 0 Tweet 0 Share 0 Google + 0

The much anticipated out-of-band release was rolled out today by Microsoft in the form of MS10-002. Included is CVE-2010-0249 (see our advisory here), addressed by Microsoft through a security advisory (979352) late last week. We released the signature "MS.IE.Event.Invalid.Pointer.Memory.Corruption" to address this particular issue. The Microsoft advisory was, of course, the subject of many headlines through an Internet Explorer zero-day exploit with reports of targeted attacks -- probably the most since Conficker made waves in 2009. Activity on the issue first exploited by Conficker (MS08-067) still remains our #1 detected threat for malicious traffic, as can be observed in our December 2009 Threat Landscape Report (MS.DCERPC.NETAPI32.Buffer.Overflow).

It should be reminded that Microsoft provided MS08-067 as an out of band patch in October 2008, shortly after in the wild activity was spotted. It quickly grew into a vast threat (2009). Thus, my advice: *MS10-002 - Get it while it's hot*! In other words, a patch is available and should be used so that we do not repeat lessons from the past. MS08-067 was exploited in the masses by a worm - so far all reported instances of exploits on CVE-2010-0249 have been targeted attacks (which can wreak more havoc in smaller numbers). The cat is certainly out of the bag as exploit code is publicly available, including Metasploit.

Heartbleed FAQ

Version 1.3 - Thursday April 17 17:59PDT

This document will be updated and maintained as new or updated information becomes available. Continue to check this page for updates.

What is Heartbleed?

The Heartbleed bug is a vulnerability discovered in the TLS heartbeat mechanism built into certain versions of the popular OpenSSL library. OpenSSL is one of the technologies employed by many sites online to create an encrypted communication session between a user and a website.

Has something like this happened before?

Yes, attacks on TLS and OpenSSL have happened in the past. In 2011, the BEAST (Browser Exploit Against SSL/TLS) exploit was created which took advantage of a weakness found in TLS version 1.0 first discovered in 2002 in order to stealthily steal authentication tokens and decrypt the communication between a web server and a browser. What's unique about Heartbleed is that there was not a requirement to intercept communications between a user and a server.

Who is affected?

If you use the Internet, it is all but guaranteed that you have been impacted in some fashion by the Heartbleed bug. While reports have stated various numbers of sites potentially exposed to Heartbleed - as many as two-

Fortinet Cyber Threat Assessment

Threat Landscape Report (SMB only)

Malware, Botnets and Spyware/Adware- SMB

Malware Name	Type	Application	Count
Sality.Botnet	Botnet C&C	Sality.Botnet	72.36K
Riskware/MSIL_Tpyn	Spyware	HTTP	2.06K
Mazben.Botnet	Botnet C&C	Mazben.Botnet	1.65K
W32/Virut.CE	Virus	HTTP	1.26K
JS/Faceliker.B!tr	Virus	HTTP	935
W32/Agent.WBX!tr	Virus	HTTP	746
JS/FBJack.A!tr	Virus	HTTP	736
JS/Nemucod.IP!tr.dldr	Virus	HTTP	684
Adware/BrowserFox	Adware	HTTP	654
W32/Ramnit.A	Virus	HTTP	598

Malware, Botnets and Spyware/Adware- Enterprise

Malware Name	Type	Application	Count
Andromeda.Botnet	Botnet C&C	Andromeda.Botnet	11.49K
Shedun.Botnet	Botnet C&C	Shedun.Botnet	28
Android/Triada.B!tr	Virus	8080/tcp	22
PossibleThreat.P0	Virus	HTTP	18
Zeus	Virus	HTTP	11
JS/Moat.2081C96D!tr	Virus	HTTP.BROWSER_IE	10
Android/Loki.A!tr	Virus	HTTP	9
Android/lop.O!tr	Virus	HTTP.BROWSER	7
Android/lop.C!tr	Virus	HTTP	6
Android/Gorpo.B!tr	Virus	8080/tcp	6

Fortinet Cyber Threat Assessment

Threat Landscape Report (SMB only)

Jeremy Kirk
IDG News Service Apr 3, 2014 7:08 AM

A botnet that was slowly shrinking has taken on a new trick: brute-forcing routers set to easy-to-guess credentials.

The malware behind the botnet, called Sality, has been around since 2003, in part due to its use of digitally-signed communications and an efficient software design, wrote Benjamin Vanheuverzwijn, a malware researcher with Eset.

