THE "NEW" SECURITY FABRIC

AGENDA

- What is the New Security Fabric
- Why a “New” Security Fabric?
- Solution Spotlight: Advanced Threat Protection Framework

The “NEW” SECURITY FABRIC

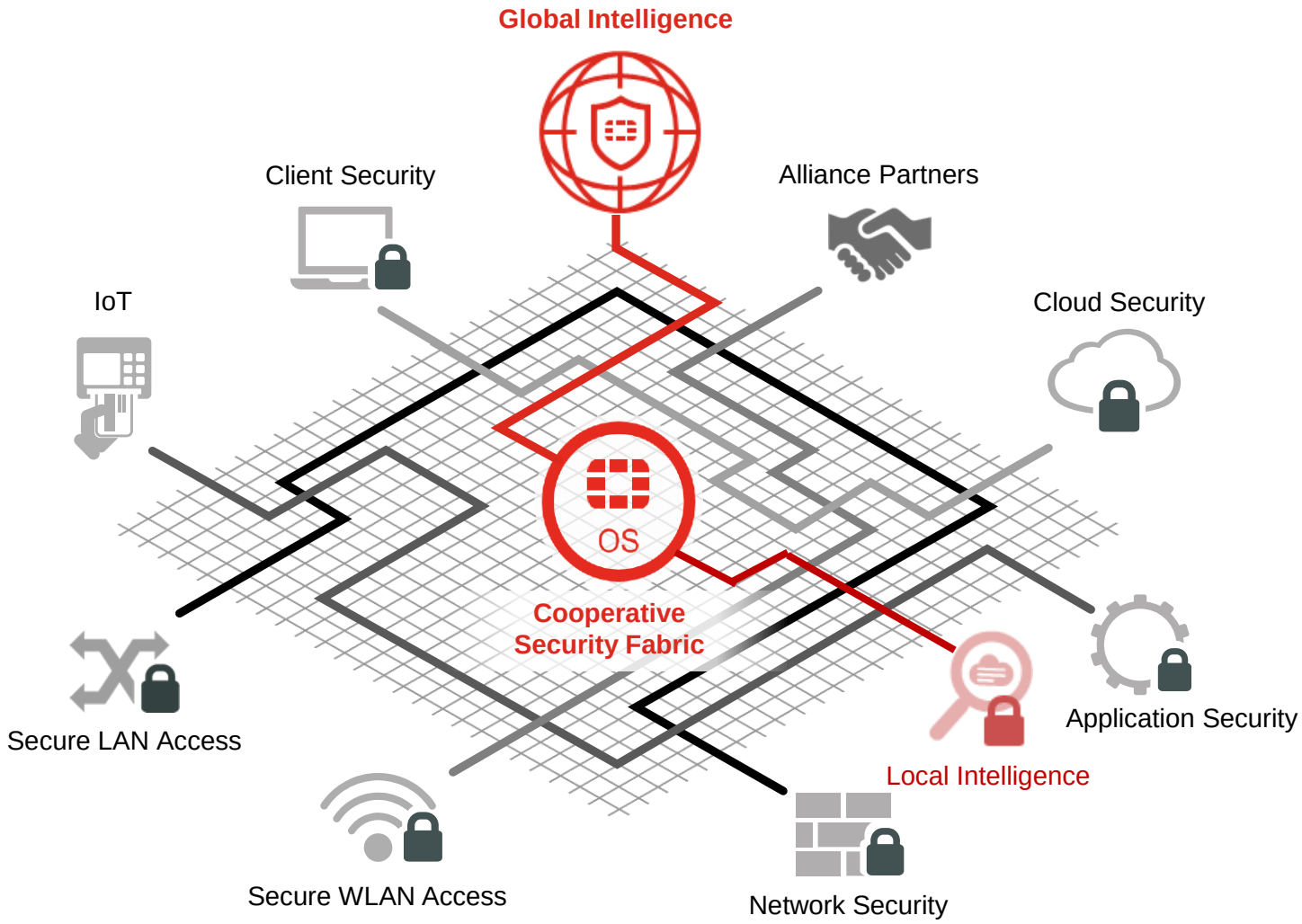
Scale

Awareness

Security

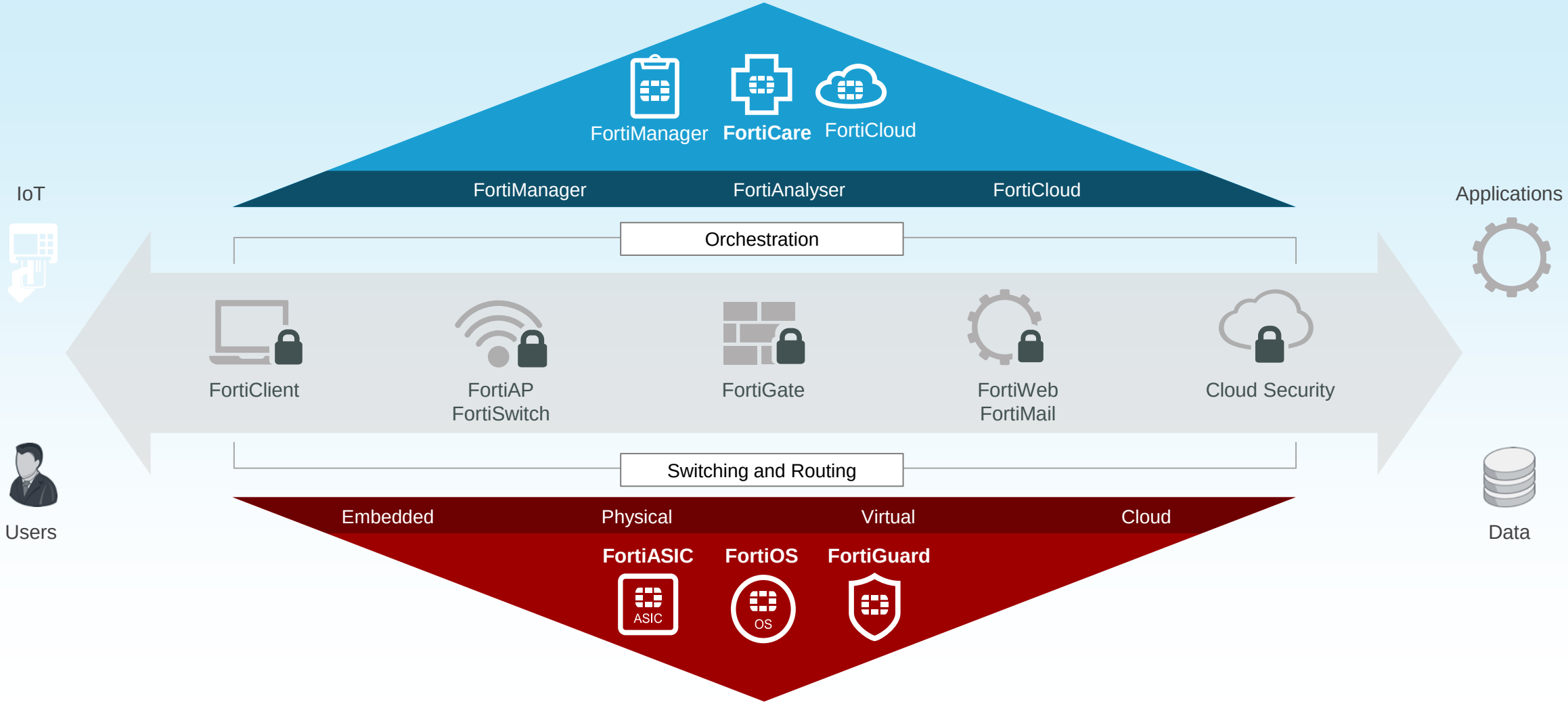
Actionable

Open

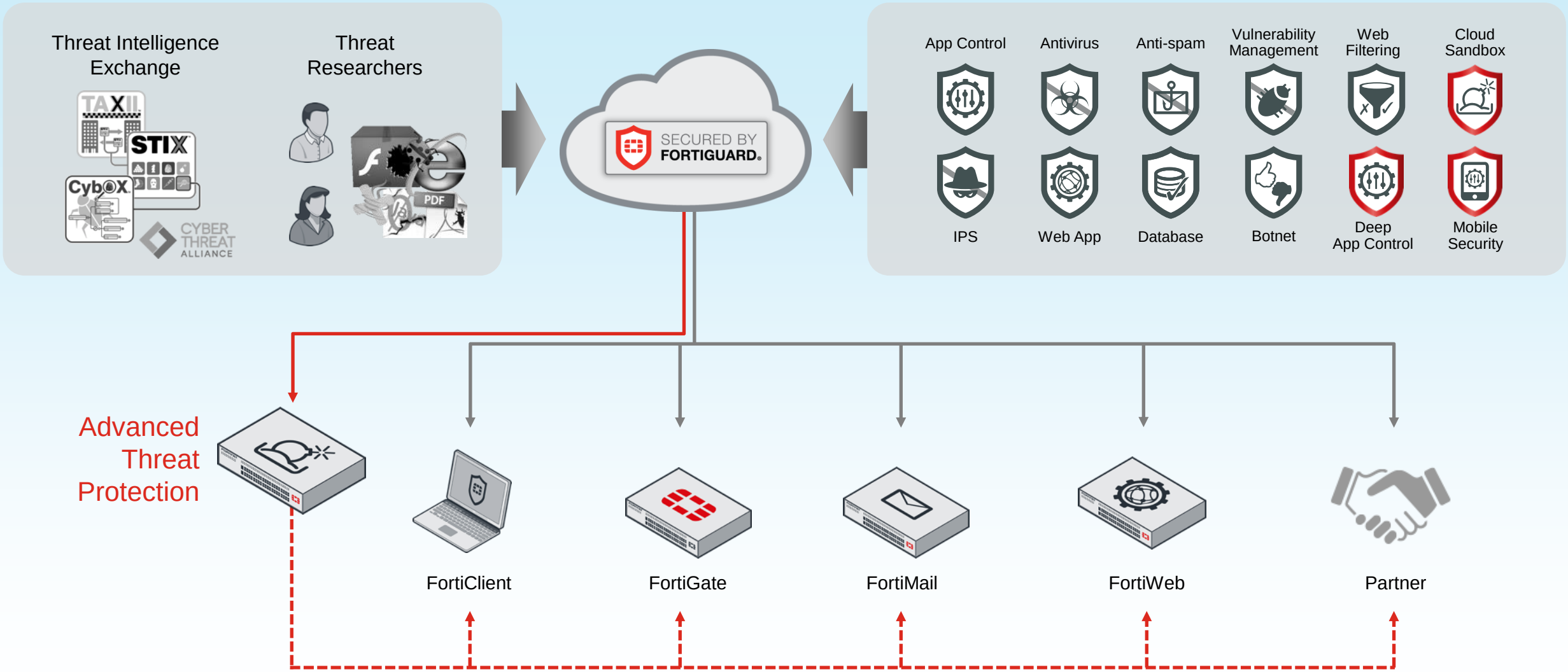


The “NEW” SECURITY FABRIC

Protects the Entire Attack Surface



ATP FRAMEWORK

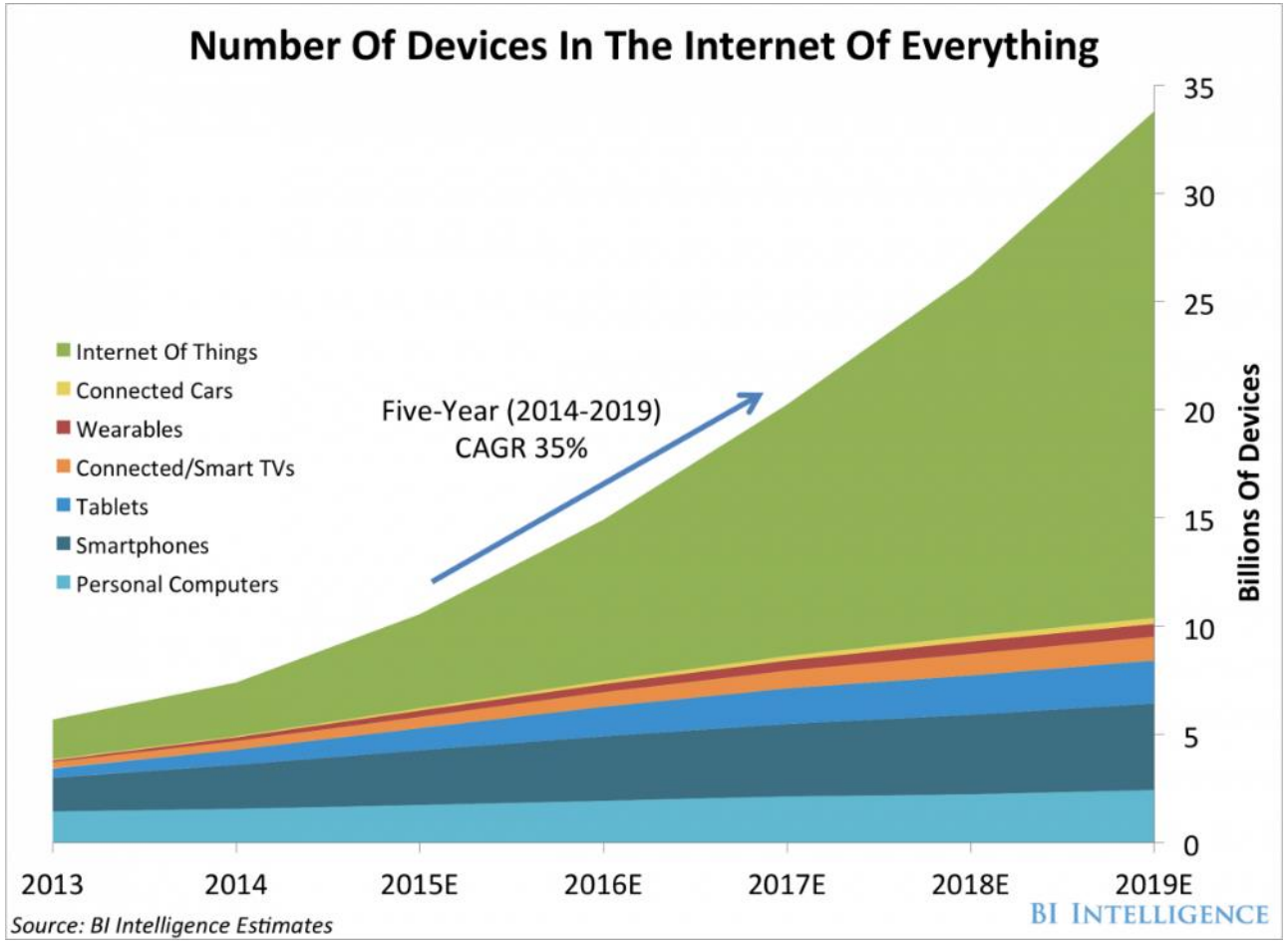


WHY "NEW" SECURITY FABRIC

Trend: Device Growth Continues

More devices and newer device types are entering the network

- 33 Billion endpoints projected to be connected by 2020 – Gartner
- New device types entering the network
  - » ‘headless’ IoT, wireless sensor nodes, beacons, wearables




2016
THE YEAR OF RANSOMWARE
Stats
500%
growth last year
FIGURE 5: GROWTH OF RANSOMWARE FAMILIES
Ransomware
Ransomware will remain a major and rapidly growing threat in 2016, fueled by anonymizing networks and payment methods.
Inexperienced cybercriminals will leverage ransomware-as-a-service, magnifying the growth in ransomware.
THE RISE OF RANSOMWARE
Ransomware Discoveries
Mikko Hypponen
Here's our statistics on the most common Ransom Trojans out there. Obviously #KeRanger did not make the list, yet.
2014-2015 Zero-Day Attacks by Vulnerable Application
New Samples of Prominent Ransomware Families
CTB-Locker
CryptoWall
Teerac
CryptoLocker
Source: McAfee Labs, 2015.
Total Ransomware
Locky Ransomware
Have you or anyone you know been infected with ransomware?
Yes
No
SYSTweak

Did you know…..

- Actual Infections practically doubled from 20% to 38%
- 61% feel email attachments pose the largest threat
- Nearly half say they would be forced to pay the ransom if backups failed
- Confidence in filters is only 72%
- 88% feel security awareness training is the most effective protection from ransomware over 83% for backup, almost identical to 2014

Interestingly enough, in the same week, Kaspersky also released data that confirms our numbers. For crypto-ransomware, which has almost become the de facto choice for black hats today, **the number of users attacked rose 5.5-times – from 131,111 in 2014-2015 to 718,536 in 2015-2016**, the firm claimed. Note that this refers to attacks, not infections.

Ransomeware is growing…

The Russian Cyber Mafia behind Dridex 220 and Locky are using the RockLoader malware to download Bart over HTTPS. Bart has a payment screen like Locky but encrypts files without first connecting to a command and control (C&C) server. It spreads with .zip attachments containing JavaScript Code and use social engineering to trick users into opening the attachments

There is a new ransomware strain called "Satana" (the reference is clear, just take the last "a" off) which is a blend between classing file encryption malware and the Petya / Misha strain which locks the Master Boot Record (MBR). This looks like a Petya copycat, for each encrypted file, Satana *prepends* their email address to each file

