Advanced Threat Protection – wie schütze ich mein Unternehmen vor dem Unbekannten?

Jürgen Hofmann Senior Systems Engineer

© Copyright Fortinet Inc. All rights reserved.

Fortinet Facts

FOUNDED
2000

IPO
2009

$1.17B
CASH

40%
GROWTH

HQ
SUNNYVALE, CA

100+
OFFICES
WORLDWIDE

4200+
EMPLOYEES

255,000+
CUSTOMERS

OVER
2,2 MILLION
DEVICES SHIPPED

#1 UNIT SHARE
WORLDWIDE
In Network Security (IDC)

MARKET LEADING
TECHNOLOGY
257 PATENTS
228 PENDING

Fortinet Customers

7 of the **TOP 10**
Fortune Companies
in **America**

8 of the **TOP 10**
Fortune Companies
in **EMEA**

9 of the **TOP 10**
Fortune Companies
in **APAC**

10 of the **TOP 10**
Fortune Telecommunications
Companies

9 of the **TOP 10**
Fortune Retail and Commercial Banks

7 of the **TOP 10**
Aerospace and
Defense

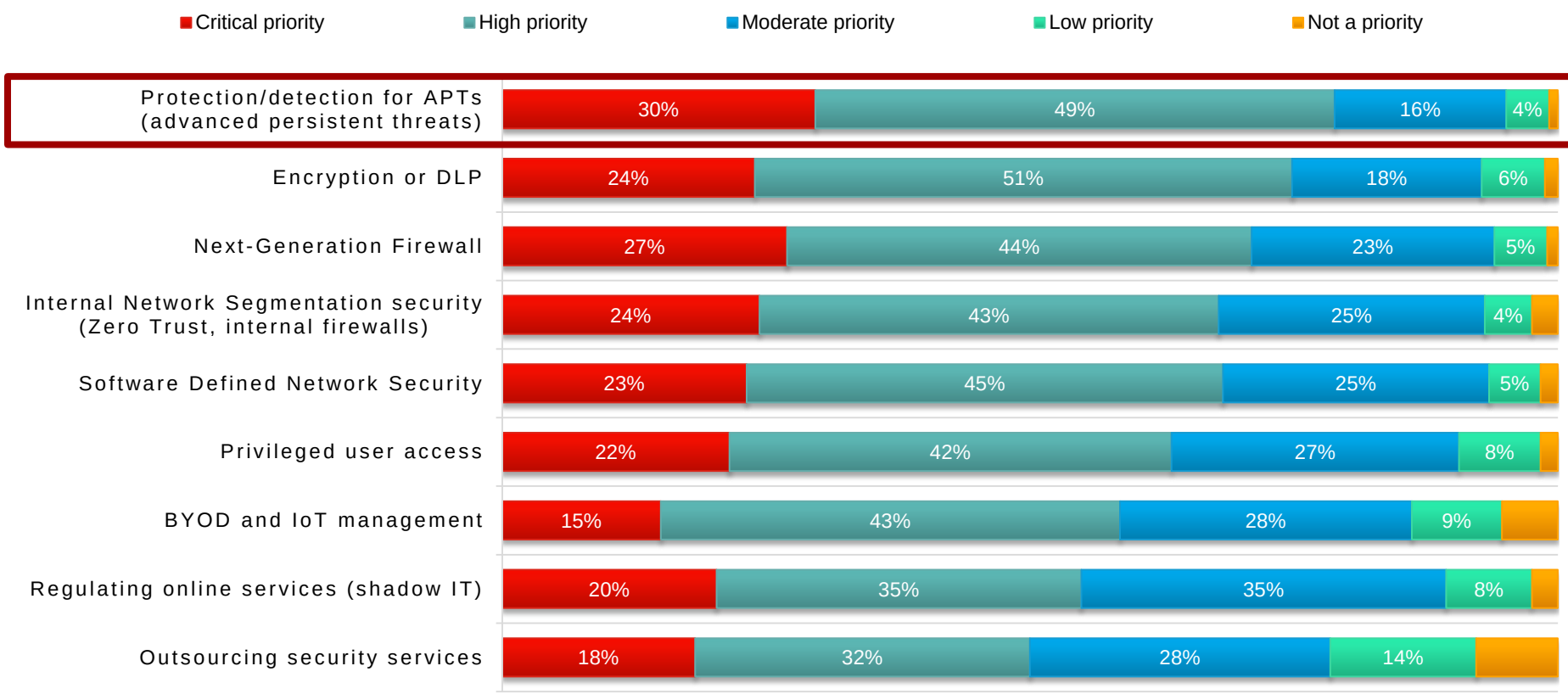
Agenda

- Market Situation
  - ✓ Breaches, Priorities and Options
  - ✓ Why Sandboxing
- Introduction to FortiSandbox
  - ✓ What it is and does
  - ✓ Key components
- What makes FortiSandbox different
  - ✓ Compared to stand-alone approaches
  - ✓ Compared to integrated offerings
- Fortinet Advanced Threat Protection and Security Fabric
  - ✓ Fortinet Advanced Threat Protection
  - ✓ Fortinet Security Fabric
- Recap and Discussion

Market Situation

APTs, Data Breaches Top of Mind

Priority of IT Security Initiatives in 2016



	2016 Critical/ High Priority	2015 Critical/ High Priority
Protection/detection for APTs (advanced persistent threats)	79%	77%
Encryption or DLP	75% ↑	67%
Next-Generation Firewall	71%	75%
Internal Network Segmentation security (Zero Trust, internal firewalls)	68%	N/A
Software Defined Network Security	68%	N/A
Privileged user access	63% ↓	71%
BYOD and IoT management	59%	N/A
Regulating online services (shadow IT)	55%	58%
Outsourcing security services	50% ↓	60%

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

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

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

News Heise: **Neues von Locky: Der Erpressungstrojaner greift jetzt massenhaft Krankenhäuser an** 19.08.2016

Die Drahtzieher hinter Locky verlegen sich von X-beliebigen Internetnutzern auf Firmen. Vor allem Krankenhäuser haben sich als lukratives Ziel erwiesen.

Ende Mai sah es noch so aus, als wäre Locky spurlos aus dem Netz verschwunden, dann meldete sich der Erpressungstrojaner keinen Monat später fulminant zurück. Nun greifen Kriminelle gezielt Krankenhäuser an – momentan vor allem in den USA und in Asien. Anstatt Javascript-Anhängen enthalten deren Spam-Mails nun .docm-Dateien, also Makro-fähige .docx-Dokumente. Die Makros enthalten dabei Schadcode, der den Erpressungstrojaner auf das System des Opfers läd, wie die Sicherheitsfirma FireEye berichtet.

Die Spam-Kampagne gibt sich wohl relativ viel Mühe, Mitarbeiter in den einzelnen Krankenhäuser gezielt anzusprechen. Die Forscher haben personalisierte Mails für jede der verschiedenen Ziel-Organisationen entdeckt. Neben Krankenhäusern wurden aber auch Firmen aus anderen Geschäftszweigen angegriffen. Die Beobachtungen scheinen darauf hinzudeuten, dass sich die Drahtzieher hinter Locky von Massenangriffen auf alle Internetnutzer hin zu gezielten Attacken auf lukrativere Ziele verlegt haben. Immer noch steht Deutschland auf Platz 6 der Spam-Ziele.

FireEye hat ebenfalls beobachtet, dass die Gruppe hinter den Angriffen sich mehr und mehr auf Locky konzentrieren zu scheint. Angriffe mit dem Banking-Trojaner Dridex, der ebenfalls von den selben Kriminellen stammen soll, lassen demnach nach. Die Sicherheitsfirma vermutet deshalb, dass Erpressungstrojaner mittlerweile lukrativer sind als Banking-Malware. (fab)

Kommentare lesen (8 Beiträge) « Vorige | Nächste »

Forum zum Thema: **Desktopsicherheit**

teilen 26 | tweet | teilen 6 | mail

http://heise.de/-3300555 Drucken

How Does it Remain Undetected? Unique Code.

99.5%

Of Malware samples are Unique to an Organization

Code Continuum	Known Good	Probably Good	Might be Good	Completely Unknown	Somewhat Suspicious	Very Suspicious	Known Bad
Security Technologies	**Whitelists**	**Reputation:** File, IP, App, Email App Signatures, Digitally singed files				**Heuristics Reputation:** File, IP, App, Email Generic Signatures	**Blacklists Signatures**

Source:
Verizon 2016 Data Breach Investigations Report, April 2016

How Should We Address it? Sandboxing.

99.5%

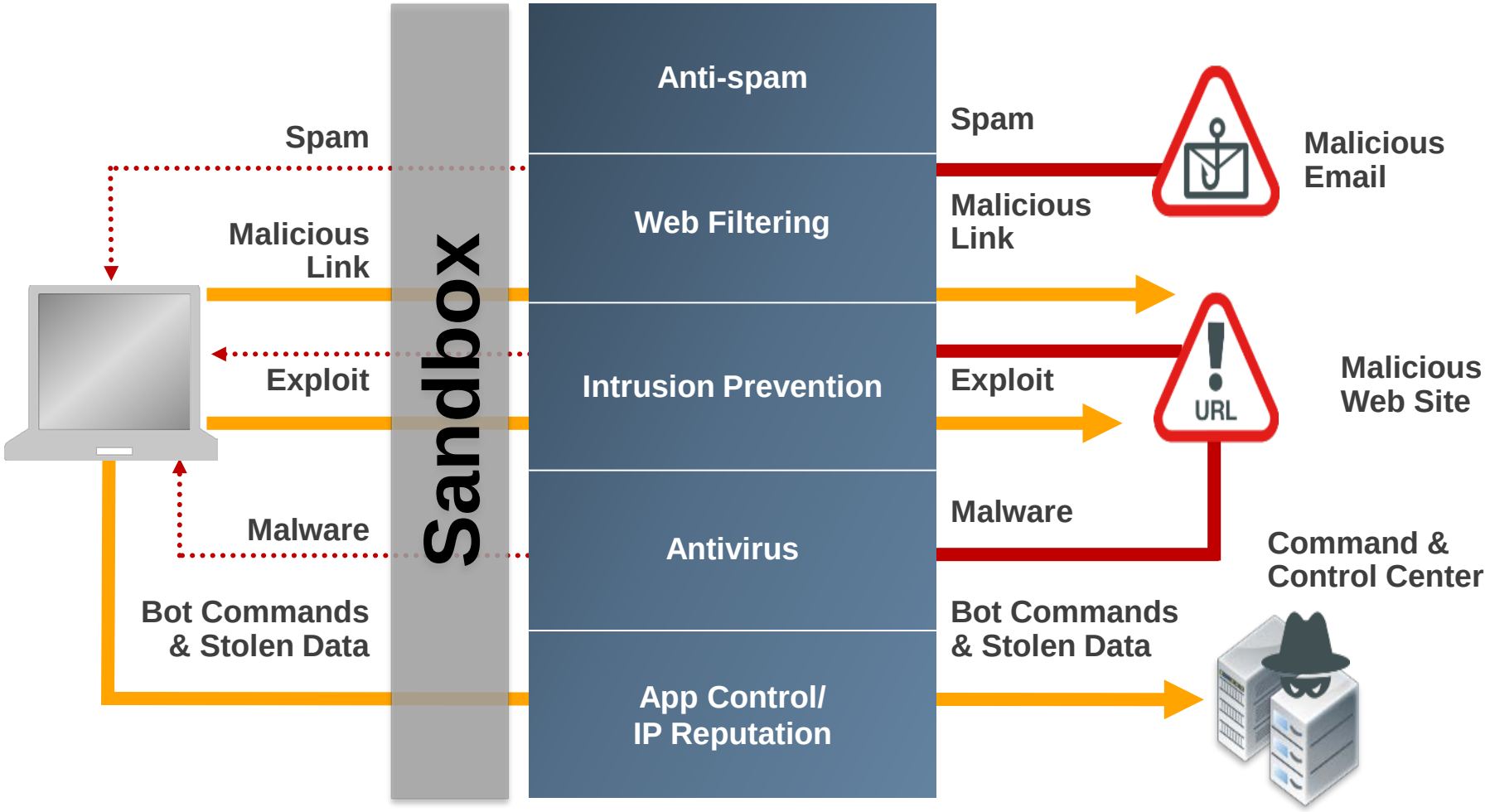
Of Malware samples are Unique to an Organization

Code Continuum	Known Good	Probably Good	Might be Good	Completely Unknown	Somewhat Suspicious	Very Suspicious	Known Bad
Security Technologies	**Whitelists**	**Reputation:** File, IP, App, Email App Signatures, Digitally singed files	**Sandboxing**			**Heuristics Reputation:** File, IP, App, Email Generic Signatures	**Blacklists Signatures**