Sality is a general piece of malware that can download other components and has been used over the years for misdeeds such as faking advertising network traffic, distributed denial-of-service attacks and cracking VoIP accounts.

But the number of computers infected by Sality appears to have been decreasing slightly over the last couple of years, perhaps due to difficulties in infecting new machines, Vanheuverzwijn wrote on a blog post on Wednesday.

To up its numbers, the latest version of Sality has a component called Win32/RBrute.A that scans the Internet for router control panels and attempts to log into them using a short list of user names and passwords.

"The usual infection vectors of W32/Sality might not be sufficient enough to keep the botnet alive; hence the botnet controllers are deploying new components to grow the botnet," Vanheuverzwijn wrote.

It is targeting 14 router models from TP-Link, three from D-Link, two made by ZTE and one from Huawei. If it successfully logs into a router, it changes the default DNS (Domain Name System) server, which is responsible for translating domain names into IP addresses that can be displayed in a browser.

http://www.pcworld.com/article/2139460/sality-malware-growing-old-takes-on-a-new-trick.html

Nemucod Adds Ransomware Routine

by Roland Dela Paz | March 16, 2016 | Category: Security Research

Share 31 Tweet 149 Share 17 Google + 3

It came to our attention that a new, rather peculiar version of Nemucod has been recently landing on users. Nemucod is a well-known JavaScript malware family that arrives via spam email and downloads additional malware to PCs. Most recently, Nemucod has been known to download TeslaCrypt ransomware variants.

However, the last few weeks saw a shift in Nemucod variants--it now has a code to drop ransomware from its body. The sample arrives via a typical Nemucod spam with encrypted JavaScript attachment.

Upon decrypting the JavaScript, we can see that it attempts to download a file on the user's temporary directory from compromised websites. The downloaded file is an executable file that is later on used to encrypt the user's files:

https://blog.fortinet.com/post/nemucod-adds-ransomware-routine

Specific Threats

Incidents and anecdotes on threats unique to traders and brokers

Petr Murmylyuk - 2012

Petr and his gang hacked into scores of trading accounts:

- Gained access then changed PII so as not to alert victims
- Stolen accounts would make illogical trades which the gang profited from
- Fidelity, Scottrade, E*Trade and Schwab claimed losses of at least $1M USD

- Petr was sentenced to 30 months in prison, 3 years of supervised release and ordered to pay over $500K in restitution

Spear Phishing & Whaling Attacks

Attackers cast a wide net… and often land big fishes:

- A managing director for a trading firm was targeted…
- ...by an attacker who compromised one of his **clients.**

- They're not just targeting you, but *targeting the people you deal with* in order to steal from you.

Malware Targeting Trading Software

Attackers can be incredibly specific…

- Specialized malware was found that targeted trading software
- Malware was cast out, and looked for evidence of trading software being used
- If detected, the malware would slurp up credentials and take screenshots

“Crypto” Malware

But cybercriminals have many other ways of making money:

- Specialized malware has exploded recently designed to encrypt ***everything*** on your computer
- You’re locked out of everything… unless you pay the ransom
- Getting your files back is usually impossible

- What would be the impact to you and your work if everything suddenly stopped working?

Background

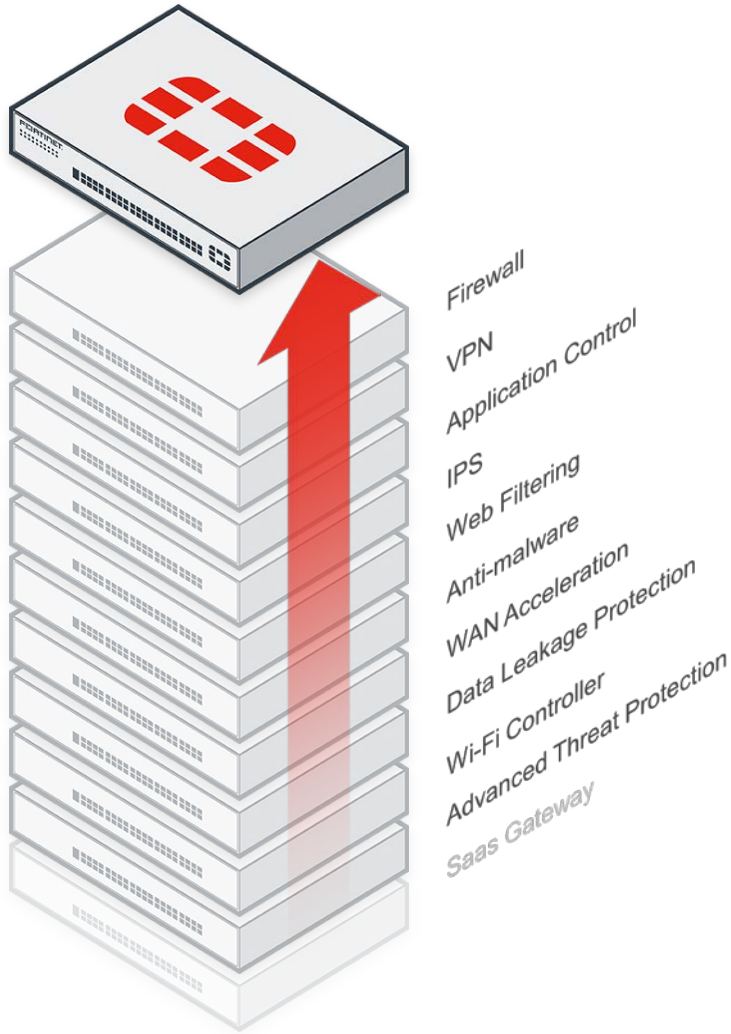
Unified Threat Management (UTM)