The number of data breaches keeps going up. Last week it was more than 1,000 Wendy's where credit card records got ripped off. Fraudsters quickly use the news release of a high-profile data breach to kick an extortion campaign into gear.
The recent uptick in email extortion comes from the data breaches at organizations like Ashley Madison, the IRS, Anthem, and many others where millions of records with (sometimes highly) personal information was stolen

RANSOMWARE

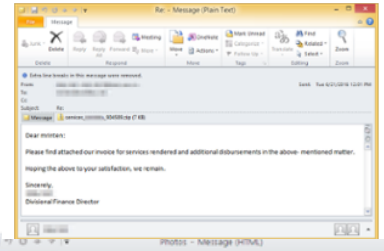
Lazy Ransomware Bad Guys Just Delete Your Files - Never Mind Decrypting

By Stu Sjouwerman, Jul 12, 2016 12:56:26 PM

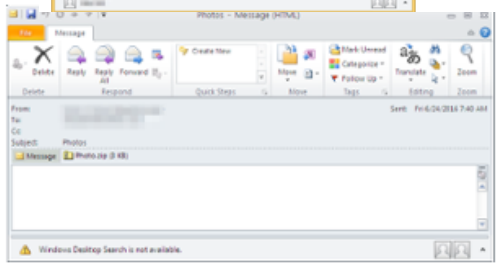
There is a new strain of "ransomware" that does not bother with the whole encryption thing at all. These bad guys seem to think it's just an unnecessary distraction and too much work. Better to just start nuking files and then present victims with a ransom note. It's called RanScam and here is how it looks:

Russian Cyber Mafia Is Back From Vacation With Smarter Locky Ransomware Strain

By Stu Sjouwerman, Jun 25, 2016 9:16:00 AM



Threatpost reported that the notorious Necurs botnet is back in business, after mysteriously going dark for nearly a month. Researchers report the Necurs has returned to spewing massive volumes of email containing an improved version of the potent Locky ransomware and the Dridex banking Trojan.



Proofpoint researchers discovered a new
strain of ransomware called "Ba
kidding.

The Russian Cyber Mafia behir
and Locky are using the RockL
to download Bart over HTTPS.
payment screen like Locky but
without first connecting to a command and control (C&C) server. It spreads with .z
containing JavaScript Code and use social engineering to trick users into opening
attachments. Here is how they look:

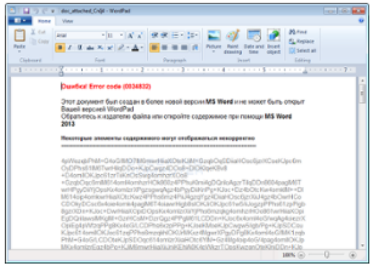
A researcher in China has discovered a design flaw in Microsoft Windows that affects all versions of the operating system using NetBIOS spoofing —including Windows 10— and lets an attacker hijack your organization's network traffic with a simple social engineering attack. It can be exploited silently with a near perfect success rate.

e bad guy just uses social engineering to trick an employee into
ia IE or Edge or to open a specifically crafted Office document.
ters will appear as either a file server or a local print server, but in
it will hijack your network traffic including things like Windows Updates.

lity has a massive security impact – probably the widest impact in the history of
said in an interview with DarkReading conducted via email. "It not only can be
gh many different channels, but also exists in all Windows vers
20 years."

New RAA Ransomware Strain Created Entirely Using Javascript

By Stu Sjouwerman, Jun 18, 2016 10:55:36 AM



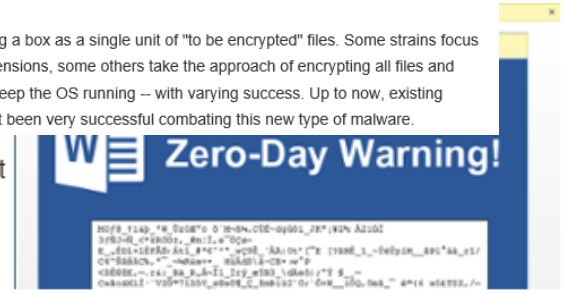
Larry Abrams, who runs Bleepingcomputer was first to report on a new strain of ransomware called RAA. The criminal coders took the somewhat unusual step of writing the whole thing in JavaScript making it more damaging in certain situations, and also install the Pony password stealer for good measure.