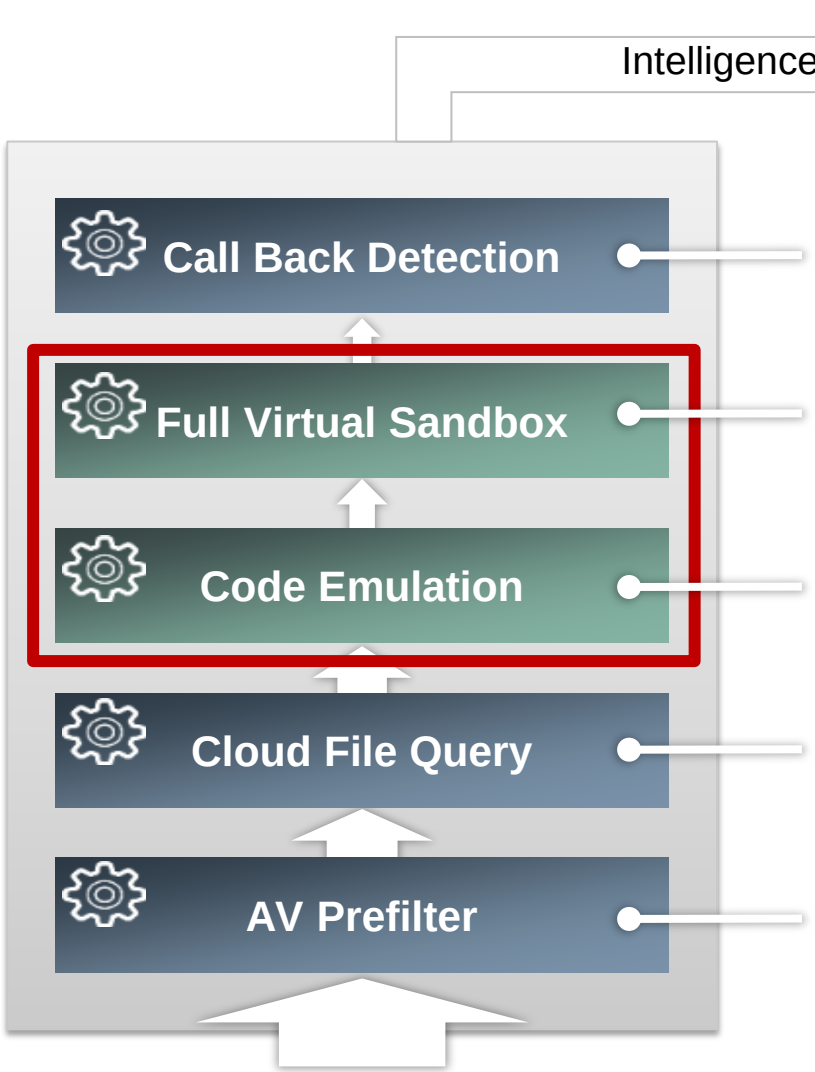
Source:
Verizon 2016 Data Breach Investigations Report, April 2016

FortiSandbox Introduction

Breaking the Kill Chain of Advanced Threats



Key FortiSandbox Components



- Distribute real-time updates
- Feed global systems

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

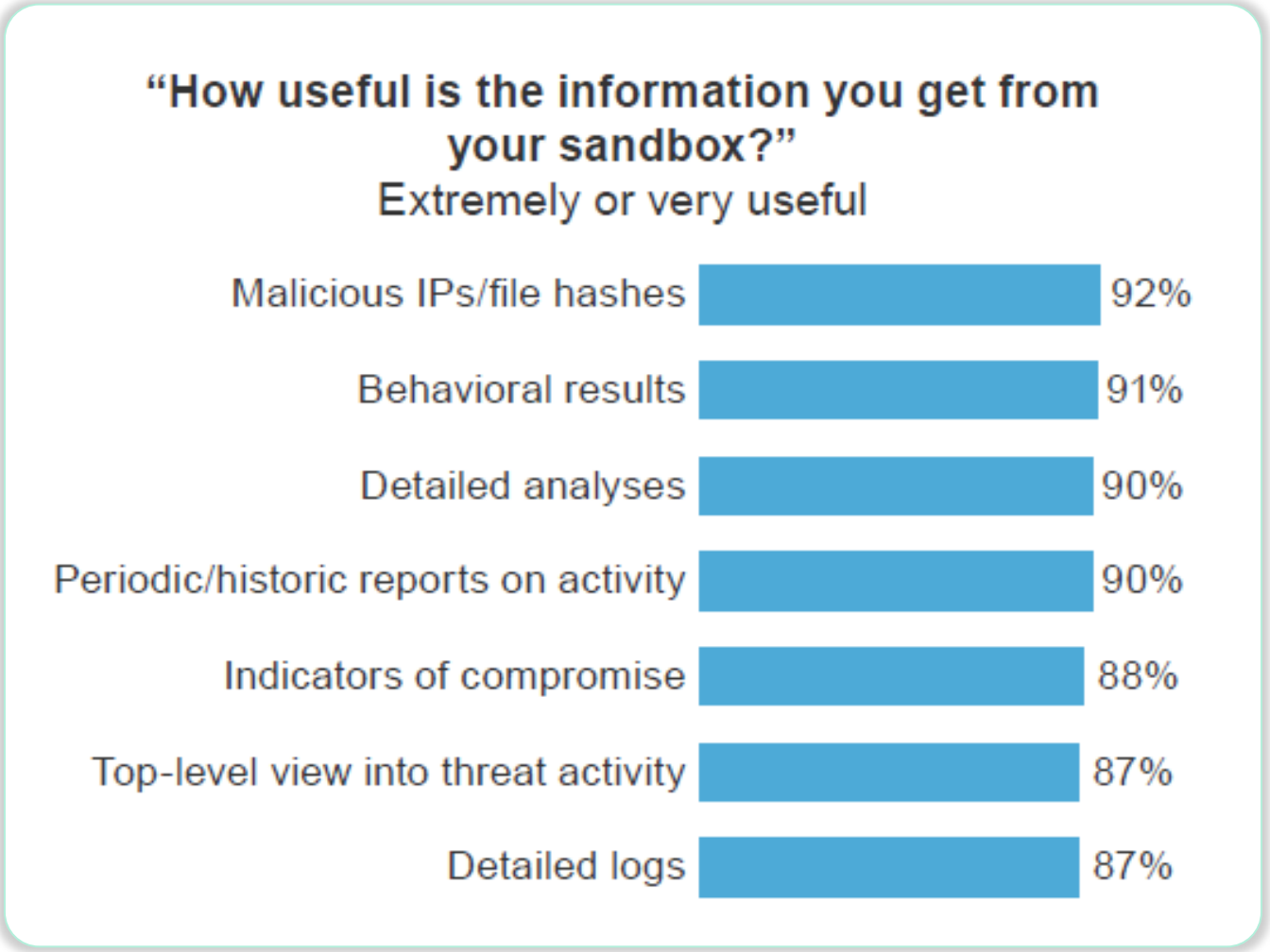
- Examine real-time, full lifecycle activity to get the threat to expose itself

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

- Check community intelligence & file reputation

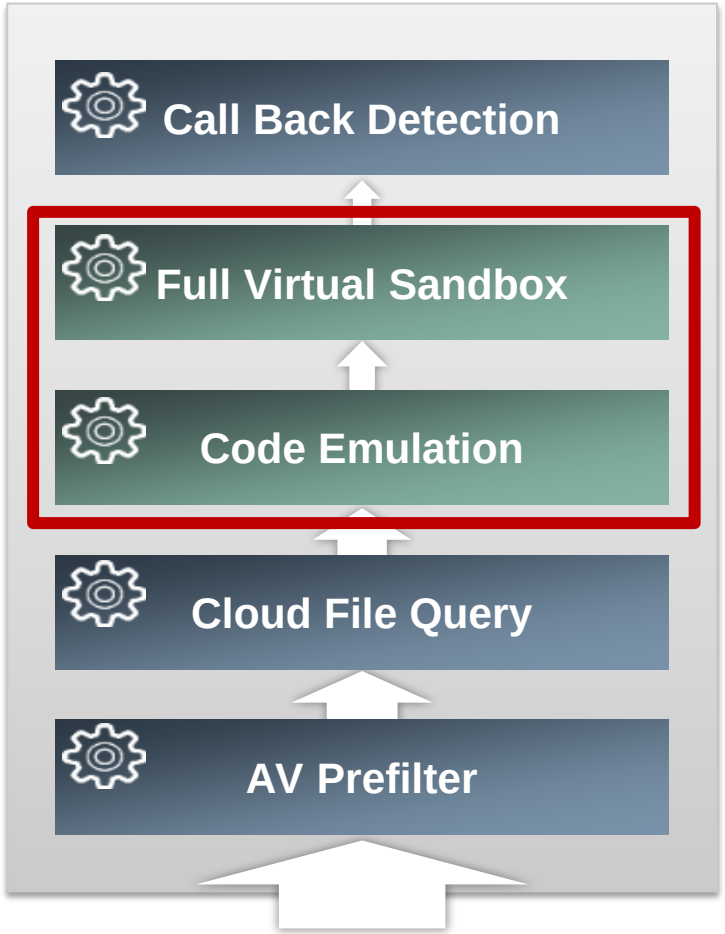
- Apply top-rated anti-malware engine

Does Sandboxing Really Work?



Source: Forrester Sandbox Survey, August 2015

What Exactly FortiSandbox Tells You



High Risk Unknown

Mark as clean (false positive)

Received	May 20 2016 13:28:32
Started	May 20 2016 13:28:35
Status	Done
Rated By	VM Engine
Submit Type	FortiGate
Source IP	172.20.2.50
Destination IP	172.20.1.50
Digital Signature	No
Scan Bypass Configuration	N/A

More Details

Behavior Summary

- This file visit webpage with certain URL
- This file connect to certain IP Addresses
- This file has network traffic
- This file dropped files
- This file modified files
- This file deleted files
- This file tried to delete massive files
- This file applied autostart registry modifications
- This file spawned process(es)

Analysis Details

Packer	N/A
File Type	exe
Downloaded From	http://172.20.1.50/2dcee7ca4b00f6a57ef7d561d0b777d8

WIN7X64VM | WINXPVM1 | WIN7X86VM

Captured Packets | Tracer Package | Tracer Log | Screenshot

Behavior Chronology Chart

Threat Level

12:25:00 12:30:00 12:35:00 12:40:00 12:45:00 12:50:00 12:55:00 13:00:00 13:05:00 13:10:00 13:15:00 13:20:00 13:25:00

Time

Medium Risk · Low Risk · Clean

Suspicious Behaviors (5)

- Suspicious IP
- Executable deleted itself after execution
- Delete massive files
- Suspicious registry
- Executable attempt to connect to remote CnC botnet server

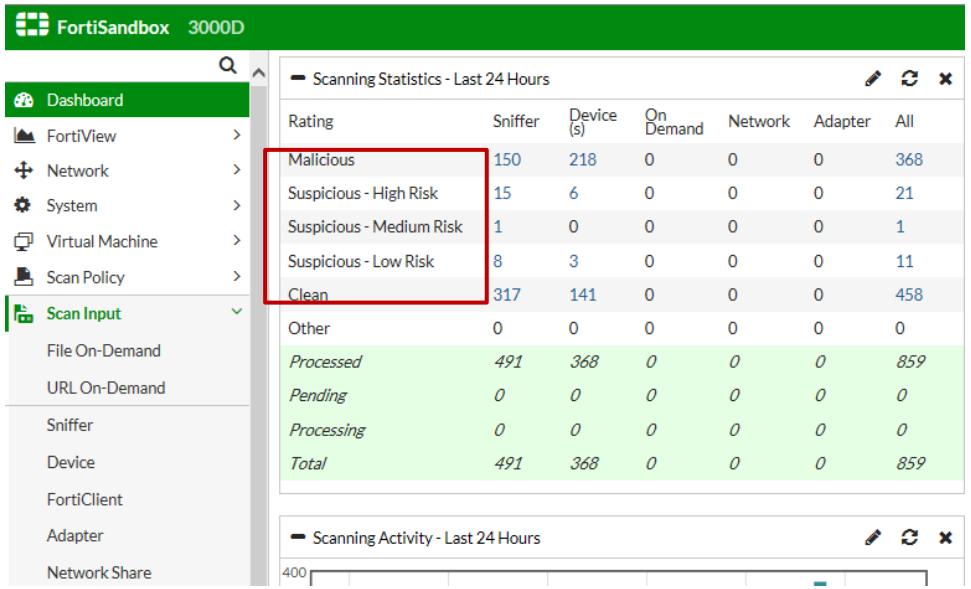
Static Analysis (1)

Files Created (460)