What is a Unified Threat Management (UTM) Appliance?

A converged platform of point security products, particularly suited to small and midsize business.

Typical feature sets fall into three main subsets, all within the UTM:

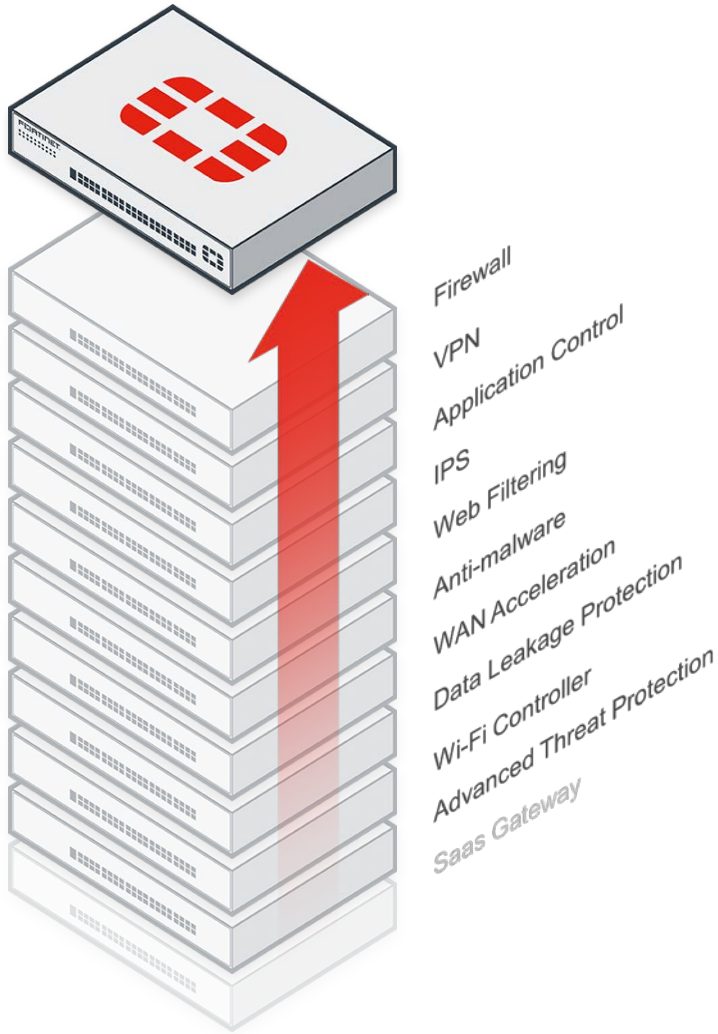
- Firewall/IPS/VPN
- Secure Web Gateway
- Messaging Security



What is a Unified Threat Management (UTM) Appliance?