Larry wrote that it is being distributed by email through attachments that pretend to be a regular Doc file. Since JavaScript itself does not have crypto functions, the bad guys use the CryptoJS library which allows them to use AES encryption to lock up their victims' files. Here is how the fake attachment looks:

Scam Of The Week: FBI Warns Against Data Breach Extortion

The number of data breaches keeps going up. Last week it was more than a 1,000
Wendy's where credit card records got ripped off. Fraudsters quickly use the news
release of a

Apparently, MS Office 365 bu
are not cutting it. A new strai
Ransomware is now targeting
e zero-day attack that
Office 365's built-in



cloud security provider Avanan shows a massive zero-day attack
with phishing emails having malicious file attachment payloads.

Expect Micro Ransomware: Extortion One Document At A Time

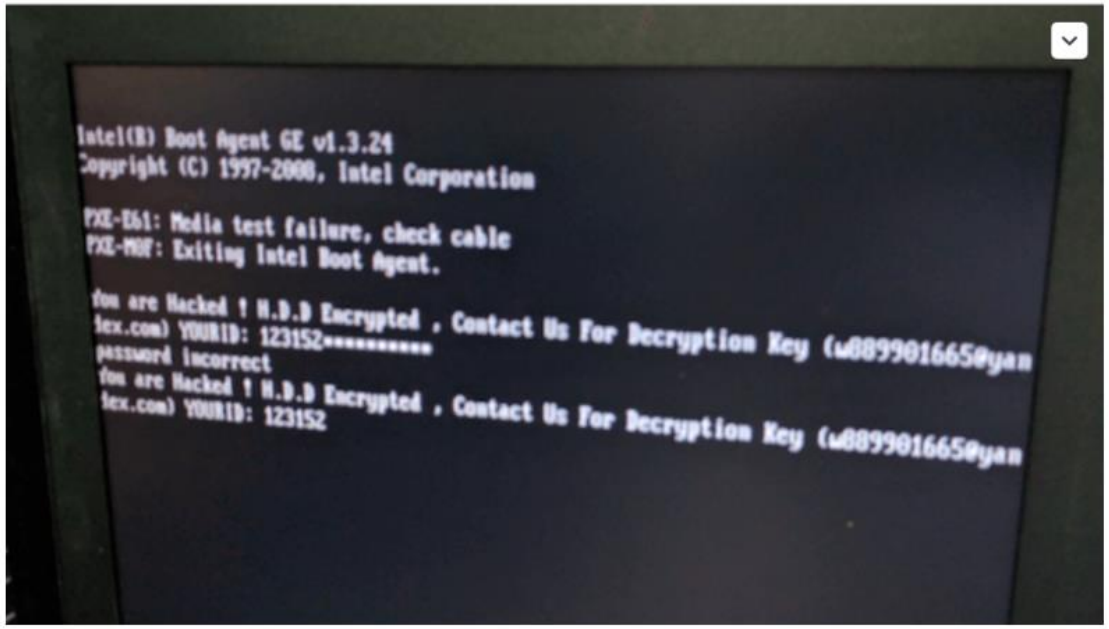
By Stu Sjouwerman, Jun 19, 2016 11:09:13 AM

I have been following the development of ransomware closely since September 2013 when the ransomware plague was unleashed on the internet in the form of CryptoLocker and its copycats.

At the time of this writing, there are now well over a hundred different strains and the end is not in sight. On the contrary, ransomware has proven to be a highly successful criminal business model and many aspiring cybercriminals big and small are now trying to muscle into this racket.

Up to now, they are treating a box as a single unit of "to be encrypted" files. Some strains focus on a specific set of file extensions, some others take the approach of encrypting all files and exclude Windows files to keep the OS running -- with varying success. Up to now, existing antivirus products have not been very successful combating this new type of malware.

SecurityAffairs just published a new discovery that you need to know about. A Brazilian Infosec research group, Morphus Labs, just discovered a new Full Disk Encryption (FDE) ransomware strain this week, dubbed “Mamba”, a snake with a paralyzing poison.
Mamba, just like Petya, uses a disk-level encryption strategy instead of the conventional file-based one. Full-disk encryption seems to be a new ransomware trend.



“You are Hacked”. This message is all that remains of the victims of this new ransomware. To get the decryption key, victims must contact somebody through the e-mail address given in the message, give their unique ID and pay 1 BTC (currently ~$600) per infected host.

There is a new strain of "ransomware" that does not bother with the whole encryption thing at all. These bad guys seem to think it's just an unnecessary distraction and too much work. Better to just start nuking files and then present victims with a ransom note. It's called Ranscam and here is how it looks:

Ranscam deceives victims by falsely claiming that files have been moved onto a hidden, encrypted partition. However, back at the ranch, this malicious code has deleted selected files and seriously messed with system settings like removing executables that drive System Restore, deleting shadow copies, and breaking Safe Mode etc. Recovering a system from this infection is very hard. This is outright destructive code and the way to recover is wipe and rebuild from bare metal.

They try to extort a ransom of 0.2 Bitcoin (about $125) but the crooks really have no mechanism at all to restore compromised files. The attackers provided the same wallet address for all payments and for all samples, said Cisco's Talos researchers.

SPOOFING

Hard drive manufacturer Seagate was sued by its own employees as the result of a successful CEO fraud attack where all the personal information of 10,000 existing and former employees were stolen. Seagate lawyers defend the company claiming that the organization is not responsible for data leaks and that the attack was unexpected. Really?

Don't be surprised if you see spam coming from the top websites in the world. Lax security standards are allowing anyone to "spoof" emails from some of the most-visited domains, according to new research.

Email spoofing — a common tactic of spammers — basically involves forging the sender's address. Messages can appear as if they came from Google, a bank, or a best friend, even though the email never came from the actual source. The spammer simply altered the email's "from" address.

Authentication systems have stepped in to try and solve the problem. But many of the top website domains are failing to properly use them, opening the door for spoofing, according to Sweden-based Detectify, a security firm.

The company analyzed the top 500 websites ranked by Alexa and found that 276 of the domains are vulnerable as a result, it said in a blog post on Monday. Here is the full article at PC World

A lawsuit filed on Friday September 16, 2016 by Tillage Commodities Fund alleges that $6 billion SS&C Technologies Holdings, a financial services software firm, showed an egregious lack of diligence and care, when they fell for an email scam that ultimately led to hackers in China looting $5.9 million.

According to authorities, a young woman working as CFO at Leoni's Bistrita factory was the target of the scam, when she received an email spoofed to look like it came from one of the company's top German executives. She then proceeded paying out $44 million in the process.

Real World Spoofing

CNBC reported some pretty stunning breaking news. I cannot come up with a better case for new-school security awareness training for employees in accounting and HR.

A lawsuit filed on Friday September 16, 2016 by Tillage Commodities Fund alleges that $6 billion SS&C Technologies Holdings, a financial services software firm, showed an egregious lack of diligence and care, when they fell for an email scam that ultimately led to hackers in China looting $5.9 million.

Tillage claims that SS&C didn't follow their own policies, which enabled the theft, but to add insult to injury, staffers actually *helped* the criminals by fixing transfer orders that had initially failed. The documents were posted online by the law firm representing Tillage in the case. Above is the stock price on Monday, before the news hit. We will see if/how this changes the next few days.

In the lawsuit, lawyers for Tillage say staff at SS&C failed to "exercise even a modicum of care and responsibility in connection with known and obvious cybersecurity threats."

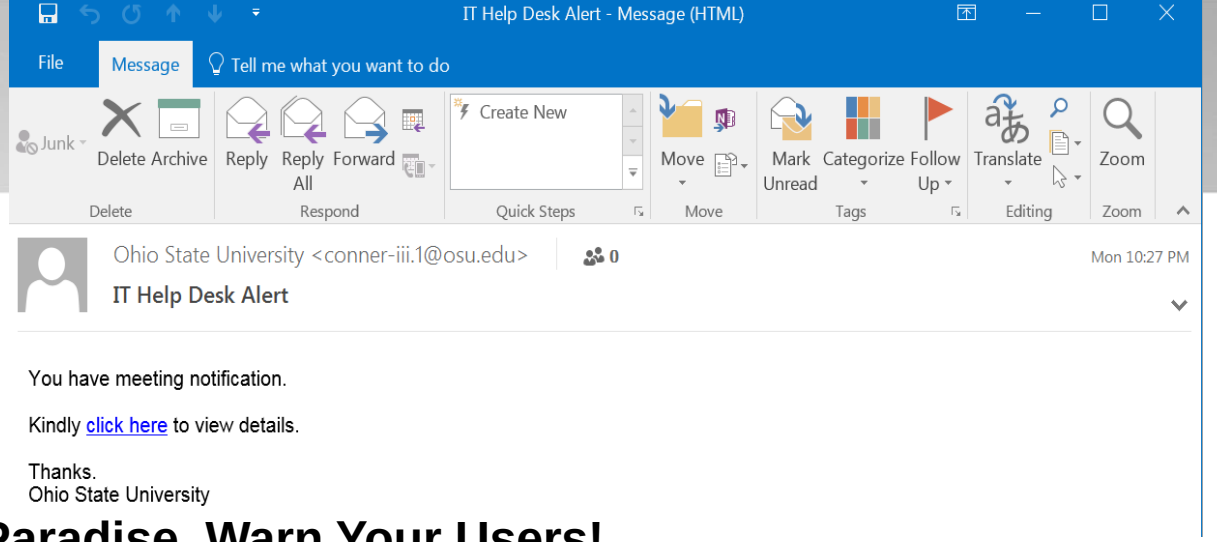
For example, according to the suit, "the email requesting the largest wire transfer during the lifetime of this scheme ($3 million) states nothing more... than: 'How was your weekend? Let's round business up today.'" The suit states that one staffer "directed the release of Tillage's funds oftentimes merely minutes after receiving the fraudulent wire requests."

The scheme was amateurish, the lawsuit says, including the use of an email account that spelled Tillage with three 'Ls' instead of two – something that should've been spotted. Further, the emails contained "awkward syntax and grammatical errors – which were wholly inconsistent with prior Tillage communications – and which were entirely unclear in substance."

All these red flags should have been caught by employees if they were trained to follow policy and keep a sharp eye out for possible CEO Fraud.

Phishing

Apple Store Phishing Attack Goes For Whole Enchilada



500 Million Hacked Yahoo Accounts Are A Phishing Paradise. Warn Your Users!

Did you know that 91% of successful data breaches started with a spear-phishing attack?

The phish in question is a fairly straightforward credentials phish. It starts with this email:

Anyone half-awake should be asking questions based on just a cursory glance at this email.

- It purports to originate from an "IT Help Desk Alert" account, yet the listed email address appears to be a personal email address (and, from the headers we inspected, likely associated with a compromised account).

- The message in the email body is not only strangely terse but awkwardly lacking an indefinite article (should read: "You have a meeting notification.").

- The message is signed simply "Ohio State University," with no other identifying information about the scheduling system that presumably generated this notification.

Phishing…..

These 500 Million Hacked Yahoo Accounts Are A Phishing Paradise.