FortiSandbox 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

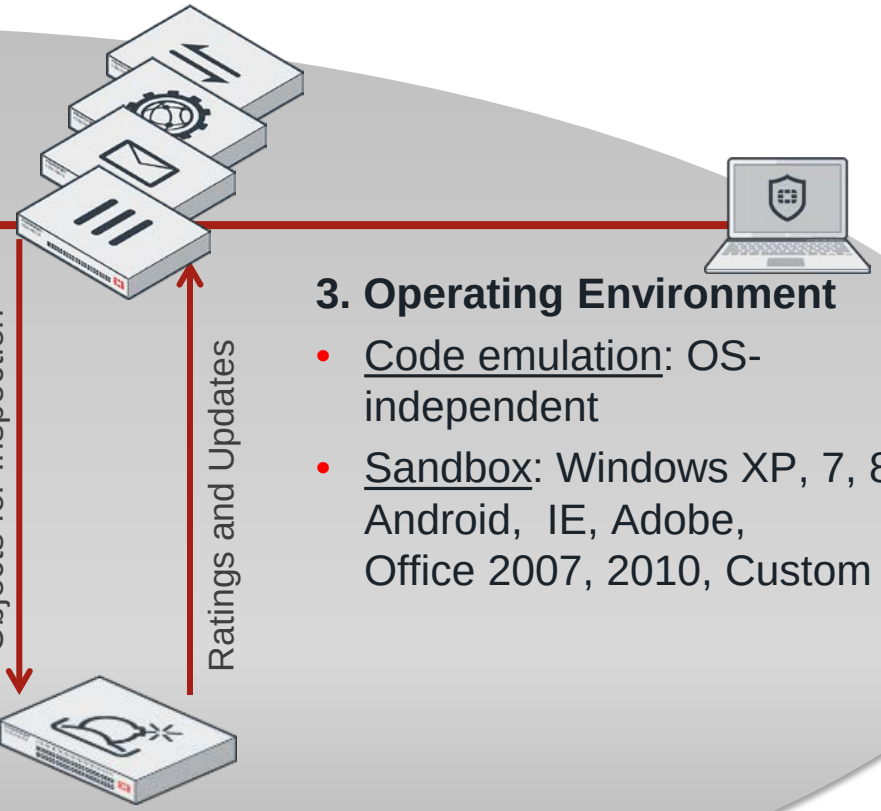


Rating	Sniffer	Device (s)	On Demand	Network	Adapter	All
Malicious	150	218	0	0	0	368
Suspicious - High Risk	15	6	0	0	0	21
Suspicious - Medium Risk	1	0	0	0	0	1
Suspicious - Low Risk	8	3	0	0	0	11
Clean	317	141	0	0	0	458
Other	0	0	0	0	0	0
Processed	*491*	*368*	*0*	*0*	*0*	*859*
Pending	*0*	*0*	*0*	*0*	*0*	*0*
Processing	*0*	*0*	*0*	*0*	*0*	*0*
Total	*491*	*368*	*0*	*0*	*0*	*859*

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

FortiSandbox Details



Network Traffic

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

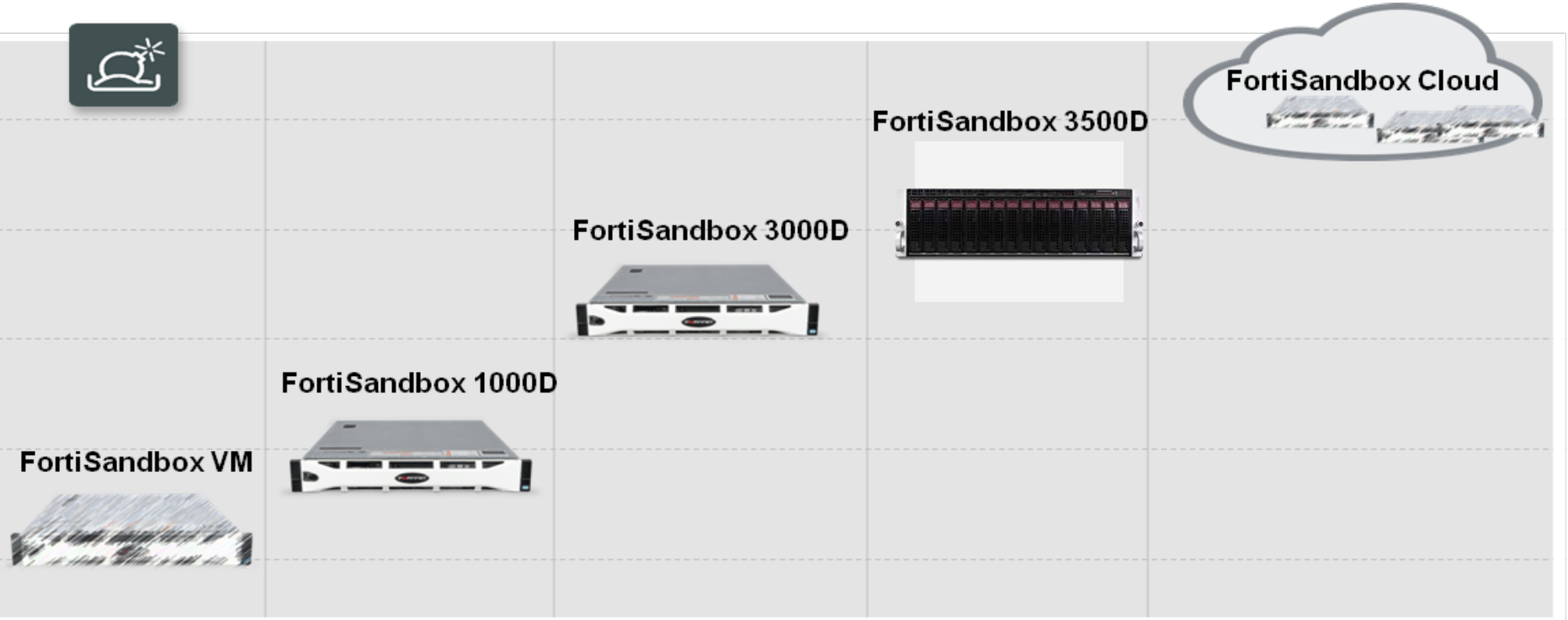
2. File type support

- AV Prefilter: all
- Full Sandbox: as follows
  - ✓ Archived: .tar, .gz, .tar.g, .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

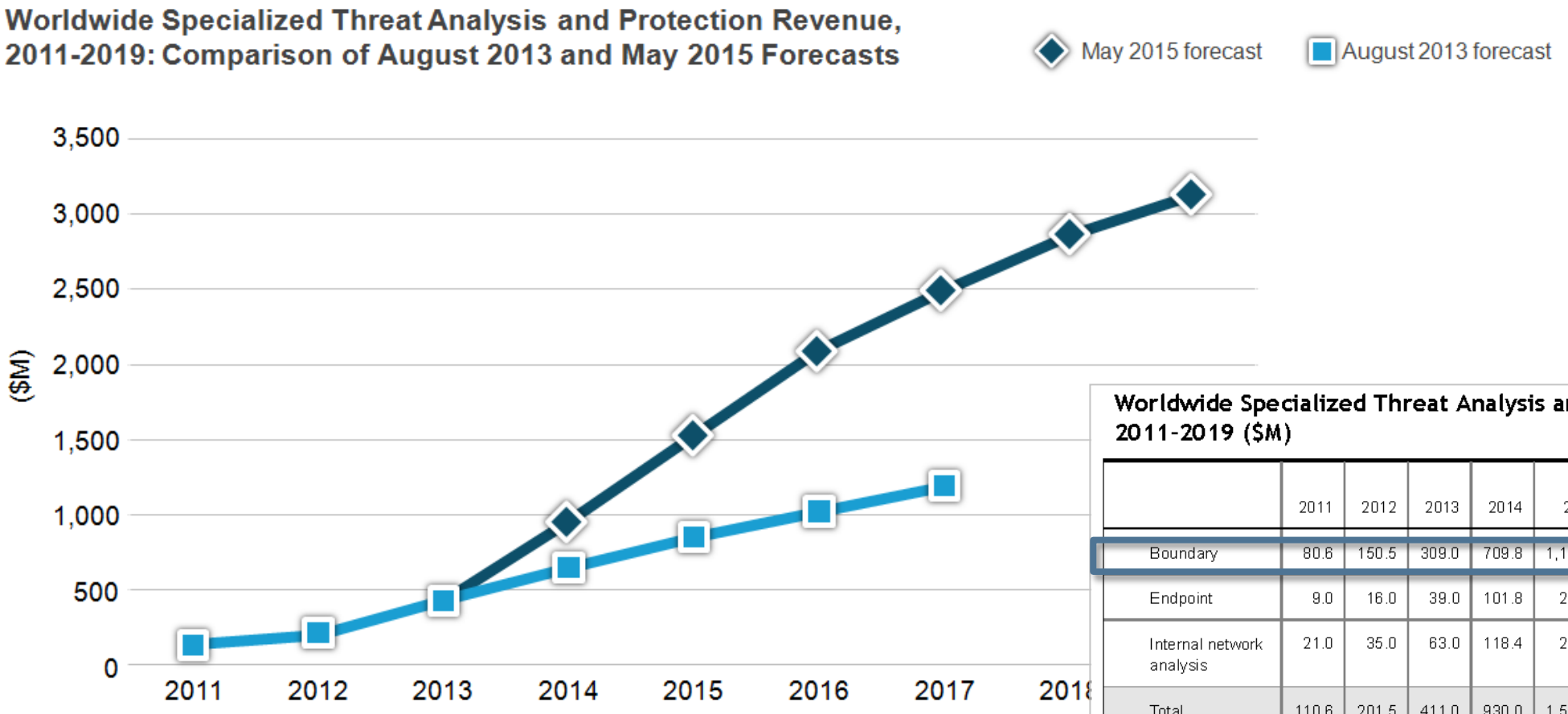
- Code emulation: OS-independent
- Sandbox: Windows XP, 7, 8, 10, Android, IE, Adobe, Office 2007, 2010, Custom VM

FortiSandbox Form Factors



	FortiSandbox VM	FortiSandbox 1000D	FortiSandbox 3000D	FortiSandbox 3500D	FortiSandbox Cloud
VMs	2+	8	28	64	As needed
Sandboxing (Files/hr)	Depends on hardware	160	560	1280*	As needed
AV Scanning (files/hr)	Depends on hardware	6,000	15,000	48,000*	As needed

IDC Forecasts Spending of $2bn…Mostly on Sandboxing



Worldwide Specialized Threat Analysis and Protection Revenue by Segment, 2011-2019 ($M)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2014–2019 CAGR (%)
Boundary	80.6	150.5	309.0	709.8	1,119.7	1,444.3	1,653.4	1,845.3	2,001.6	23.0
Endpoint	9.0	16.0	39.0	101.8	212.7	353.2	494.4	618.0	716.9	47.8
Internal network analysis	21.0	35.0	63.0	118.4	202.5	287.6	342.2	386.7	421.5	28.9
Total	110.6	201.5	411.0	930.0	1,535.0	2,085.0	2,490.0	2,850.0	3,140.0	27.6
Growth (%)	NA	82.2	104.0	126.3	65.1	35.8	19.4	14.5	10.2	

What Makes FortiSandbox Different

What Makes Fortinet Different Than…

FireEye

- No Integrated Mode
- Protocol and Function-specific Sandboxes
- Physical Appliance Only

paloalto NETWORKS

- Fewer Integration Points (no WAF, SEG, EPP)
- Real-time Intelligence Exchange
- Viable On-Premise

CISCO

- Fewer Integration Points (no WAF or EPP)
- No Real-time Intelligence Exchange
- Complex Deployment