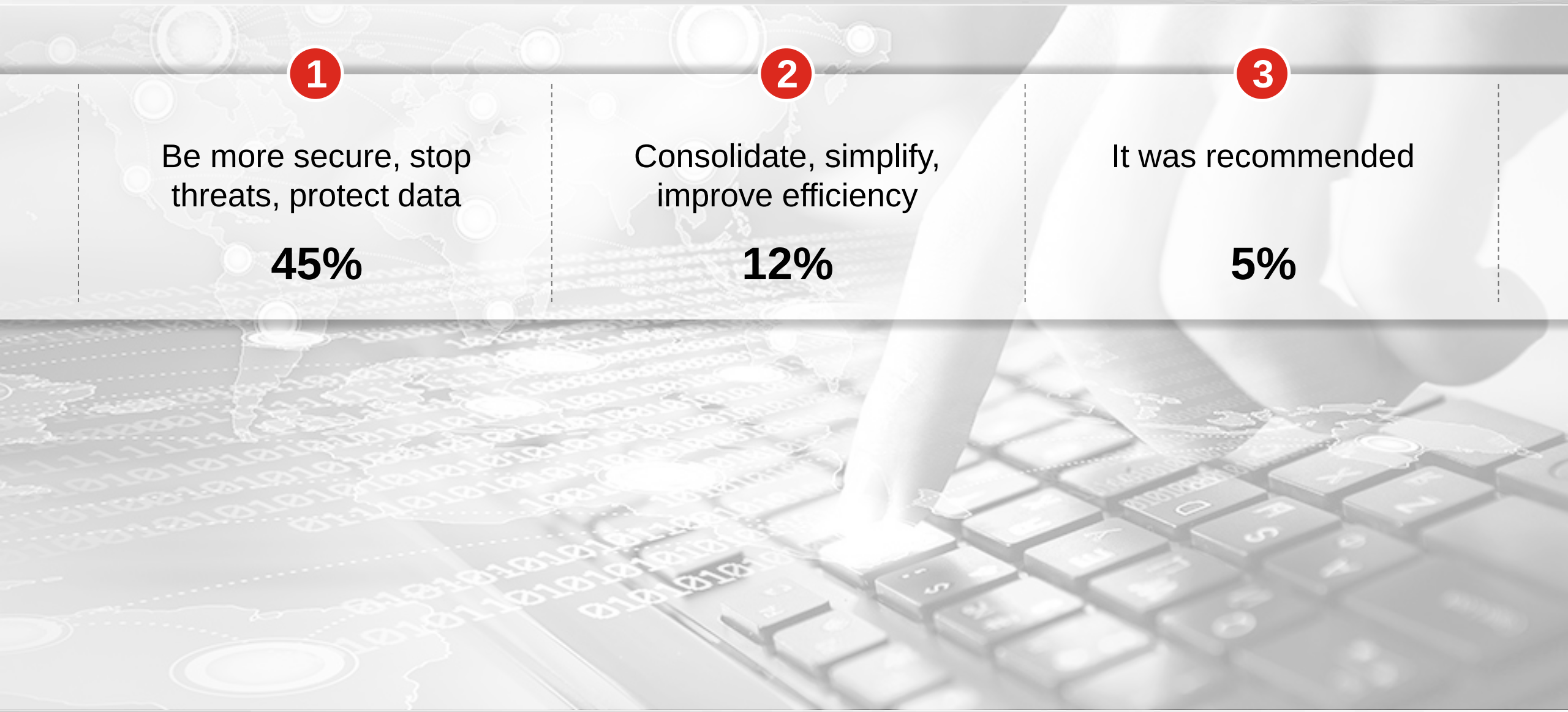
79%

of SMBs have one



Source: Osterman Research. SMB IT/Security Priorities and Preferences Survey. January 2016.

Why did SMBs Deploy a UTM?



1. Be more secure, stop threats, protect data

45%

2. Consolidate, simplify, improve efficiency

12%

3. It was recommended

5%

Source: Osterman Research. SMB IT/Security Priorities and Preferences Survey. January 2016.

What do they now like most about their UTM?