Warn your users...

Hi,

It's all over the press. Here is a quote from Reuters: "Yahoo Inc said on Thursday information associated with at least 500 million user accounts was stolen from its network in 2014 by what it believed was a "state-sponsored actor."

The data stolen may have included names, email addresses, telephone numbers, dates of birth and hashed passwords (the vast majority with the relatively strong bcrypt algorithm) but may not have included unprotected passwords, payment card data or bank account information, the company said.

Top 10 Phishing Schemes

The new category "Reported Phishes of the Week" collects the ten best real-world phishing emails seen over the previous seven days and makes them available as templates for customers interested in using actual phishes sent by the bad guys. This week's collection of "reported phishes" includes the following new templates:

•"**Account Update Security Alert!**" -- Fake security alert prompts users to update their credit card profile at an alleged "secure login portal"
•"**Alert - New Transaction Review**" -- Employees are instructed to download and review a summary of account transactions
•"**Download the schedule document**" -- Email instructs users to download a "schedule document"
•"**Help Desk Support**" -- Email directs users to download and read a "secure message from Helpdesk Administrator"
•"**New or modified user account information**" -- Fake Microsoft email prompts users to update their expired passwords
•"**Payment Advice - ACH credits**" -- Email provides users with a malicious attachment billed as "payment advice"
•"**Re: formal complaint**" -- False customer complaint email includes malicious attachment allegedly sent for a manager's eyes
•"**Re: Re: casefarmsnet.com invoice**" -- Email supplies a malicious attachment advertised as an invoice
•"**Settlement Agreement (Initial version) - 1TOS11710**" -- Email includes a malicious attachment billed as a "draft settlement agreement"
•"**TD Web Business Banking News - Security Device Required**" -- Fake banking email prompts customers to upgrade their bank account by logging on to a fake bank web site or opening a malicious attachment

SOLUTION SPOTLIGHT:
FortiMail & FortiSandbox

DID YOU KNOW…

79,790

Number of incidents investigated by Verizon in 2015

229

Average number of days attackers were on a network before detection

70-90%

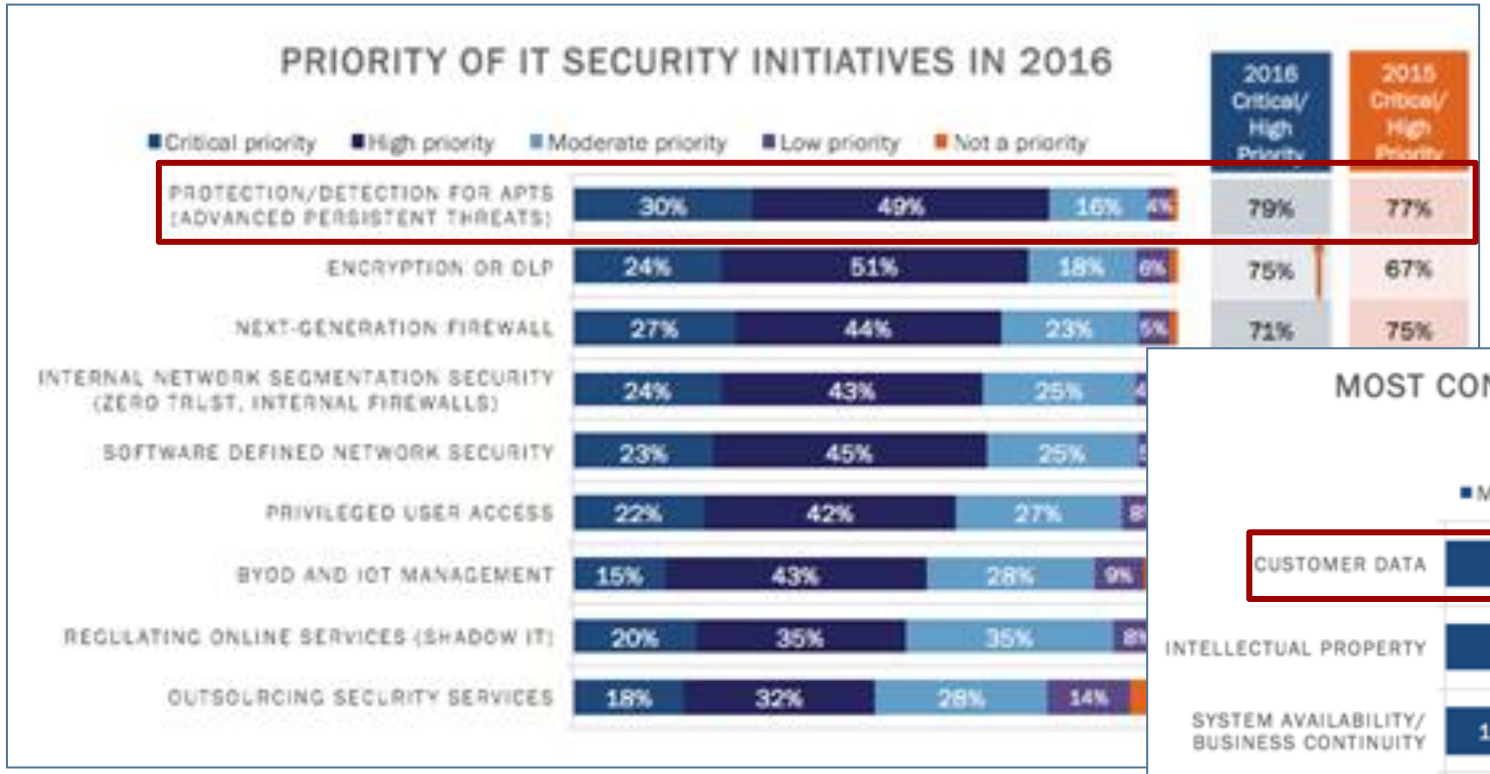
Percent of time unique malware was found

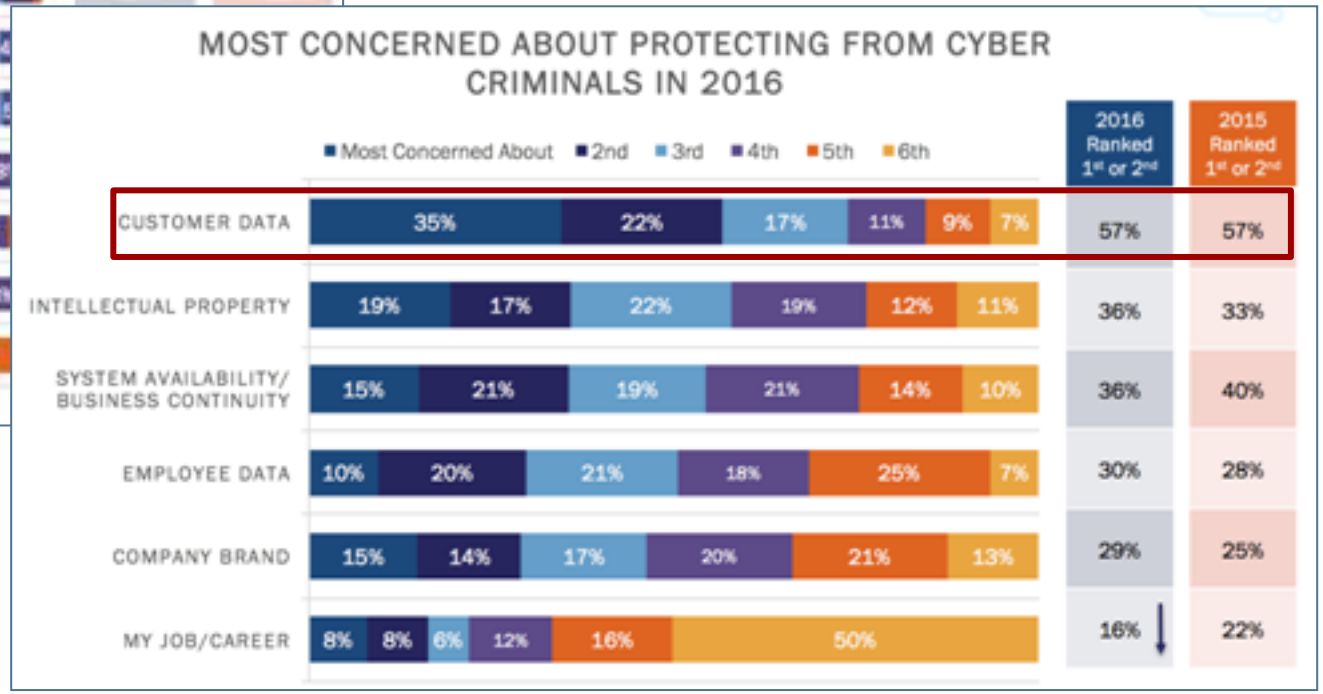
Gartner: All organizations should assume they are in a state of continuous compromise

DID YOU KNOW…

- 205 Billion emails sent every day
- 39% of attachments contain malicious files
- 34% of links embedded in emails are malicious
- 77% of all malware is installed via email
- Malware by file type: 52% are PDF, and 44% are EXE format

APTs, DATA BREACHES TOP OF MIND





Source: IDG Research, January 2016

THERE IS GOOD REASON FOR CONCERN

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

> All organizations should now assume that they are in a state of continuous compromise.
>
> *— Gartner, 2/14/14*

	Incidents				Breaches			
Industry	Total	Small	Large	Unknown	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143	282	136	10	136
Administrative (56)	44	6	3	35	18	6	2	10
Agriculture (11)	4	1	0	3	1	0	0	1
Construction (23)	9	0	4	5	4	0	1	3
Educational (61)	254	16	29	209	29	3	8	18
Entertainment (71)	2,707	18	1	2,688	38	18	1	19
Finance (52)	1,368	29	131	1,208	795	14	94	687
Healthcare (62)	166	21	25	120	115	18	20	77
Information (51)	1,028	18	38	972	194	12	12	170
Management (55)	1	0	1	0	0	0	0	0
Manufacturing (31-33)	171	7	61	103	37	5	11	21
Mining (21)	11	1	7	3	7	0	6	1
Other Services (81)	17	5	3	9	11	5	2	4
Professional (54)	916	24	9	883	53	10	4	39
Public (92)	47,237	6	46,973	258	193	4	122	67
Real Estate (53)	11	3	4	4	5	3	0	2
Retail (44-45)	159	102	20	37	137	96	12	29
Trade (42)	15	3	7	5	4	2	2	0
Transportation (48-49)	31	1	6	24	15	1	3	11
Utilities (22)	24	0	3	21	7	0	0	7
Unknown	9,453	113	1	9,339	270	109	0	161
Total	64,199	521	47,408	16,270	2,260	447	312	1501

Sources:
Verizon 2016 Data Breach Investigations Report, April 2016
Gartner. Designing an Adaptive Security Architecture for Protection From Advanced Attacks. February 2014.