McAfee An Intel Company

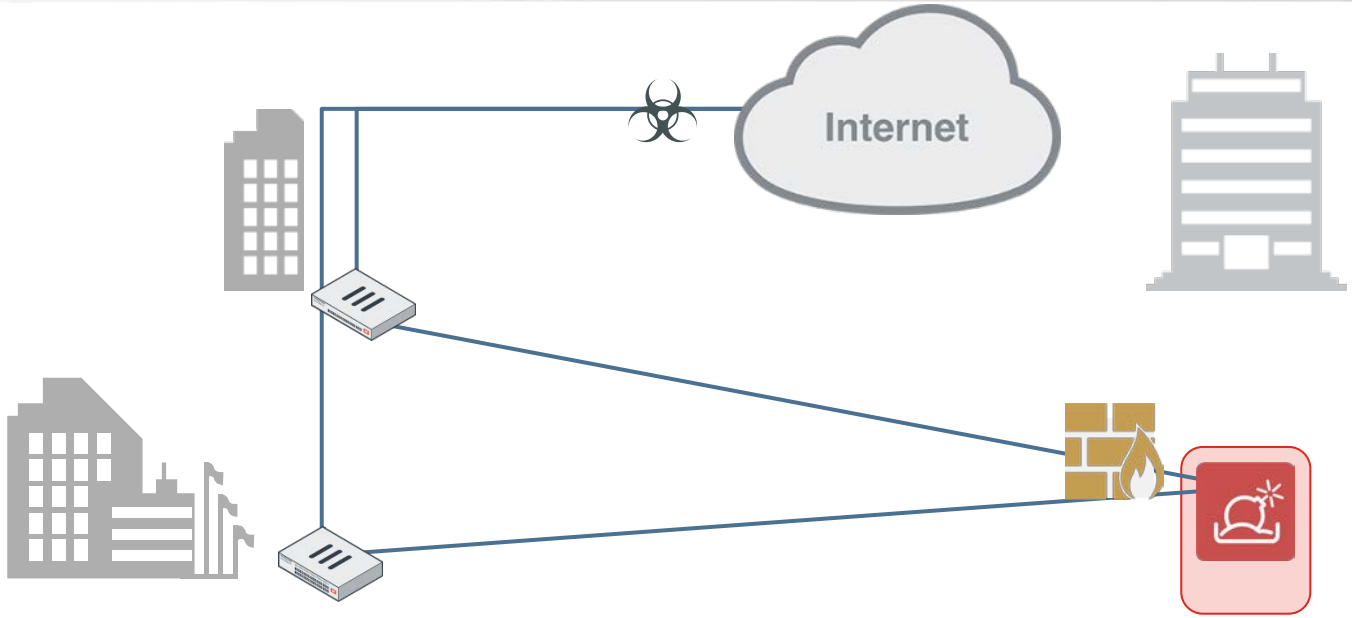
- More Integration Points (no NGFW, SEG, WAF)
- No Independent Validation (NSS Labs, ICSA)

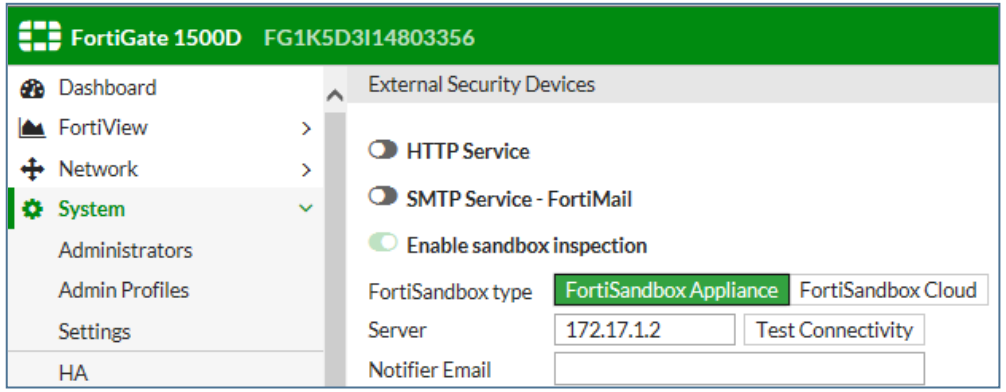
Our Integrated Approach Sets Us Apart

	Segment			Platform		Threat Vector Integrated				Certification	
Vendor	SMB	ENT	VLE	On-premise	Cloud	Firewall	Email	WAF	Client	NSS	ICSA
FORTINET	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
TREND MICRO	X	✔	✔	✔	X	X	✔	X	✔	✔	✔
Check Point SOFTWARE TECHNOLOGIES LTD.	X	✔	X	✔	✔	✔	X	X	X	✔	X
Symantec	X	✔	✔	X	✔	X	✔	X	✔	X	✔
paloalto NETWORKS	X	✔	X	✔	✔	✔	X	X	✔	X	✔
FireEye	X	X	✔	✔	✔	X	✔	X	✔	X	X

Fortinet Advanced Threat Protection Solution

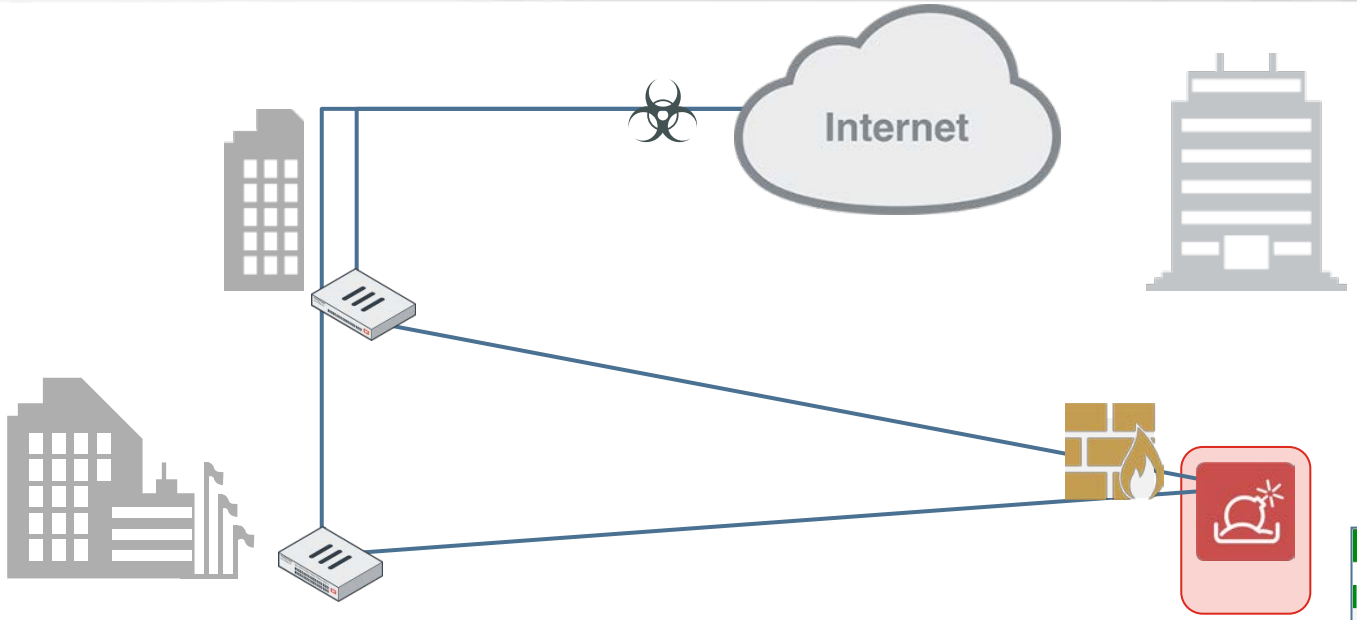
#1 ATP Use Case: NGFW + Sandbox Share Objects and Info

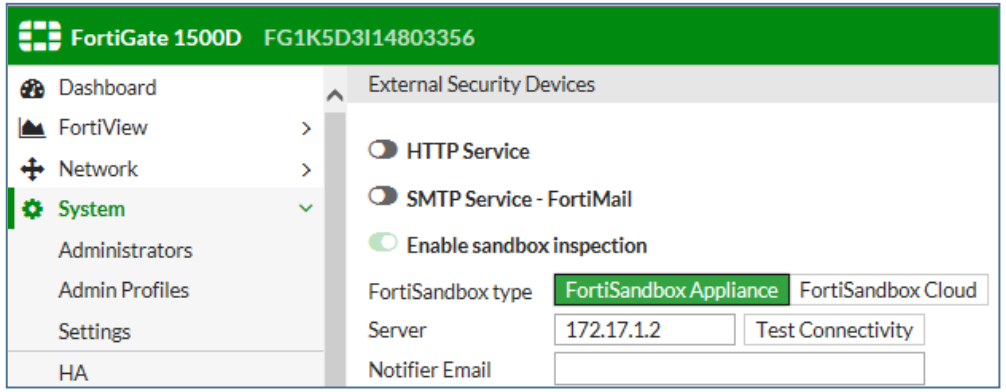


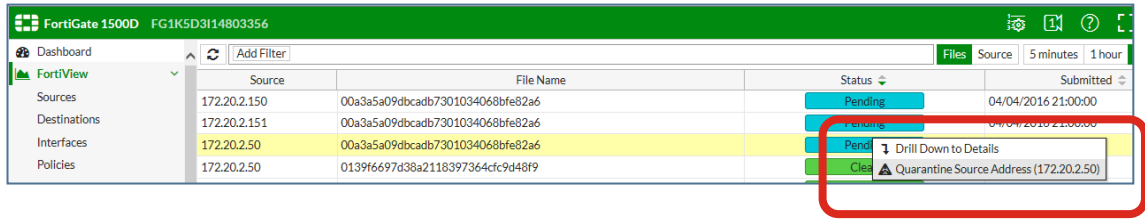


- FortiGate blocks as much as it can, routes remaining objects to FortiSandbox
- FortiSandbox returns ratings and updates
- FortiGate admin quarantines device, FortiGate starts blocking new threats

#1 ATP Use Case: NGFW + Sandbox Share Objects and Info

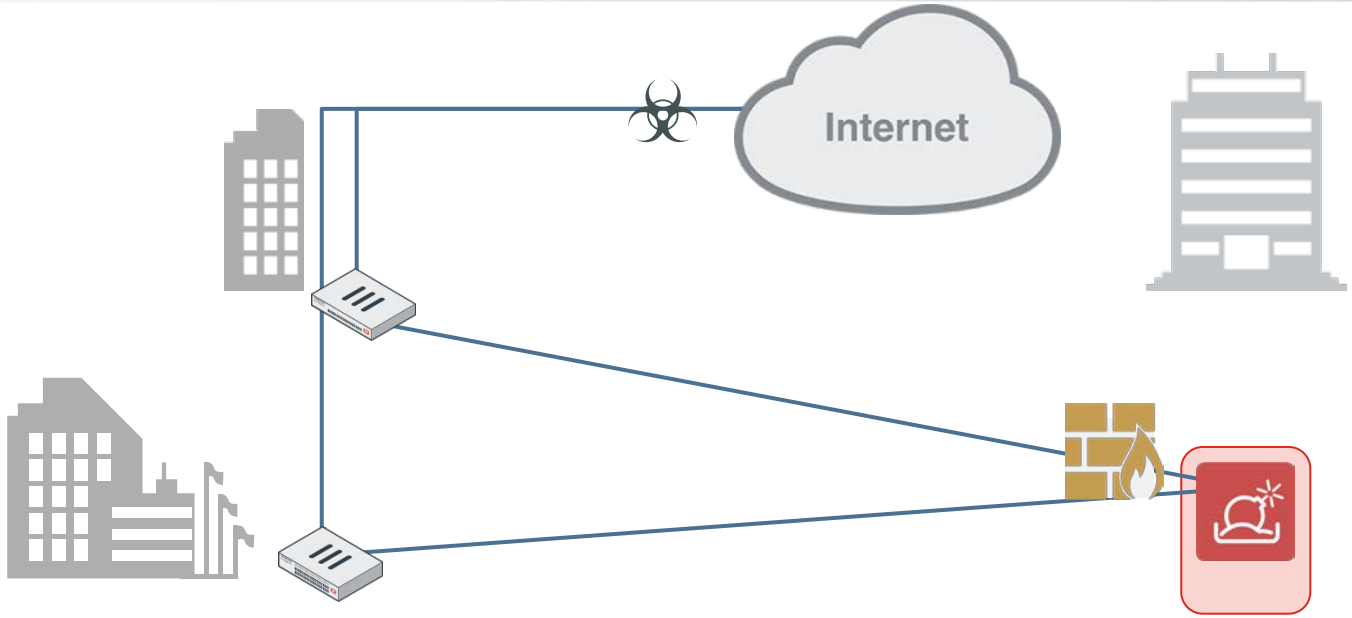


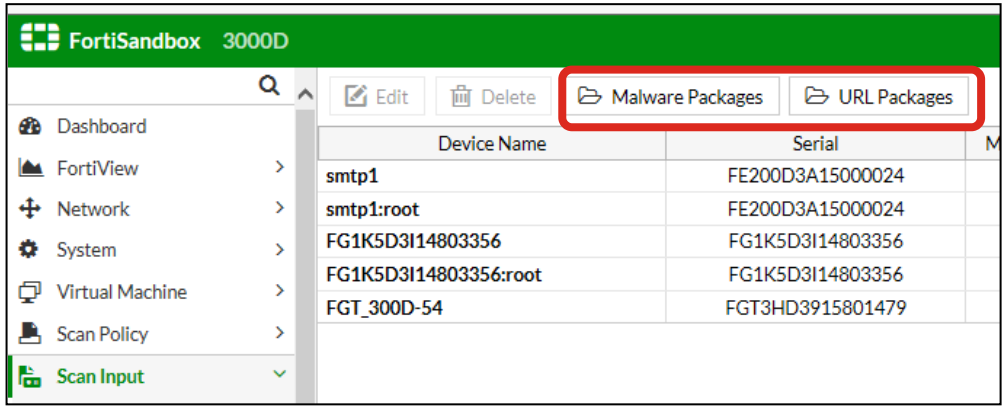


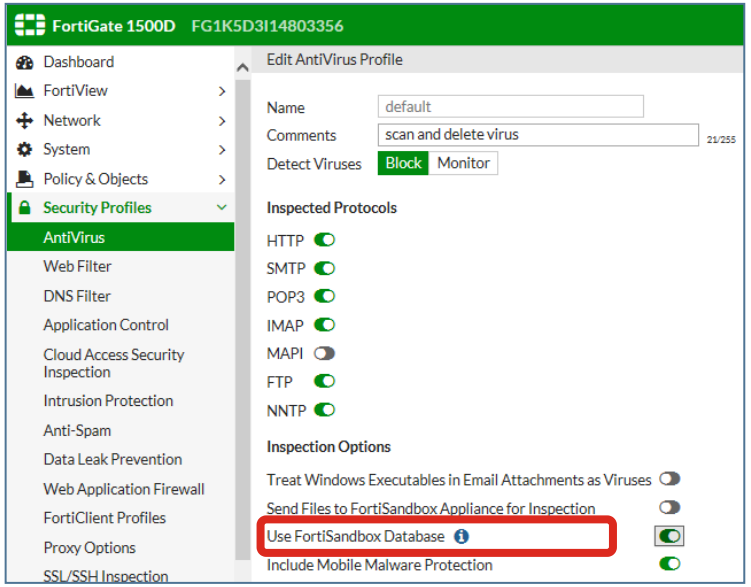


- FortiGate blocks as much as it can, routes remaining objects to FortiSandbox
- FortiSandbox returns ratings and updates
- FortiGate admin quarantines device, FortiGate starts blocking new threats