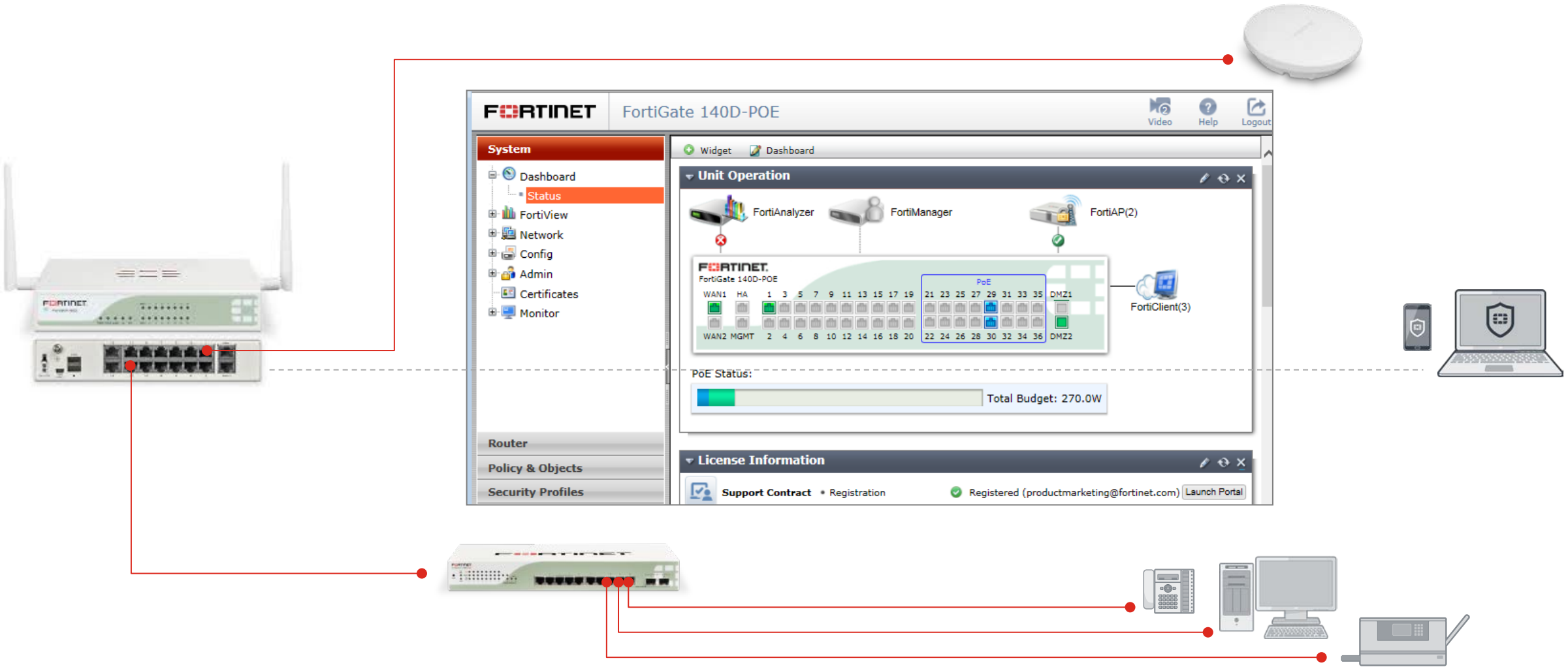
1. Be more secure, stop threats, protect data — **45%**
2. Consolidate, simplify, improve efficiency — **12%**
3. It was recommended — **5%**

1. Easy, efficient, consolidated, reliable — **43%**
2. Effective, improves safety, etc. — **13%**
3. Good for business, customers — **5%**

Source: Osterman Research. SMB IT/Security Priorities and Preferences Survey. January 2016.