Why We Promote Advanced Threat Protection (ATP)

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

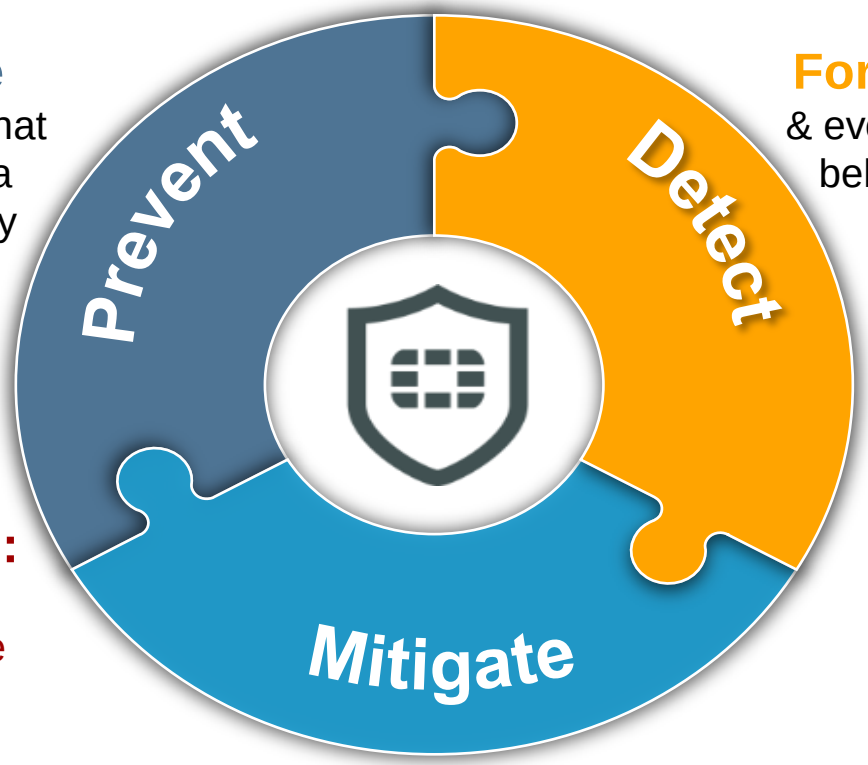
Unknown Threats
- Identify Unknown Threats
- Assess Behavior & Identify Trends

Response
- Identify scope
- Mitigate impact

Hand off :
High risk items

FortiGate
& everything that can enforce a security policy

FortiSandbox
& everything that is behavior based



Hand off :
Creating a fix & update prevention

Hand off :
Provide ratings & results

FortiGuard
teams and automation

FORTIGUARD MINUTE

Per Minute

21,000
Spam emails intercepted

390,000
Network Intrusion Attempts resisted

460,000
Malware programs neutralized

160,000
Malicious Website accesses blocked

50,000
Botnet C&C attempts thwarted

43 Million
Website categorization requests

Updates Per Week

46 Million
New & updated spam rules

120
Intrusion prevention rules

1.8 Million
New & updated AV definitions

1.4 Million
New URL ratings

8,000
Hours of threat research globally

SECURED BY
FORTIGUARD®

FortiGuard Database

190
Terabytes of threat samples

18,000
Intrusion Prevention rules

5,800
Application Control rules

250 Million
Rated websites in 78 categories

337
Zero-day threats discovered

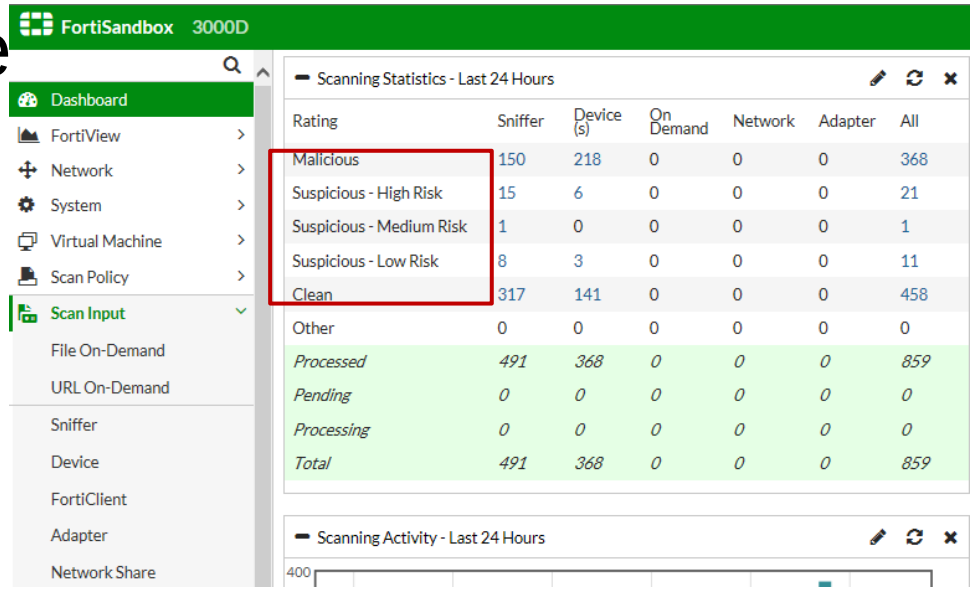
Sandbox

- In computer security, a **sandbox** is a security mechanism for separating running programs. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system.[1] A sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted.
- In the sense of providing a highly controlled environment, sandboxes may be seen as a specific example of virtualization. Sandboxing is frequently used to test unverified programs that may contain a virus or other malicious code, without allowing the software to harm the host device.[2]

SANDBOX OVERVIEW

An advanced threat detection solution the analyzes dynamic activity, rather than static attributes, to identify previously unknown malware

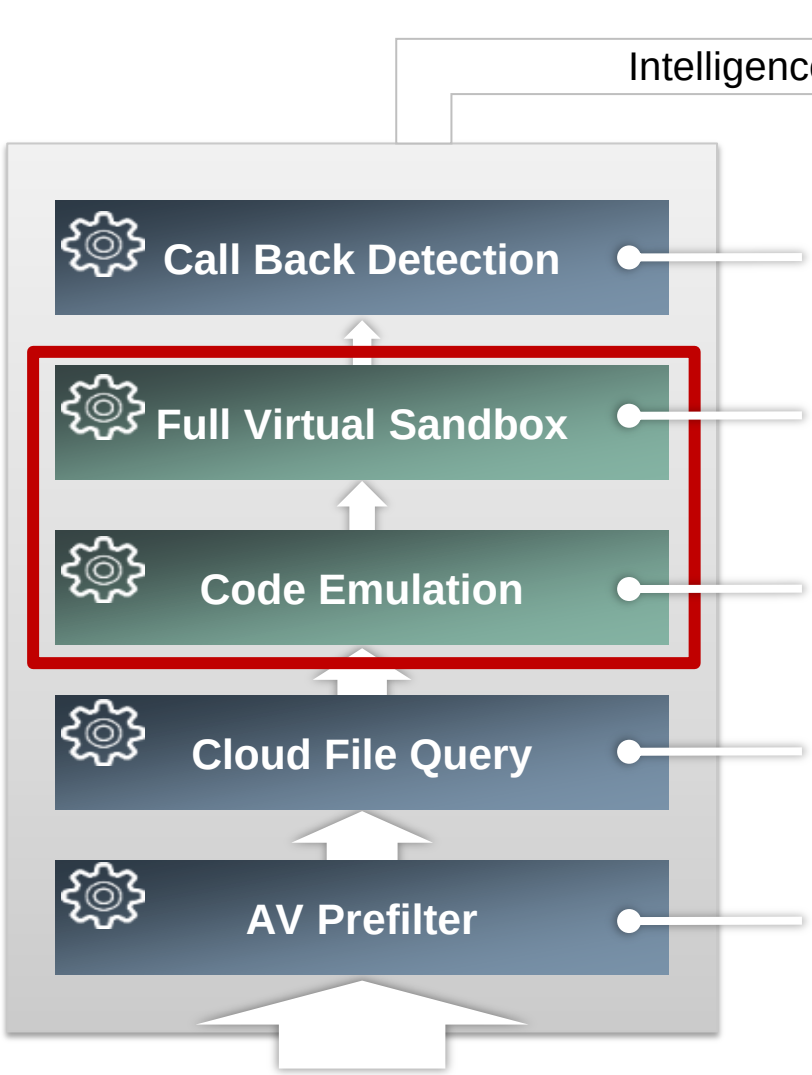
- Extracts objects for more inspection
- Analyzes runtime operation in a virtual environment
- Provides risk ratings
- Uncovers, distributes threat intelligence
- Detects call back attempts



3 modes of operation

Sniffer: span port mode to capture all packets
On-demand: manual submission of files
Integrated: with NGFW, SEG, WAF and EPP

KEY SANDBOX COMPONENTS



- Distribute real-time updates
- Feed global systems

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

- Examine real-time, full lifecycle activity to get the threat to expose itself

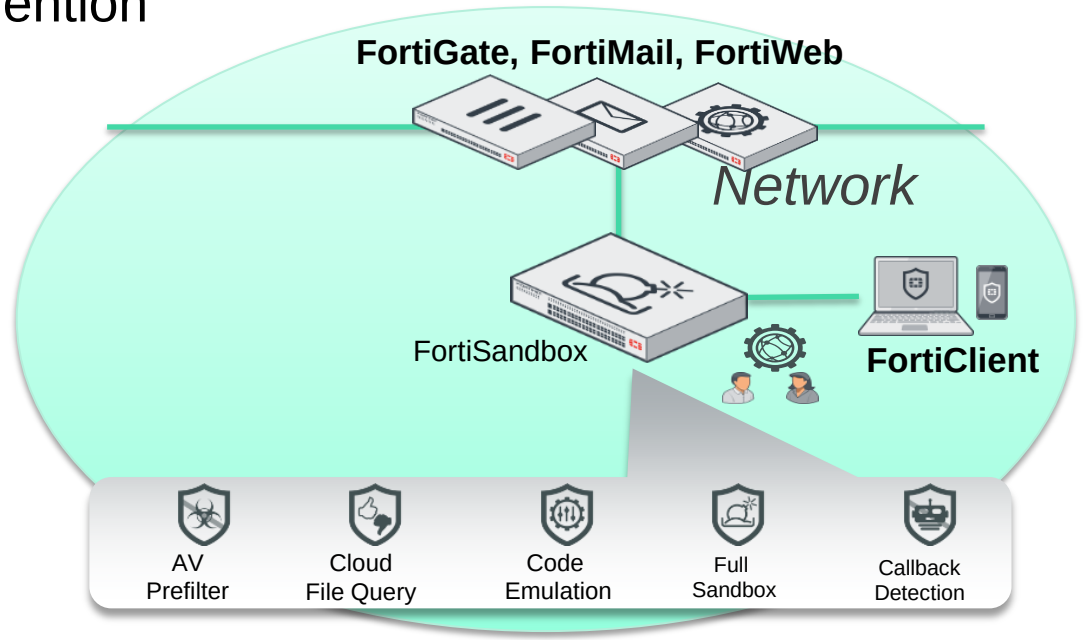
- Quickly simulate intended activity
- OS independent and immune to evasion/obfuscation