#1 ATP Use Case: NGFW + Sandbox Share Objects and Info

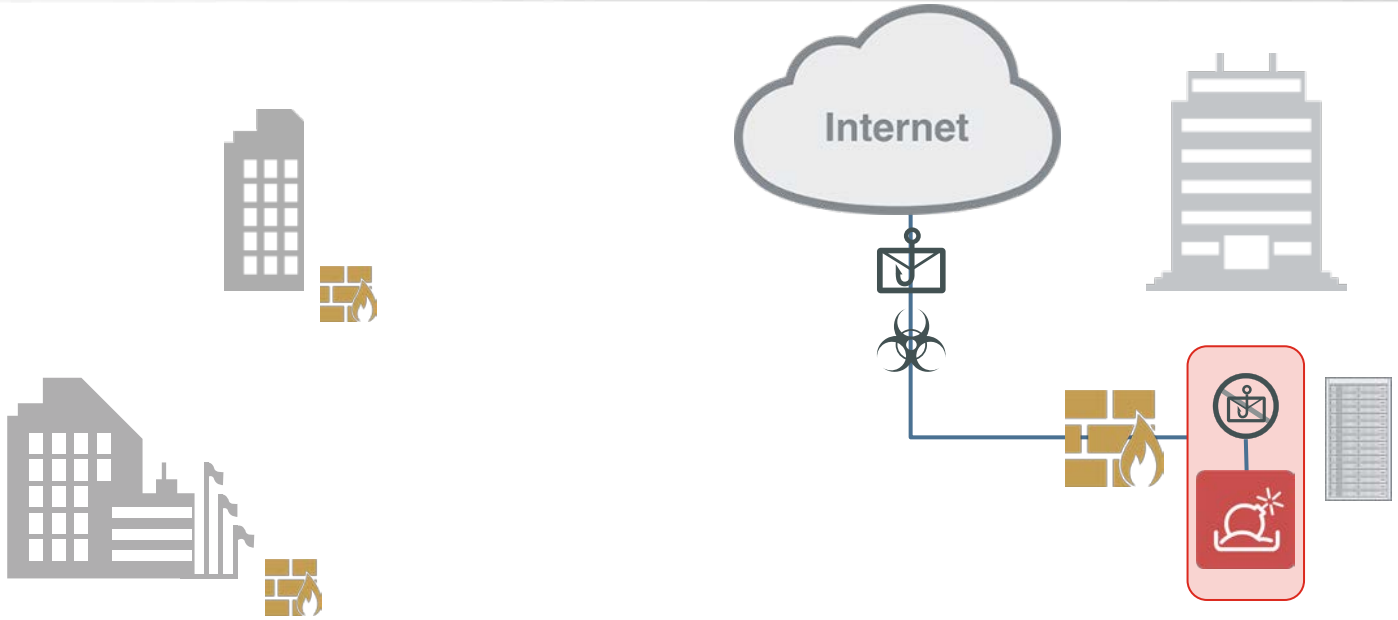


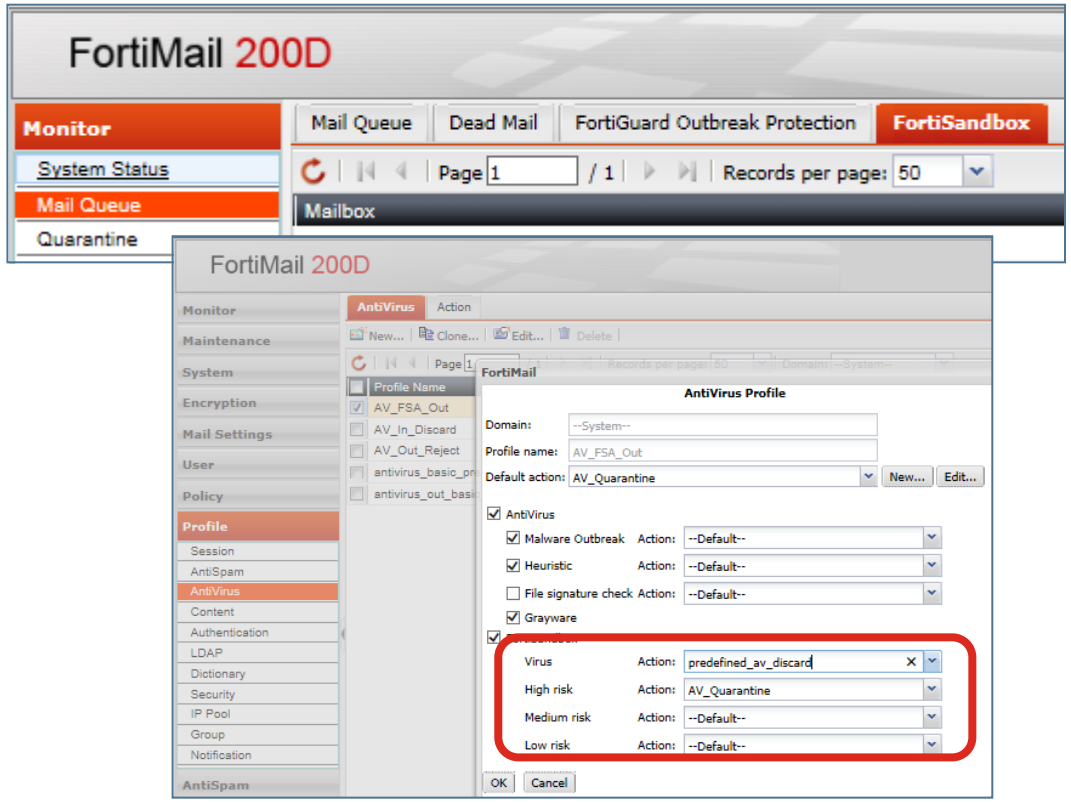




- FortiGate blocks as much as it can, routes remaining objects to FortiSandbox
- FortiSandbox returns ratings and updates
- FortiGate admin quarantines device, FortiGate starts blocking new threats

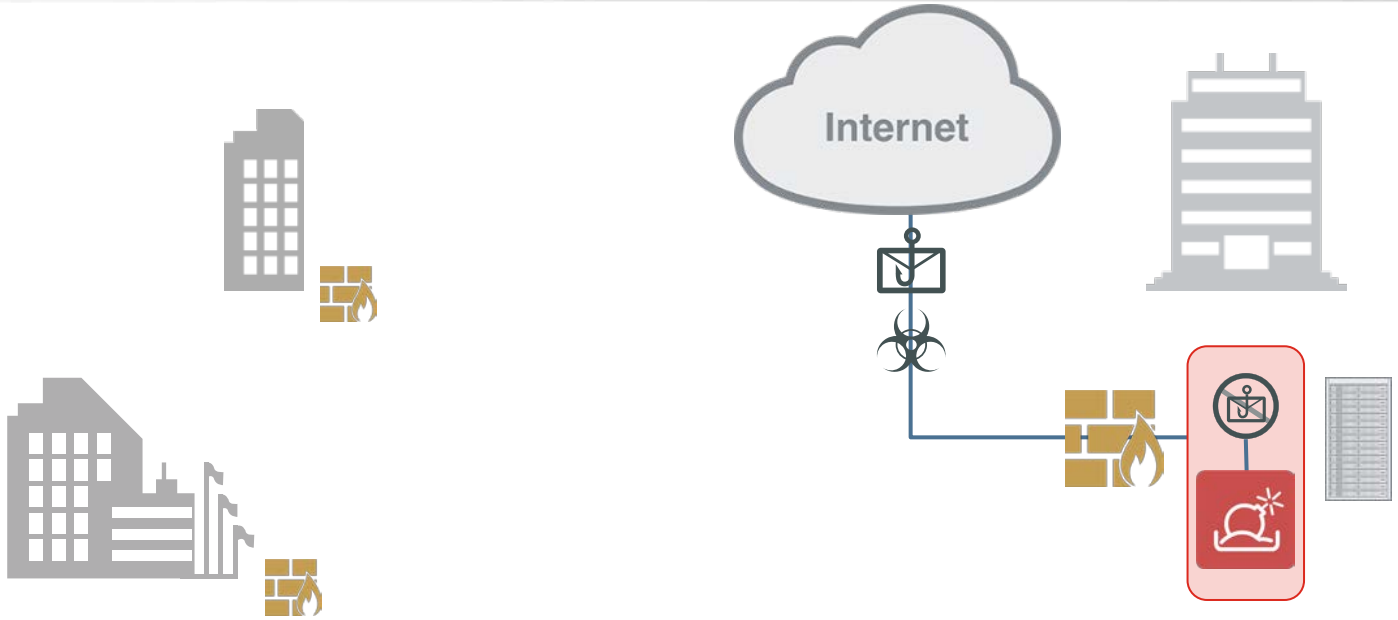
#2 ATP Use Case: SEG + Sandbox Hold and Analyze

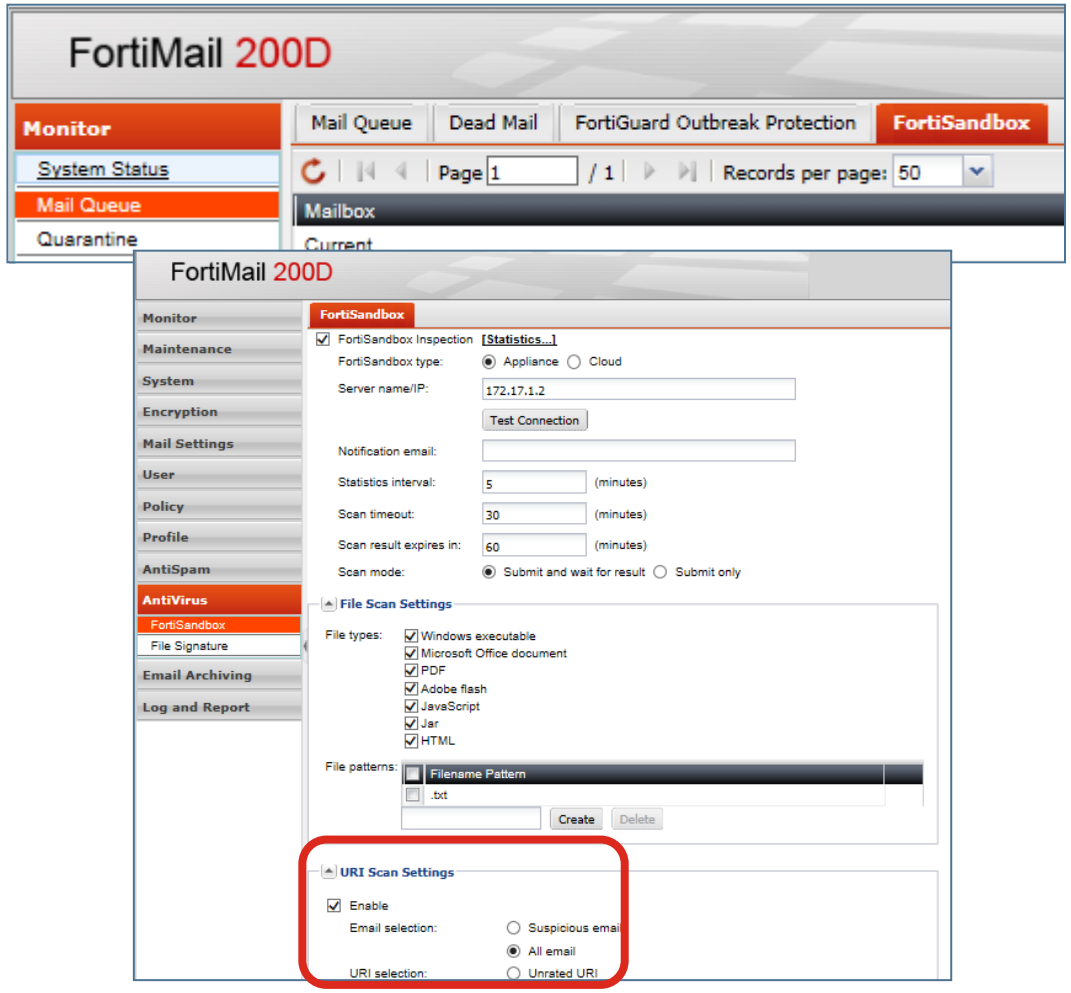




- FortiMail blocks as much as possible, queues messages for additional FortiSandbox analysis
- Quarantine or Deliver based on result
- Send URLs as well as attachments