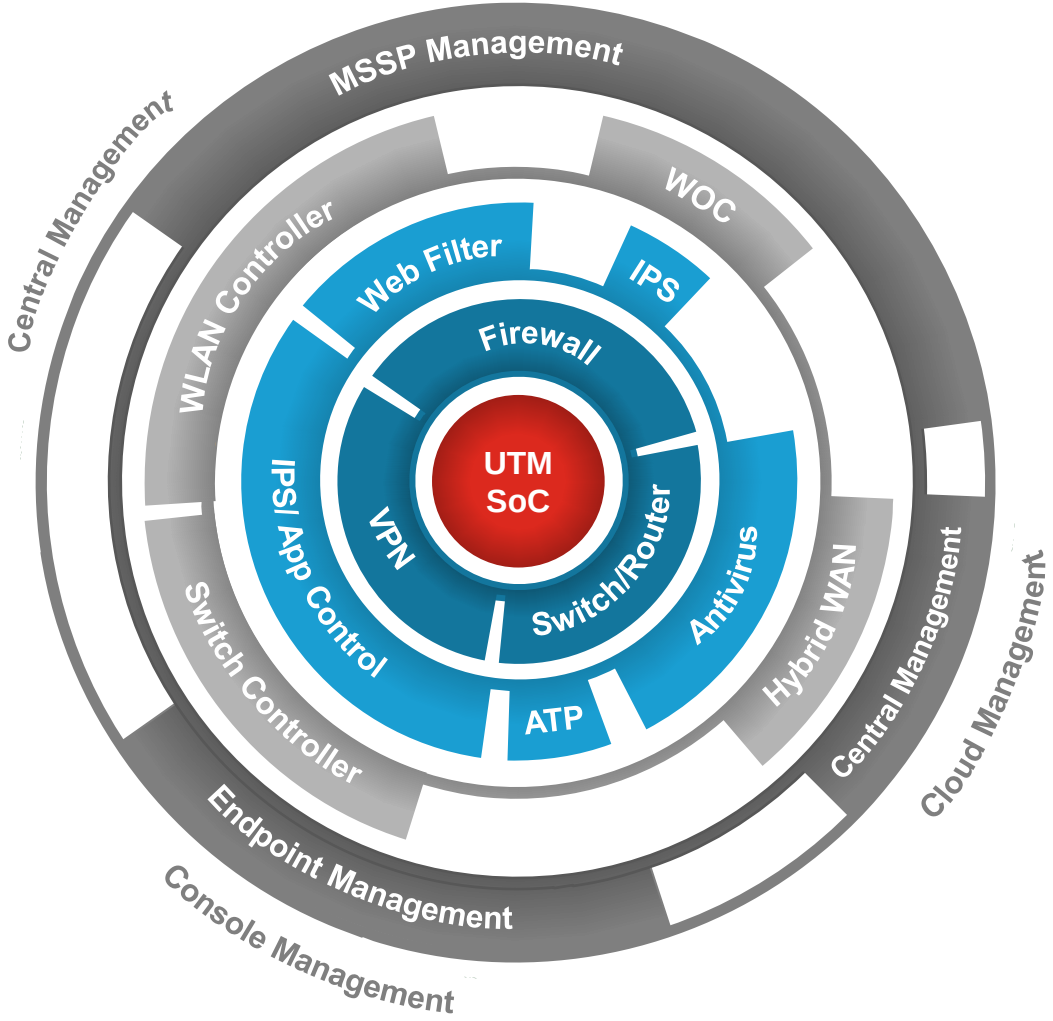
Connected UTM

All Centrally Managed for Ease of Use



Connected UTM

All Centrally Managed for Ease of Use



What Should I Do?

A series of recommendations to improve your security, right now

What's Going on at Home?

The attack surface in your home is probably bigger than you think…

- Virtually *everything* is vulnerable to attack in some form or another
- Internet of Things (IoT) devices are starting to be targeted
- Do you use your trading computer for things?
- Do you know what your kids' computers are up to?
- Is your wireless secure?

Going on the Road?

Dangers can be found anywhere…

- Open WiFi **is** dangerous, and not to be trusted.
- Theft of hardware – it still happens. Is your data secure?
- Are you using a VPN when connected to wireless outside of the home?

Recommendations

1. Educate Yourself!
2. Isolate your Network
3. Minimize your Attack Surface
4. Back it Up and Protect Yourself
5. The UTM Solution – Managed and Unmanaged

Recommendations

Educate Yourself

If you take nothing else from this presentation:

- Treat **everything** as suspicious
- Attachments are **bad**
- **Stop** clicking links in email

Recommendations

Isolate your Network

- Consider separating your home network from your work network entirely
- If you can’t, segment it as best you can: separate routers/switches

Recommendations

Minimize the Attack Surface

- If you don’t need it on your computer, **get rid of it!**
- Don’t mix business with pleasure. On both the PC and smartphone
- Be careful when using your mobile devices, especially Android
- **PATCH** YOUR COMPUTERS!

Recommendations

Back it Up!

- If you're not backing up everything regularly… it's not a question of "**if**".
- **Store** your backups "cold"
- **Test** your backups
- **Protect** your backups

Recommendations

Protect Yourself

- If a service offers two factor authentication, **use it.**
- Passwords – change your view on them, don’t recycle them
- Make sure you have endpoint protection as an additional layer of security. Something is better than nothing.

Recommendations

Unified Threat Management (UTM) Appliances and Managed (or unmanaged) Security

- UTM appliances are affordable… compared to the cost of an incident or data loss.
- There are many vendors to choose from, not just Fortinet.
- If you want to “set it and forget it”, there are Managed Security Providers who will do all the heavy lifting.

Questions?

Thank You!

rhenderson@fortinet.com

https://linkedin.com/in/richardthenderson


FORTINET