- Check community intelligence & file reputation

- Apply top-rated anti-malware engine

ADVANCED THREAT PROTECTION IN ACTION

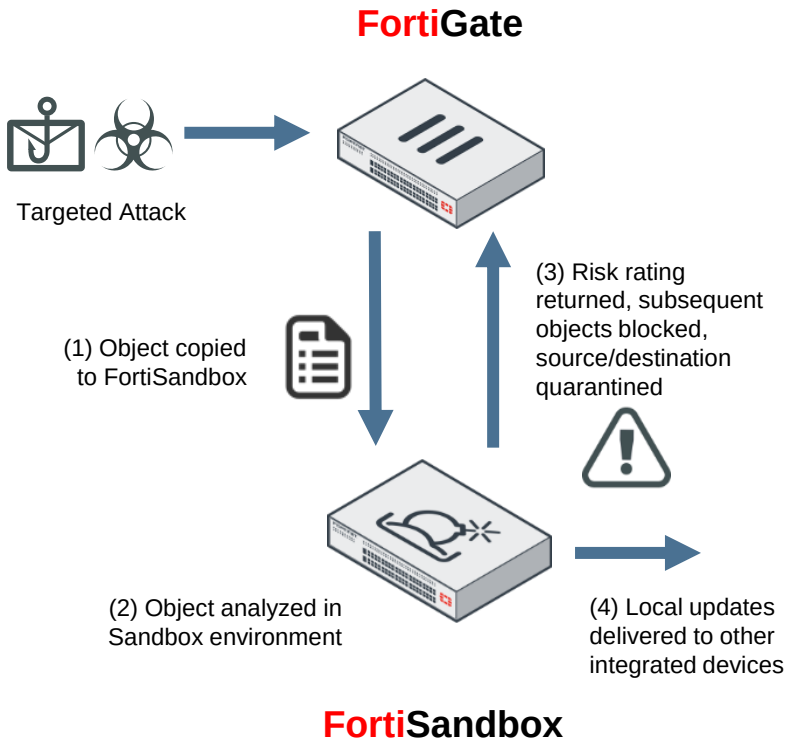
- Firewall, SEG, Web App Firewall, End Point for Prevention
  - » Block as many threats as possible
  - » Submit at risk objects for additional analysis
  - » Mitigate previously unknown threats
- Sandbox for Payload Analysis
  - » Accept at risk objects for additional analysis
  - » Execute objects to assess and rate risk
  - » Provide intelligence and generate updates for prevention products



- ✓ Identify more, previously unknown, threats
- ✓ Minimize the cost of comprehensive coverage
- ✓ Speed and simplify response

Firewall – SANDBOX INTEGRATION

- On the Firewall Side
  - » Inspects ingress, egress and internal traffic
  - » Passes benign objects and URLs to Sandbox
  - » Receives submission results and local updates
  - » Presents one-click actions
  - » Blocks subsequent elements of the attack
- On the Sandbox Side
  - » Watches the wire for objects to analyze or indicators of command control activity
  - » Receives objects from Firewall
  - » Analyzes all objects and activity
  - » Assigns and return a rating for the object
  - » Dynamically generates/distributes threat intelligence



SECURED BY FORTIGUARD®

NGFWService
- Application Signatures
- IPS Rules

Web FilterService
- Risk Ratings
- Category Designations

Antivirus Service
- Signature database
- Heuristic, emulation rules

FortiSandbox Cloud Service
- Full OS sandbox
- Callback detection

Mobile Malware Service
- Signature database

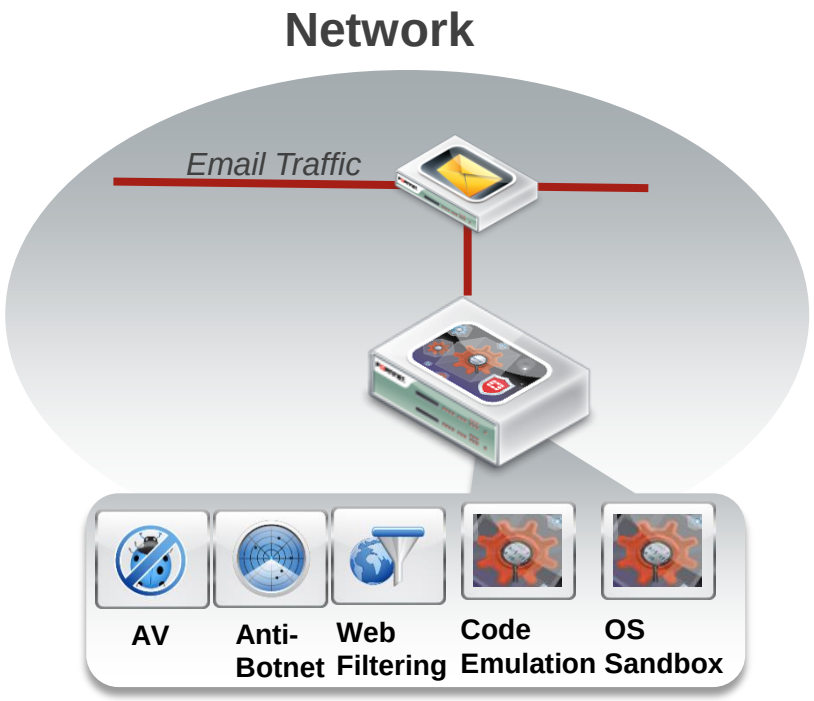
ADDRESSING ADVANCED THREATS

Secure Email Gateway

- Blocks known threats using connection, content, recipient intelligence and more
- Quarantines suspicious (or high risk) objects for more inspection
- Releases/deletes messages based on FortiSandbox risk rating

Sandbox for Payload Analysis

- Runs objects in a contained environment, analyzing activity
- Provides a malicious or low, medium or high risk rating
- Uncovers threat lifecycle information and allows information sharing with FortiGuard experts for protection updates



SEG: KEEP EMAIL CLEAN AND USERS PRODUCTIVE

- Connection level, header and full content inspection for spam
- Dedicated newsletter category and handling
- Top rated antimalware engine combining signature, heuristic, emulation and unpacking techniques
- Optional FortiSandbox integration

Independent Validation

ADVANCED SPAM AND ANTI-MALWARE PROTECTION

Low impact scanning

Avoid queuing mail when destination is available

- Global FortiGuard IP Reputation
- FortiGuard Botnet Tracking Database
- Local Dynamic Sender Reputation

- FortiGuard Spam Content Database
- Content & Behavior Based Heuristic Detection
- Mail Content URL Filtering – Adult, Malware

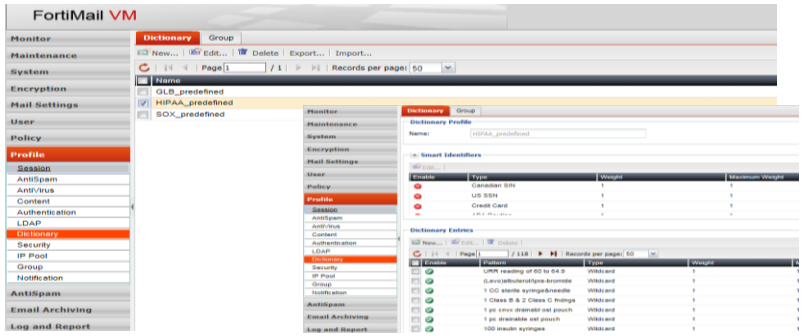
- FortiGuard Malware Detection
- Policy Based Archiving and Encryption

Reject spam at connection stage

Real time updated, 3rd party validated

FortiGuard Threat Research

DATA PROTECTION DETAIL



- **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**

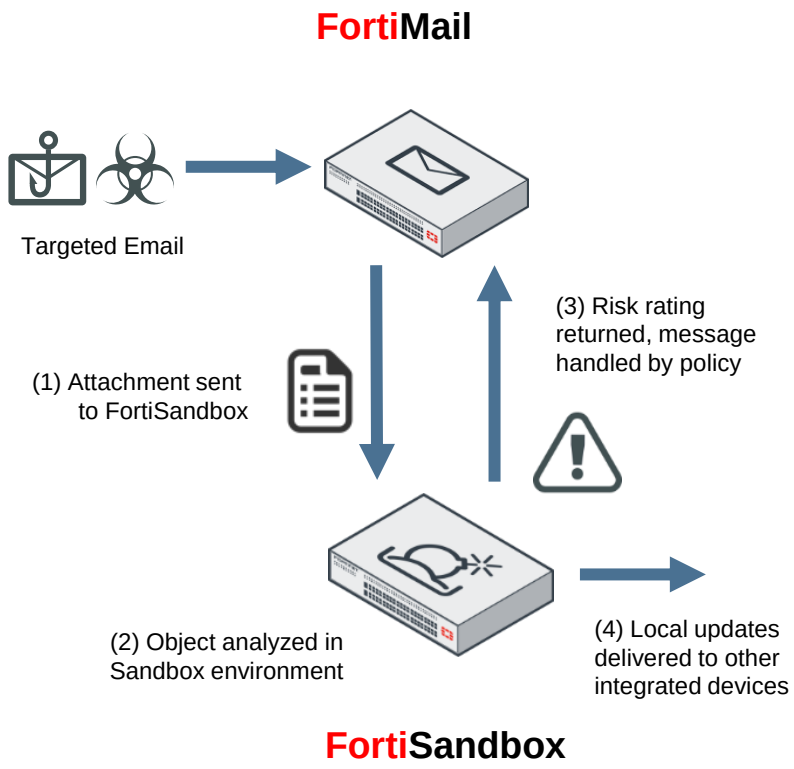
SEG –SANDBOX INTEGRATION

On the SEG Side

- Submit objects and URLs for additional analysis
- Control submissions based on File Type
- Queue messages during analysis
- Automatically handle messages based on results
- Access additional FortiSandbox intelligence through FortiGuard Labs

On the Sandbox Side

- Watch the wire for objects to analyze or indicators of command control activity
- Receive objects from FortiMail
- Analyze all objects and activity
- Assign and return a rating for the submission
- Dynamically generate/distribute threat intelligence



SECURED BY FORTIGUARD®

Antispam Service
- Sender IP reputation
- Heuristic rules
- Signature database
- Outbreak protection
- White/black list

Antivirus Service
- Signature database
- Heuristic, emulation rules

FortiSandbox Cloud Service* (5.3)
- Various pre-filters
- Full OS sandbox
- Callback detection

How does it all work?