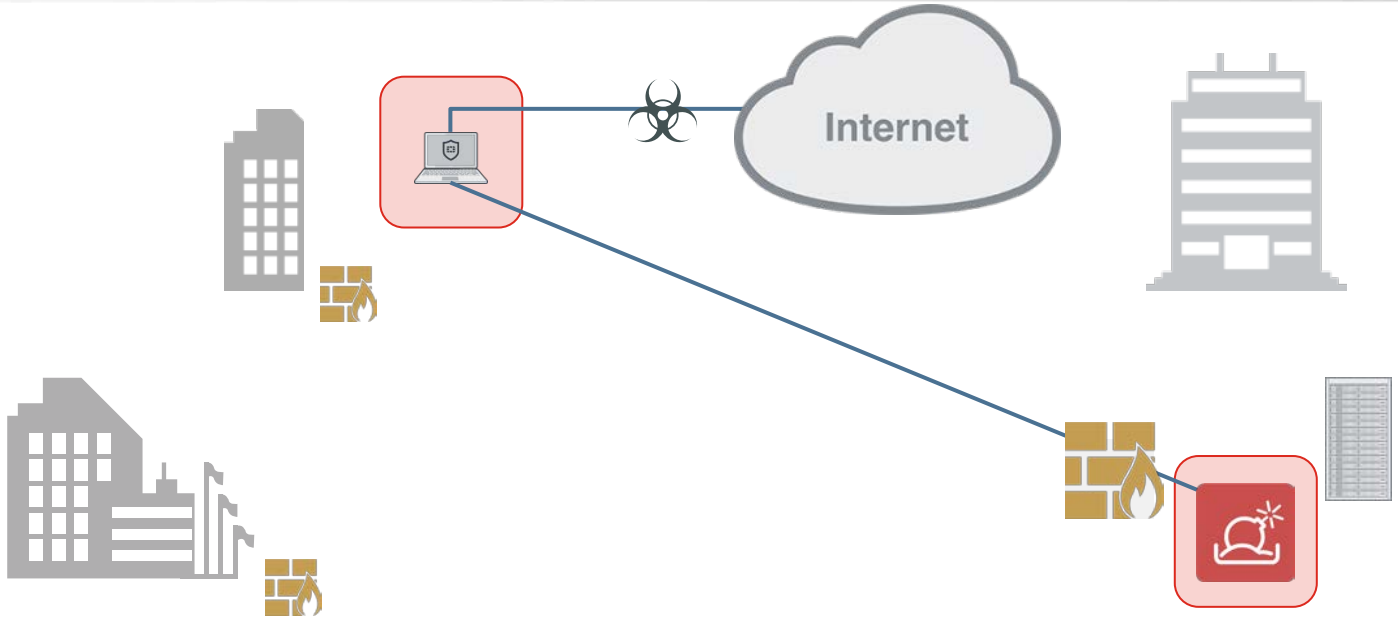
#2 ATP Use Case: SEG + Sandbox Hold and Analyze

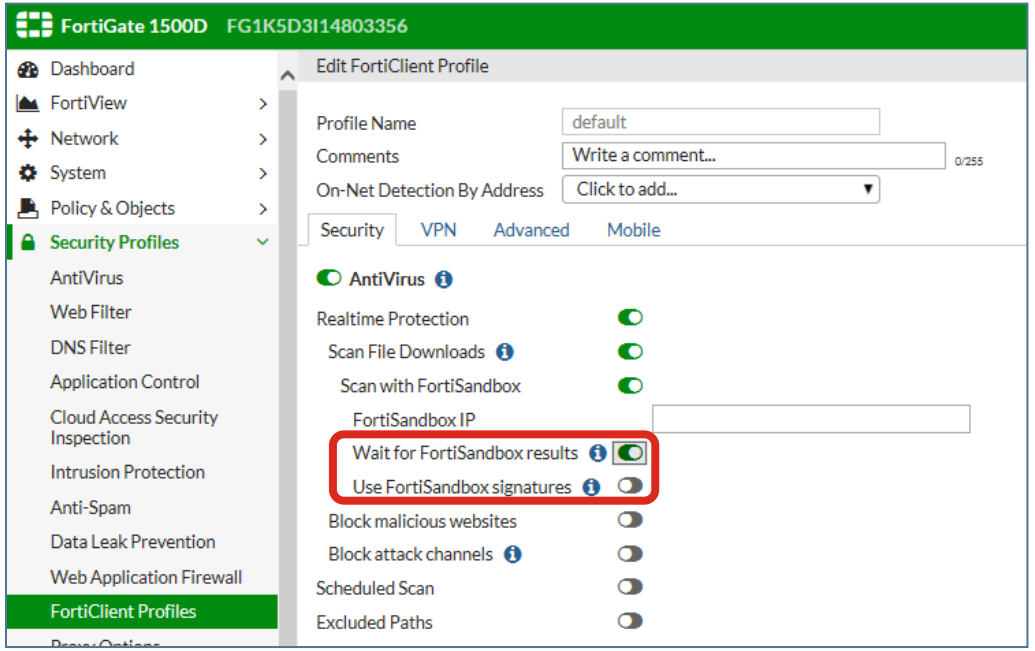




- FortiMail blocks as much as possible, queues messages for additional FortiSandbox analysis
- Quarantine or Deliver based on result
- Send URLs as well as attachments

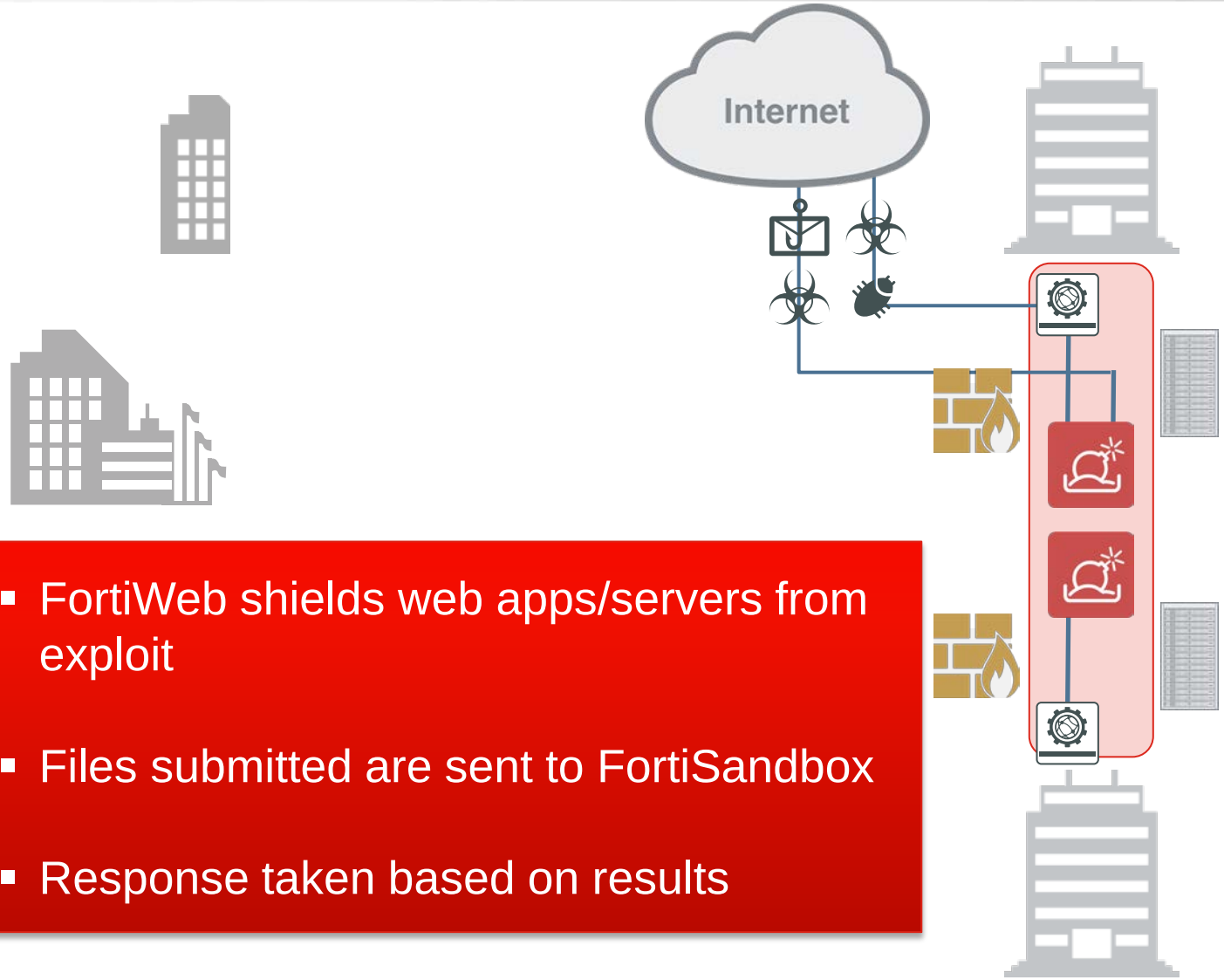
#3 ATP Use Case: Client + Sandbox Hold and Analyze





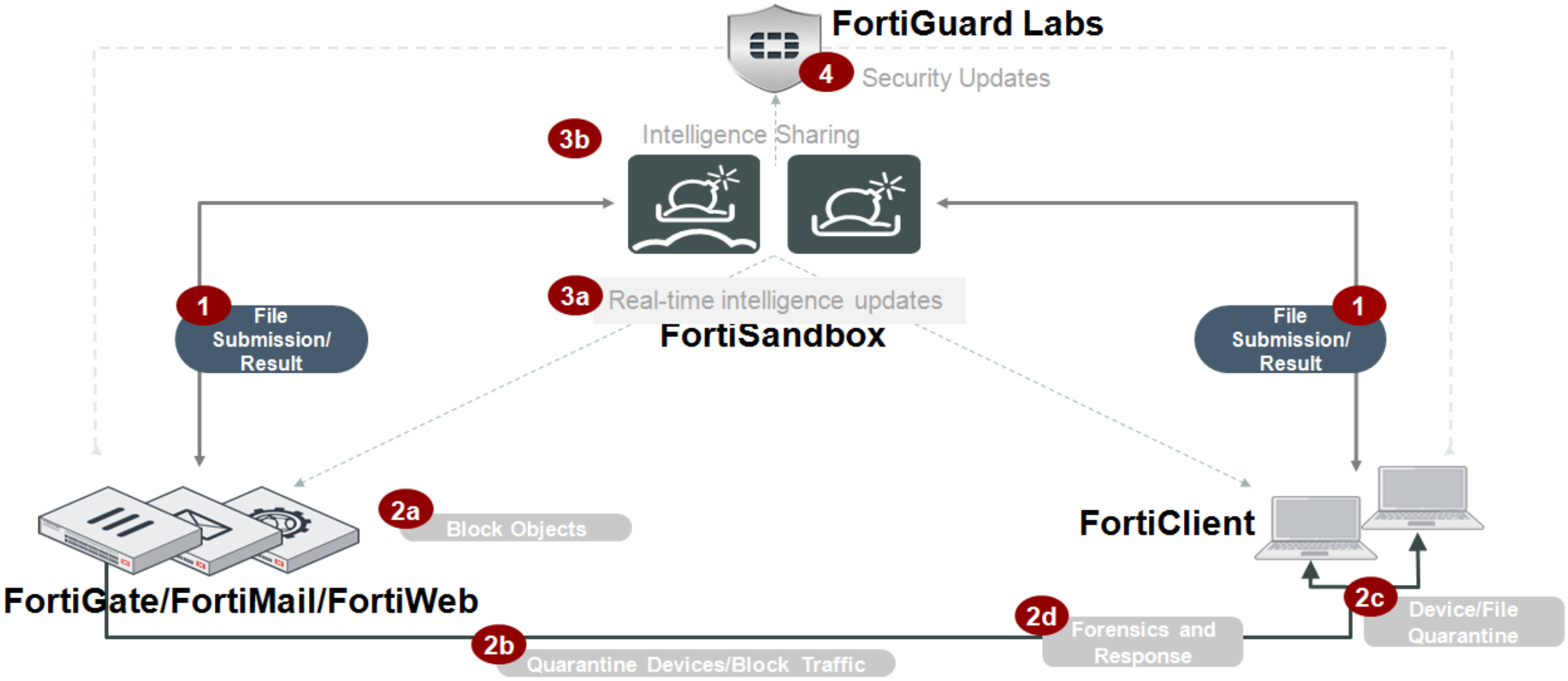
- FortiClient sends files to FortiSandbox
- Hold for Rating or Install and Quarantine
- Receive FortiSandbox Updates to Block