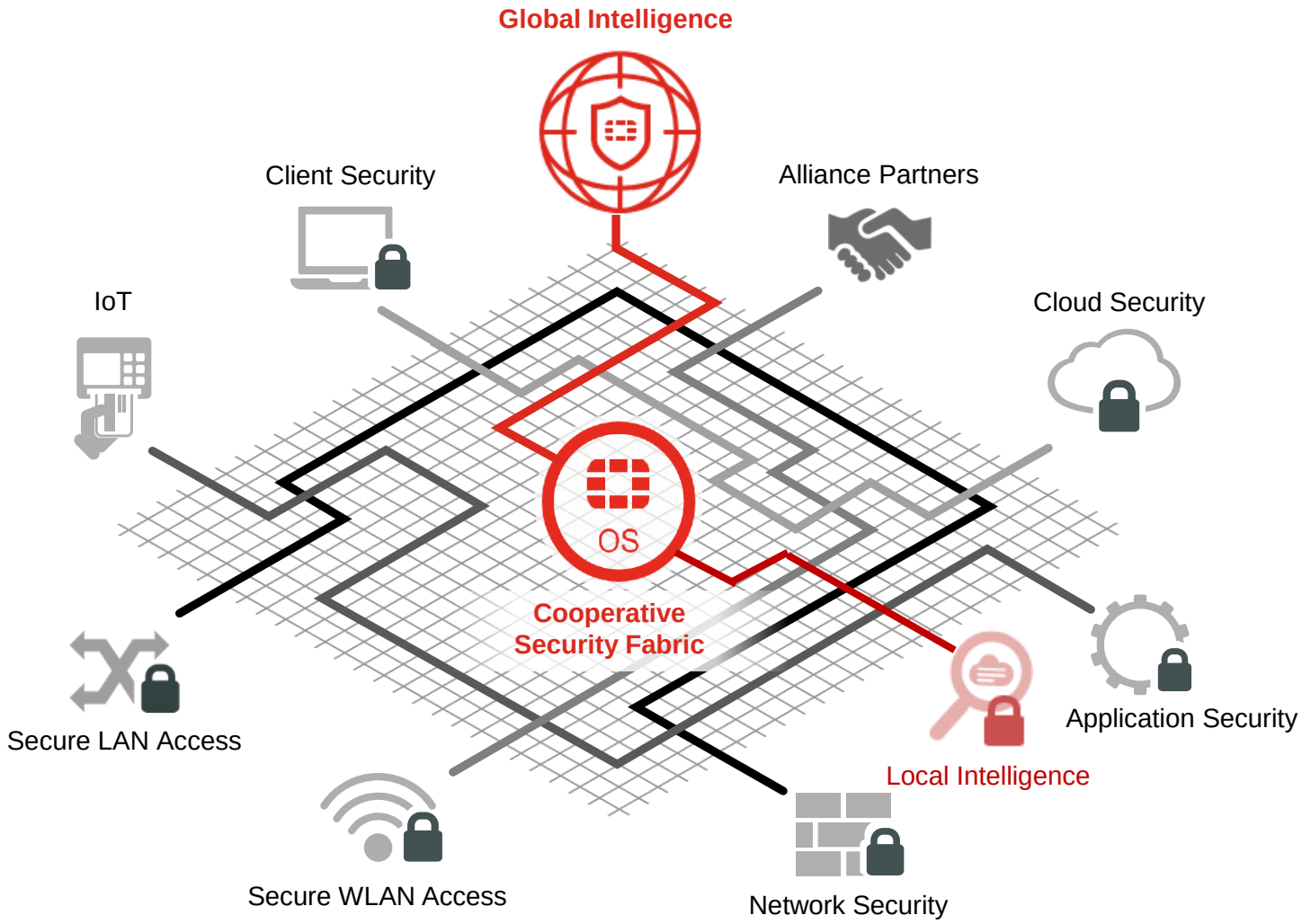
Scale

Awareness

Security

Actionable

Open



CERTIFICATIONS ARE KEY TO CUSTOMER TRUST

- NSS Labs
- Get The Edge

NSS BREACH DETECTION RESULTS

FORTINET

REPORT SUMMARY

NSS Labs 2016
Breach Detection System (BDS) Group Test Results

Nowhere to Hide – 100% Exploit and Evasion Detection
Fortinet Security Fabric, NSS Recommended Breach Detection

Highlights:

- 3rd annual BDS Test, 3rd NSS Recommendation for Fortinet FortiSandbox
- FortiSandbox Appliance (with FortiClient), FortiSandbox Cloud (and FortiGate) Recommended
- 100% detection of exploits and evasions, 99%+ overall effectiveness
- Exceptional Time to Detection at an average of 4.1 minutes by FortiSandbox Cloud
- 10Gbps real-world throughput by FortiSandbox 3000D, 1 Gbps by FortiGate+ FortiSandbox Cloud
- Fortinet NGFW, DCIPS, WAF, and EPP, also NSS Recommended along with BDS

Importance

There is arguably no industry more full of hype than the security industry. The number of vendor claims can quickly overwhelm customers seeking to better protect their organizations. In the subcategory of network sandboxing, the 2015 Gartner Market Guide identified more than 20 vendors and clearly there are many more than those noted.

As a result, there is no substitute for testing critical security products within an organization's production environment for an extended period of time. But expert independent testing has emerged as a critical shortlisting and decision-making tool for IT security teams. In this year's NSS Labs BDS testing, products were tested over a month-long period and subjected to more than 600 attacks. FortiSandbox showcased its ability to detect nearly all of them.

Exceptional Time to Detection

According to Verizon, 99% of malware is seen for 58 seconds or less, making time to detection and response critical. The FortiGate with FortiSandbox Cloud demonstrated exceptional time to detection (4.1 minutes).

4.1 minutes

Appliance or Cloud, Edge or Endpoint Integrated

Both the FortiSandbox appliance and cloud service successfully detected 99% or more of the attacks.

100% in Multiple Categories

both solutions were perfect in handling drive-by downloads, social exploits, and six classes of evasion including the use of SSL for evasion.

100%

Strong Enterprise Performance

The FortiSandbox appliance demonstrated 10 Gbps throughput for real-world protocol mix (enterprise perimeter) traffic, while the mid-range FortiGate 500D with FortiSandbox cloud showed 1Gbps throughput with full filtering.

10 Gbps

www.fortinet.com

Breach Detection Systems Security Value Map

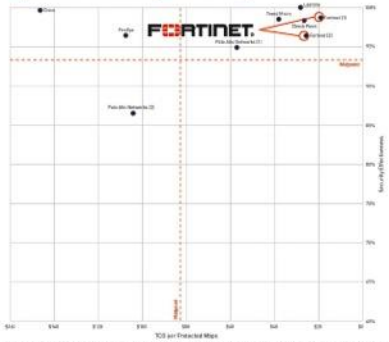


FIGURE 1 - NSS LABS' 2016 SECURITY VALUE MAP (SVM) FOR BREACH DETECTION SYSTEMS (BDS)

Fortinet Product Analysis Report Summary

PRODUCT	BREACH DETECTION RATE	NSS TESTED THROUGHPUT	3-YEAR TCO (LIST PRICE)	3-YEAR TCO (STREET PRICE)
Fortinet FortiGate 500D v5.4.1 with FortiSandbox Cloud Service	99.9%	1,000 Mbps	$ 22,350	$17,900

False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Offline Infections	Evasions	Stability & Reliability
0.00%	100.0%	100.0%	99.6%	100.0%	70.9%	100.0%	PASS

PRODUCT	BREACH DETECTION RATE	NSS TESTED THROUGHPUT	3-YEAR TCO (LIST PRICE)	3-YEAR TCO (STREET PRICE)
Fortinet FortiSandbox 3000D v2.1.0 with FortiClient v5.4.1.0640	99.9%	5,000 Mbps	$ 274,585	$255,050

False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Offline Infections	Evasions	Stability & Reliability
2.63%	100.0%	100.0%	98.5%	99.1%	100%	100.0%	PASS

Closing Remarks

Cybercriminals are evolving new attack strategies at an alarming rate and creating a situation in which the time from breach to full compromise occurs in minutes. This makes rapid detection and automated response a key component for defense. We're honored to receive NSS Labs Recommendations for Breach Detection, which reinforce the superior effectiveness of our sandbox solutions as well as the fastest time to detection when using our latest version of FortiSandbox. These new test results, combined with additional NSS Labs Recommended components across our Security Fabric, complete the critical steps of converting rapid detection into automatic mitigation to protect against the most advanced threats facing organizations today.

For More Information

Fortinet Advanced Threat Protection Solution Page
Full NSS Labs Test Reports

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33.4 8987 0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Aug 1, 2016

SOLUTION SPOTLIGHT: SIEM

BUSINESS DRIVERS FOR A SIEM

believe IoT is the biggest future concern (#1 answer) – Black Hat

believe they do not have the staff to defend – Black Hat

of Boards concerned to very concerned about cyber security – ISACA

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

Moblility/BYOD

SIEM vs. ForitSIEM

Single Pane of Glass

Only NOC & SOC Analytics

Rapid & Flexible Integrations

Multi-Tenant Architecture

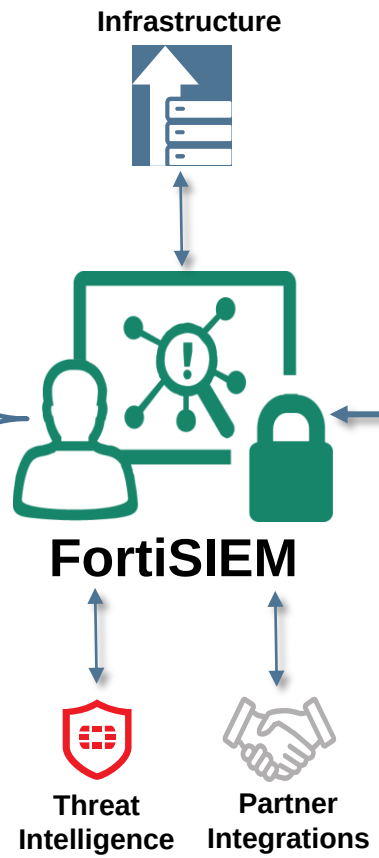
Rapid Scale Architecture

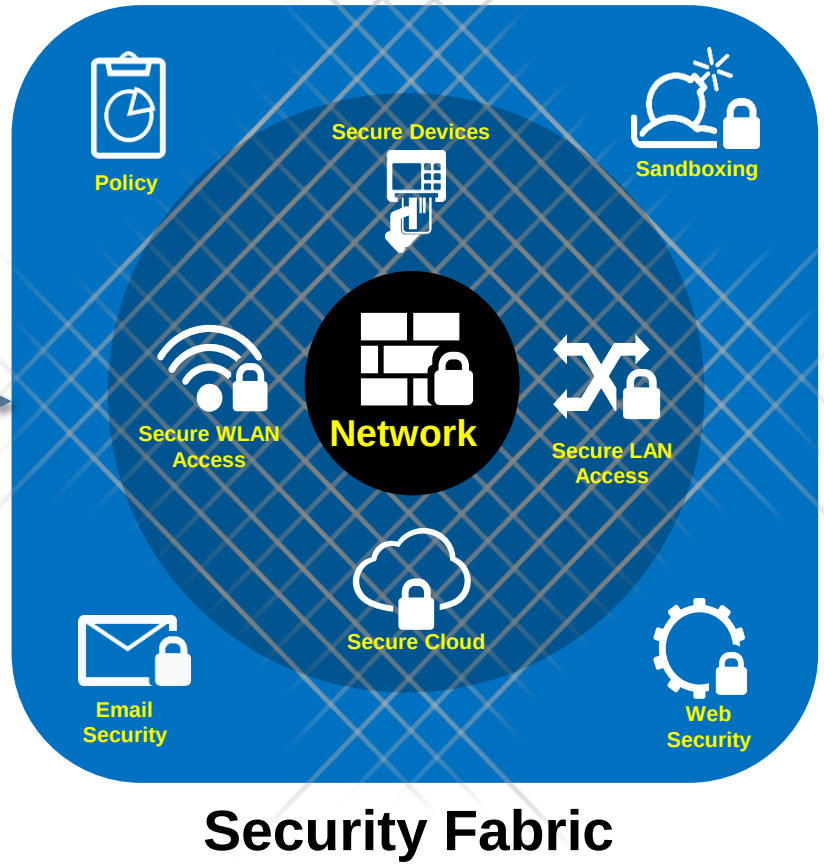
Real-Time Asset/Config. Discovery

Real-Time Analytics (patented)

Gartner SIEM Criteria

- Analytics
- Application Log Analysis
- Behavior Profiling
- Data & User Monitoring
- Deployment/Support Simplicity
- Log Management
- Real-Time Monitoring
- Threat Intelligence





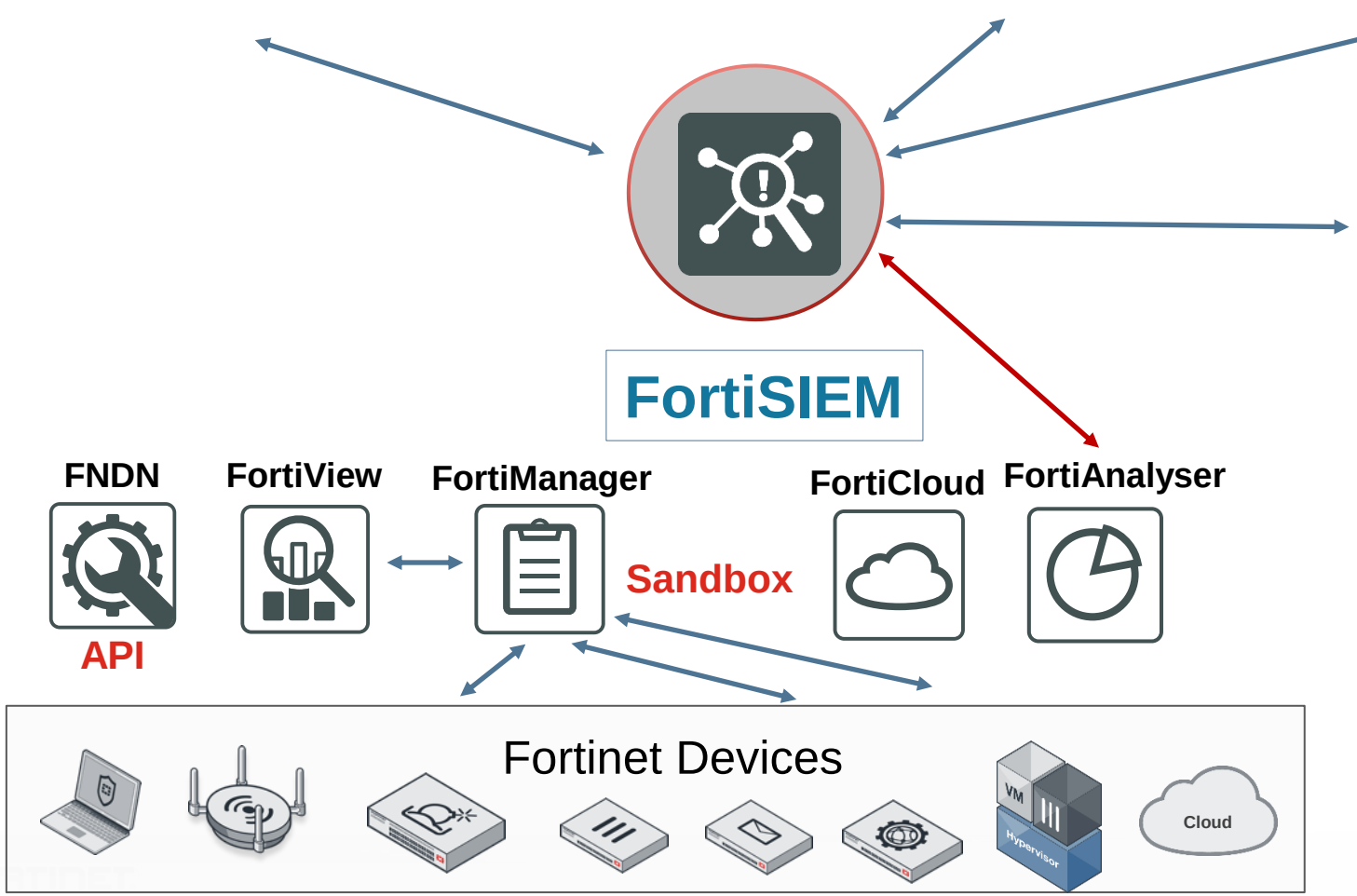
Security Fabric

SECURITY OPERATIONS ANALYTICS PRODUCTS AND SERVICES

Assets, Configuration, Policy & PAM Visualization

Performance, Compliance, Security Analytics

Threat Intelligence And Operations



- Web Proxies/VPN/Anti Virus
- Individual End Points
- Business Applications
- Cloud - Public/Private/Hybrid
- IPS/IDS Devices
- Servers (Physical/Virtual)/Databases
- Routers, Switches, Firewalls

TYPICAL NOC/SOC ENVIRONMENT

NOC

PRTG NETWORK MONITOR

Nagios

Kaseya

ScienceLogic

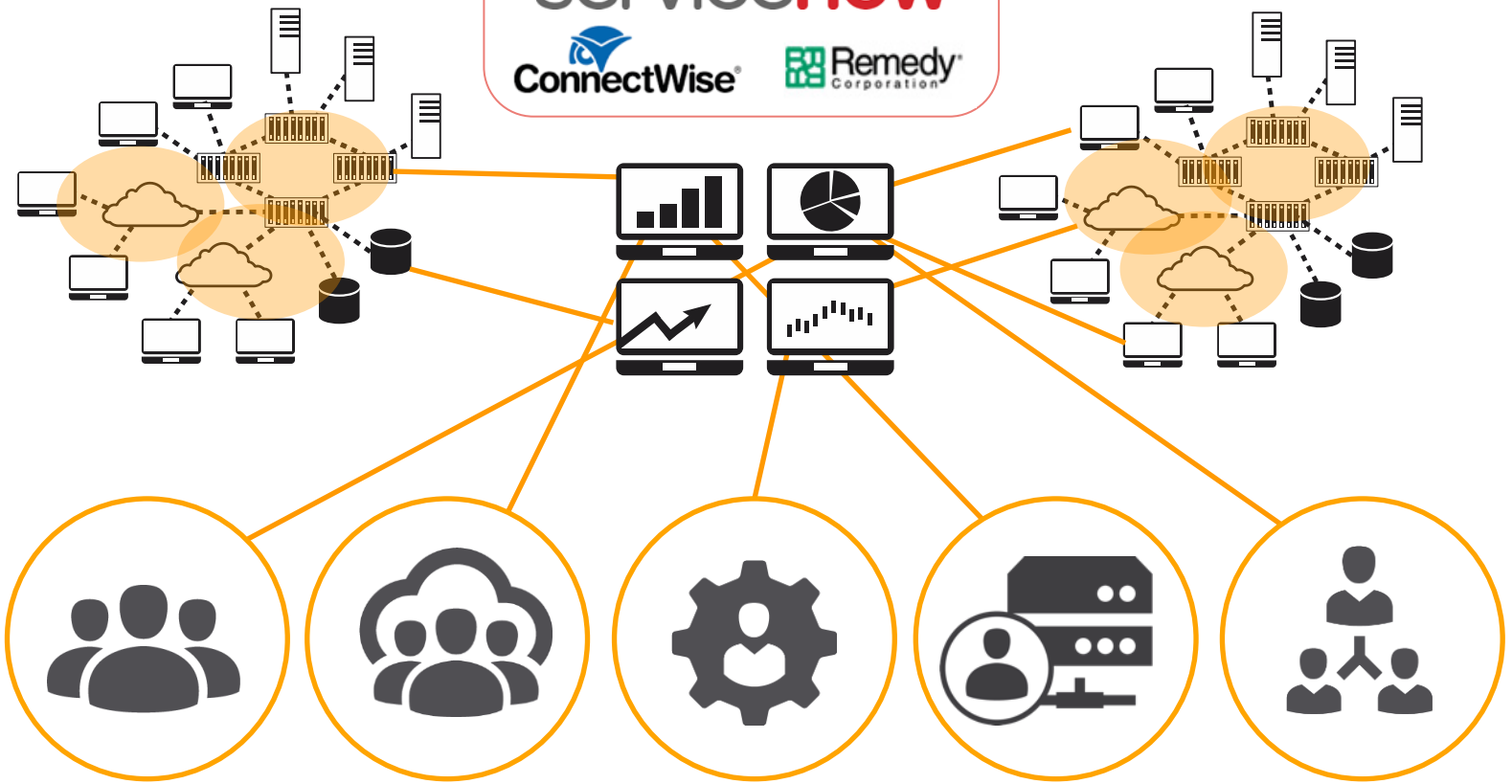
WIRESHARK

Ticketing Systems

servicenow

ConnectWise

Remedy Corporation



SOC Team

NOC Team

Help Desk

Datacenter Director

Systems, Admin

SOC

NetIQ

loggly

TIBCO

tripwire

sumologic

FLEXIBLE TECHNOLOGY INTEGRATIONS

FORTISIEM KEY DIFFERENTIATORS

- Only NOC & SOC solution in a “Single Pane of Glass”

  Holistic “Unified Network Analytics” view of events across the entire organization

- Real-Time Correlation of Security & Network Threats

  Rapid identification, triage and future prevention

- Powerful Automated Device Discovery Engine

  Self-Learning, Real-Time CMBD

- Large inbuilt knowledge base

  IT community in a box 200+ log parsing templates, 150K normalized event types, 2000+ reports, 500+ correlation rules

- Multi-Tenant Architecture

  Segment network views into physical, logical dashboards


FORTINET