#4 ATP Use Case: WAF + Sandbox Harden and Analyze



- FortiWeb shields web apps/servers from exploit
- Files submitted are sent to FortiSandbox
- Response taken based on results

Technical Interaction



Fortinet Security Fabric

Fortinet Strategy – Security for a New World

COMPLEX

BORDERLESS

SLOW

SECURITY WITHOUT COMPROMISE

SEAMLESS

INTELLIGENT

POWERFUL

Fortinet Security Fabric

Seamless Security Across the Entire Attack Surface

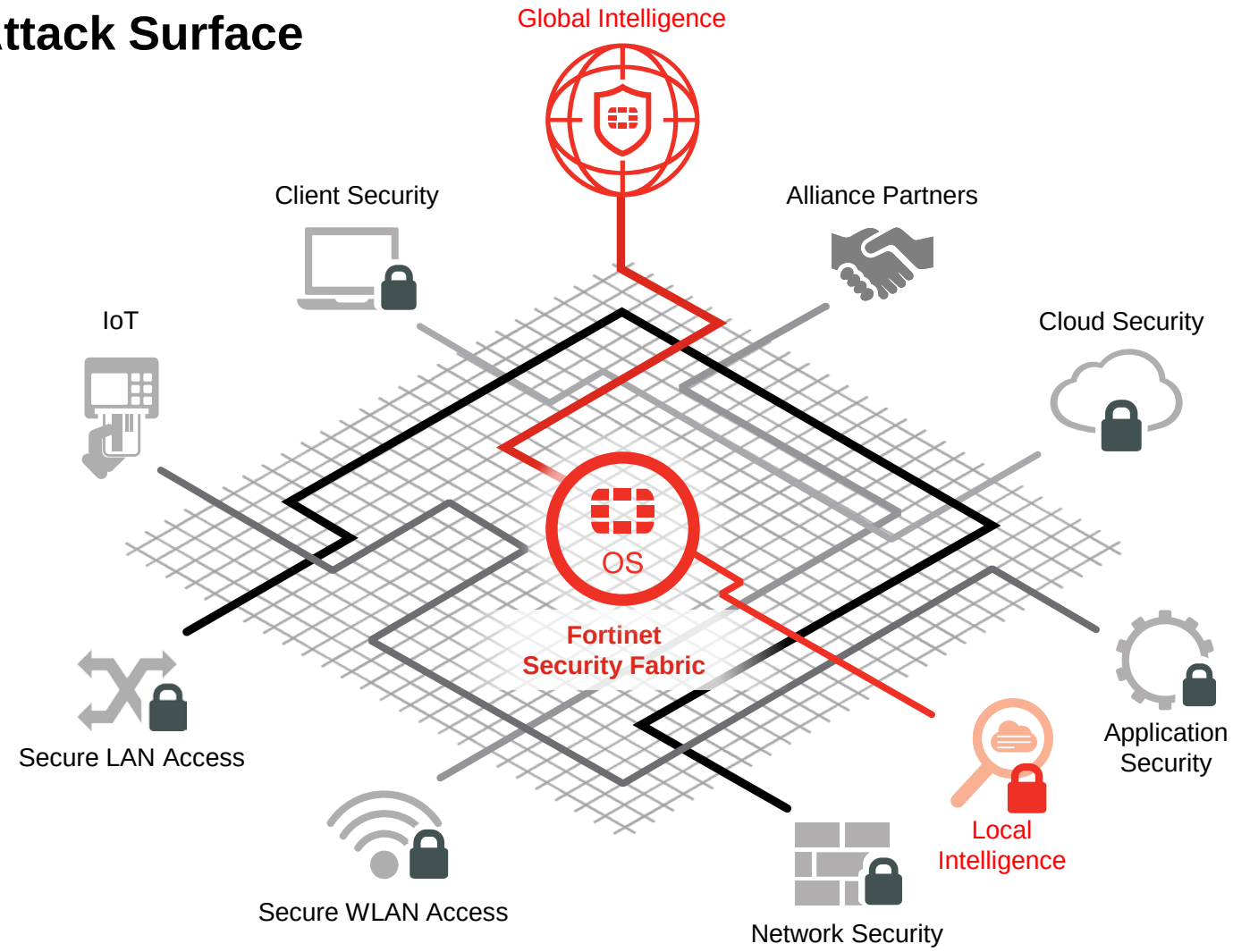
Scalable
IoT to the Cloud

Aware
Single Entity

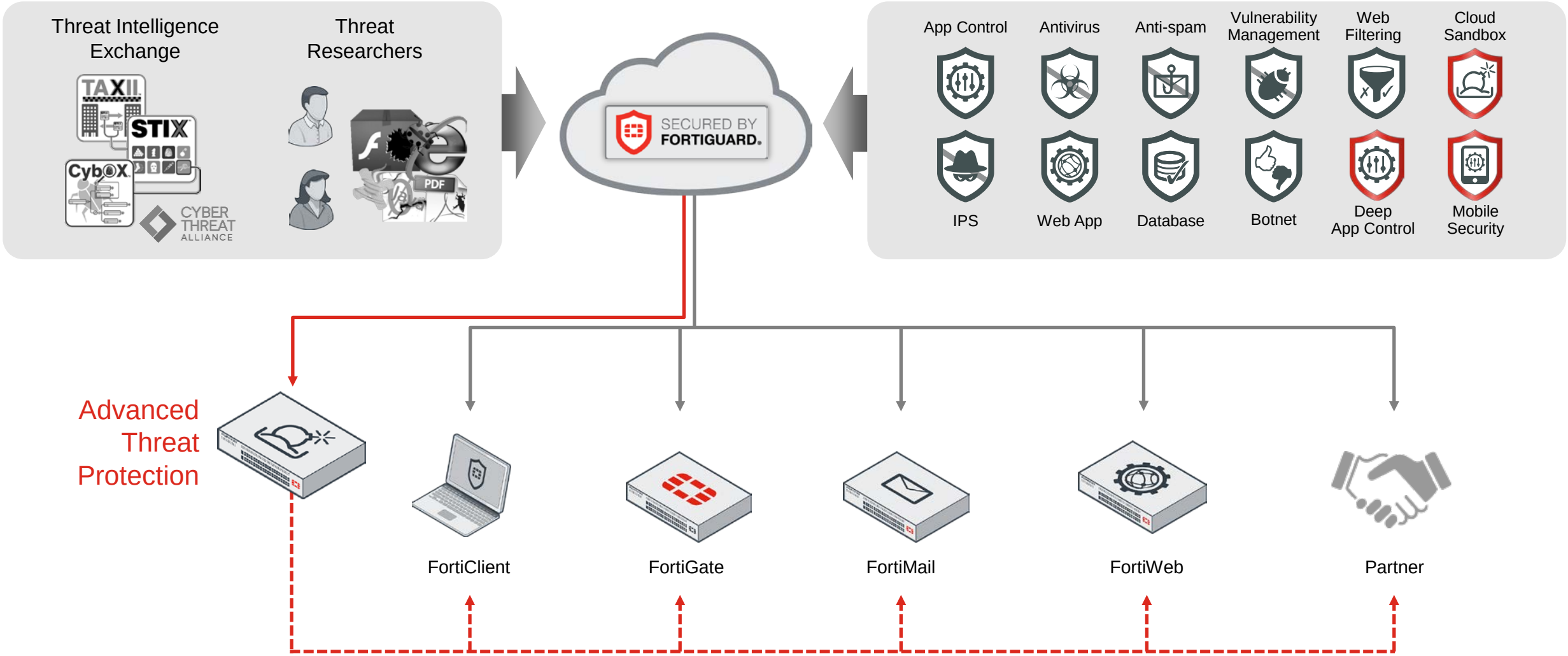
Secure
Global and Local intelligence

Actionable
Big Data Correlation

Open
Available to Partners

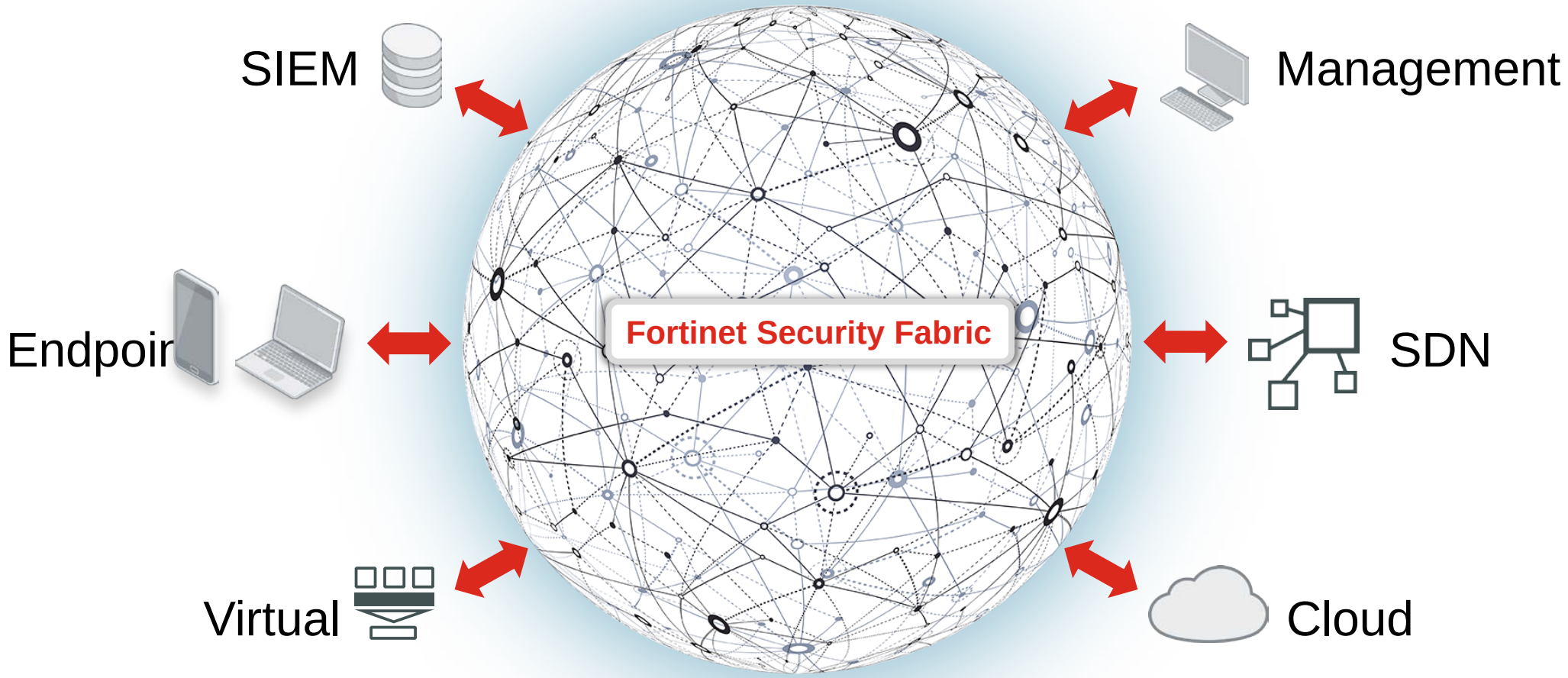


Fabric Attribute: Global and Local Security



Fabric Attribute : Open

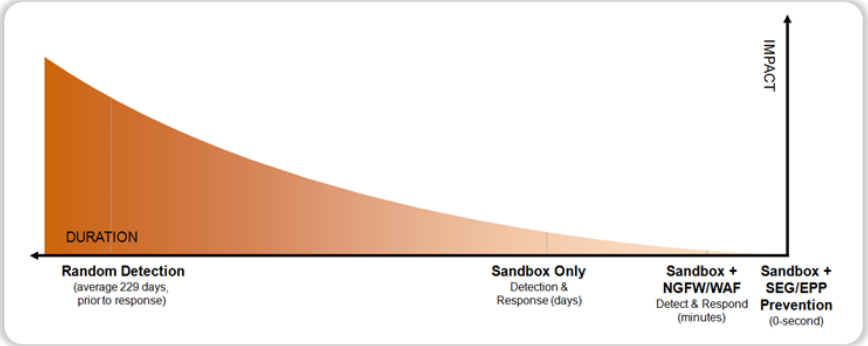
Ecosystem Alliance Partners



Recap

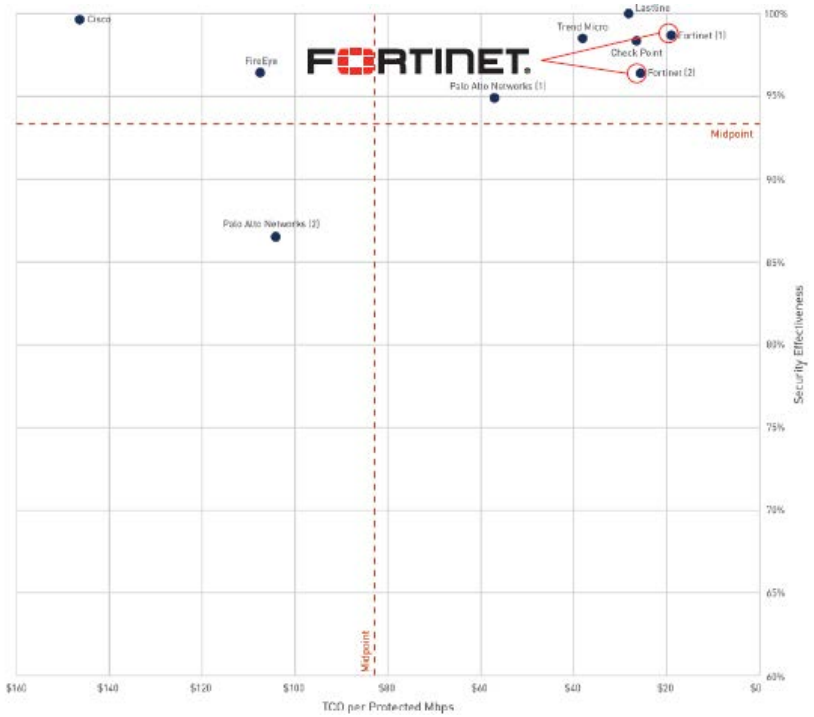
Key Points

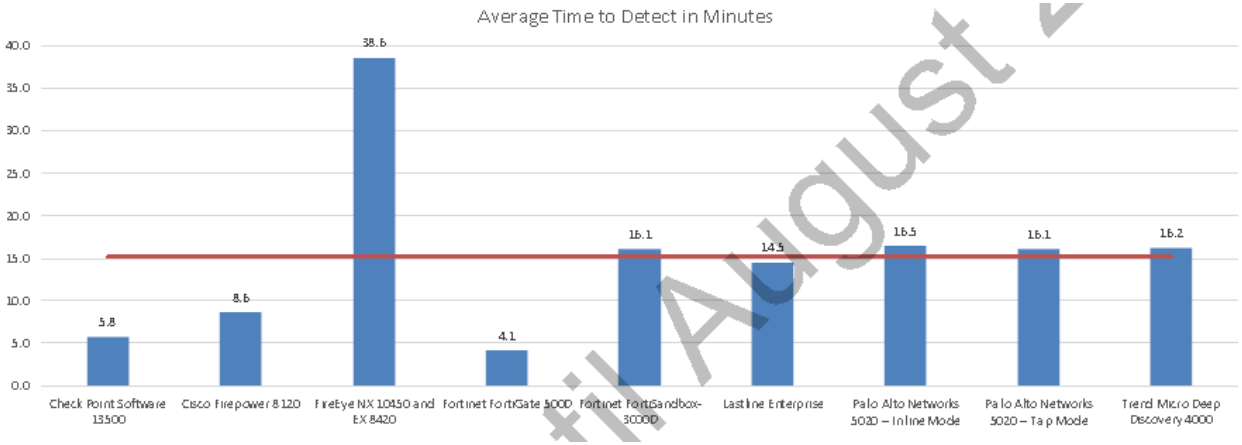
- Data breaches continue to make headlines, are the #1 priority for 2016
- Sandboxing addresses the source (custom malware) of the problem
- The integrated approach of Fortinet Advanced Threat Protection is unmatched
- It's also a key component of the broader Fortinet Security Fabric
- Pick the point(s) of integration that make sense over time



More on FortiSandbox NSS Tests

Independent Validation of FortiSandbox



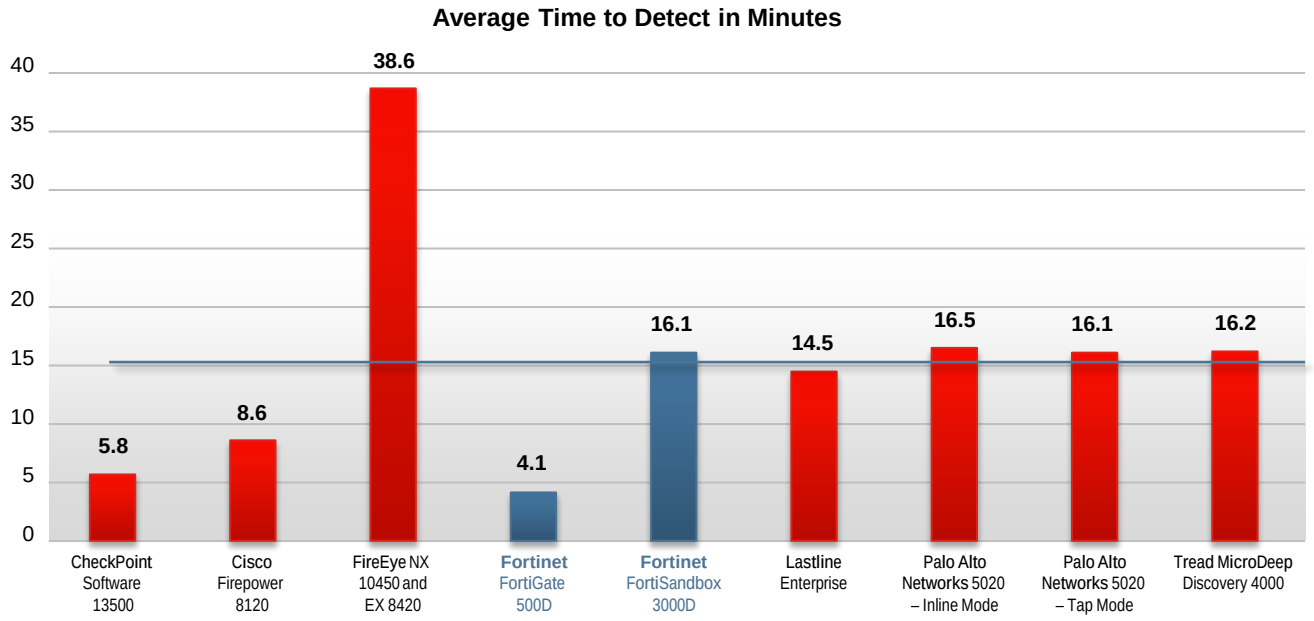


Product				Breach Detection Rate[1]	NSS-Tested Throughput	3-Year TCO (List Price)	3-Year TCO (Street Price)
Fortinet FortiGate 500D v5.4.1 with **FortiSandbox Cloud Service**				99.4%	1,000 Mbps	$22,300	$17,960
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Offline Infections	Evasions	Stability & Reliability
0.66%	100.0%	100.0%	99.6%	100.0%	76.9%	100.0%	PASS

Product				Breach Detection Rate[1]	NSS-Tested Throughput	3-Year TCO (List Price)	3-Year TCO (Street Price)
Fortinet FortiSandbox-3000D v2.1.3 with FortiClient v5.4.1.0840				99.0%	9,000 Mbps	$274,968	$220,093
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%	100.0%	100.0%	PASS

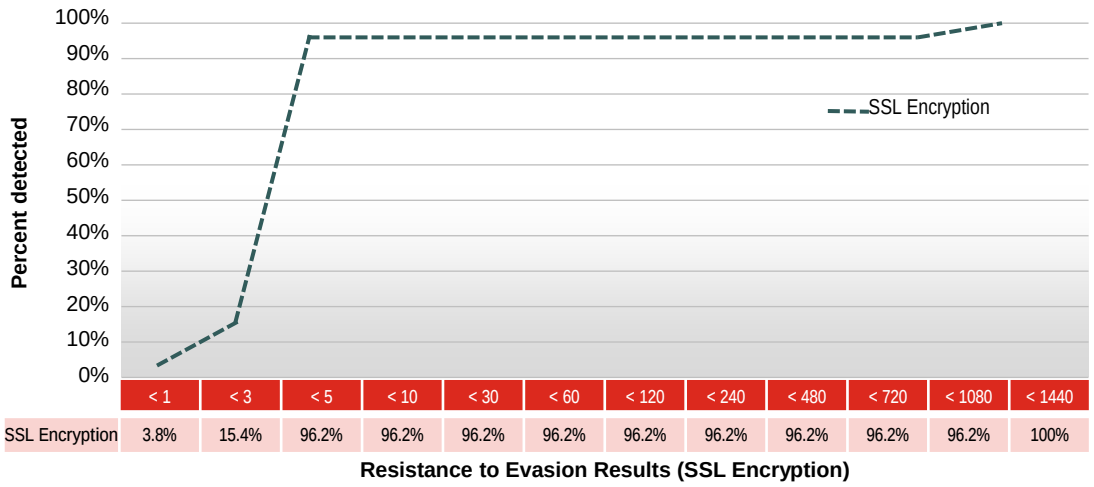
FortiSandbox Cloud with FortiGate 500D

- 99.4% Overall, 100% on Evasions
- Fastest Time to Detect (4.1 mins)
- <1% False Positives
- 1Gbps Throughput
- Best Value at $18/Mbps Protected



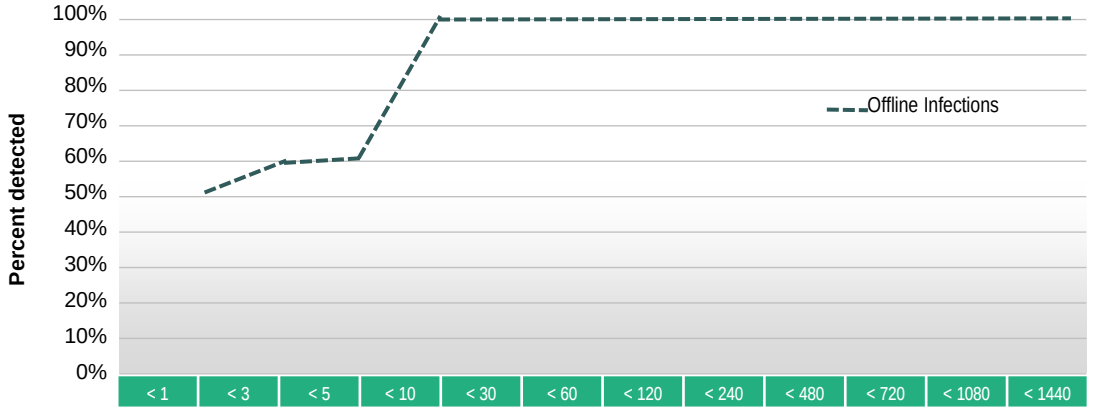
FortiSandbox Appliance with FortiClient

- 99% Overall,100% on Evasions, Offline Infections
- 10 Gbps Enterprise Throughput
- Next Best Value at $25/Mbps Protected



	< 1	< 3	< 5	< 10	< 30	< 60	< 120	< 240	< 480	< 720	< 1080	< 1440
SSL Encryption	3.8%	15.4%	96.2%	96.2%	96.2%	96.2%	96.2%	96.2%	96.2%	96.2%	96.2%	100%

Resistance to Evasion Results (SSL Encryption)



	< 1	< 3	< 5	< 10	< 30	< 60	< 120	< 240	< 480	< 720	< 1080	< 1440
Offline Infections	53.8%	61.5%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Offline Infections

Haben Sie momentan Sicherheitsprobleme ?

....woher wissen Sie das ??

Nutzen Sie unser kostenloses ***CTAP Programm (Cyber Threat Assessment Program)*** *um Klarheit über Ihre Netzwerksicherheit und Performance zu gewinnen!!!*

DON’T GO UNPROTECTED

FORTINET®