

Next generation security by Fortinet

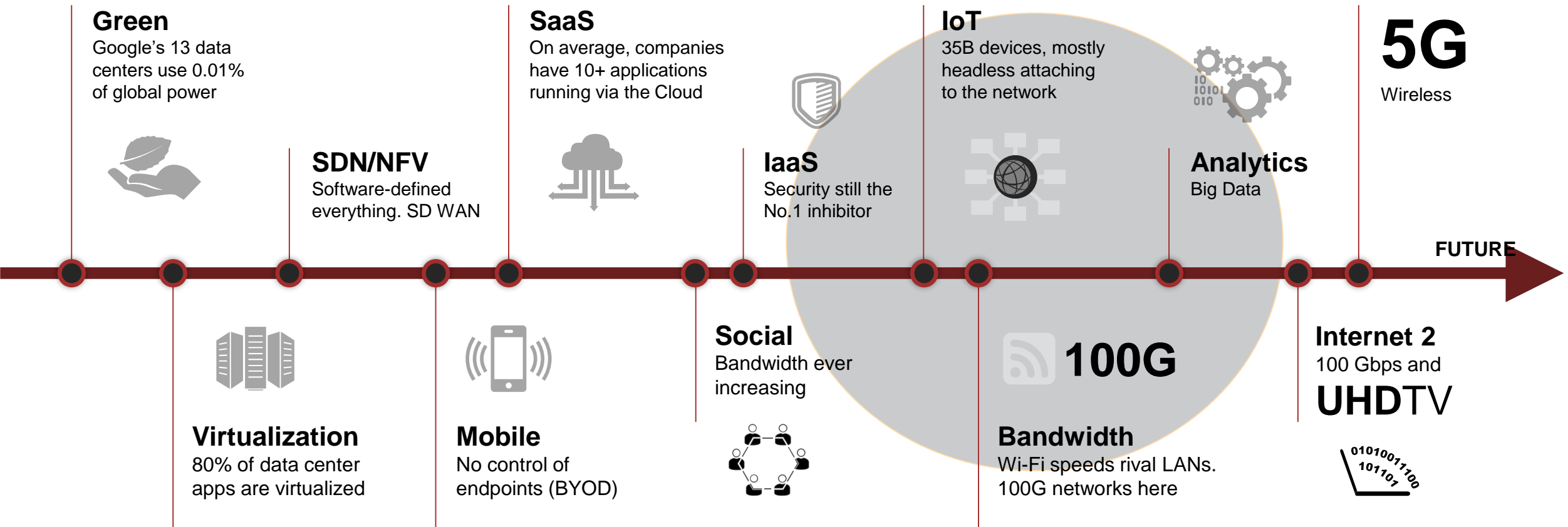
Ivan Ščavničar – Presales systems engineer

iscavnicar@fortinet.com



DO WE NEED A CHANGE IN SECURITY?

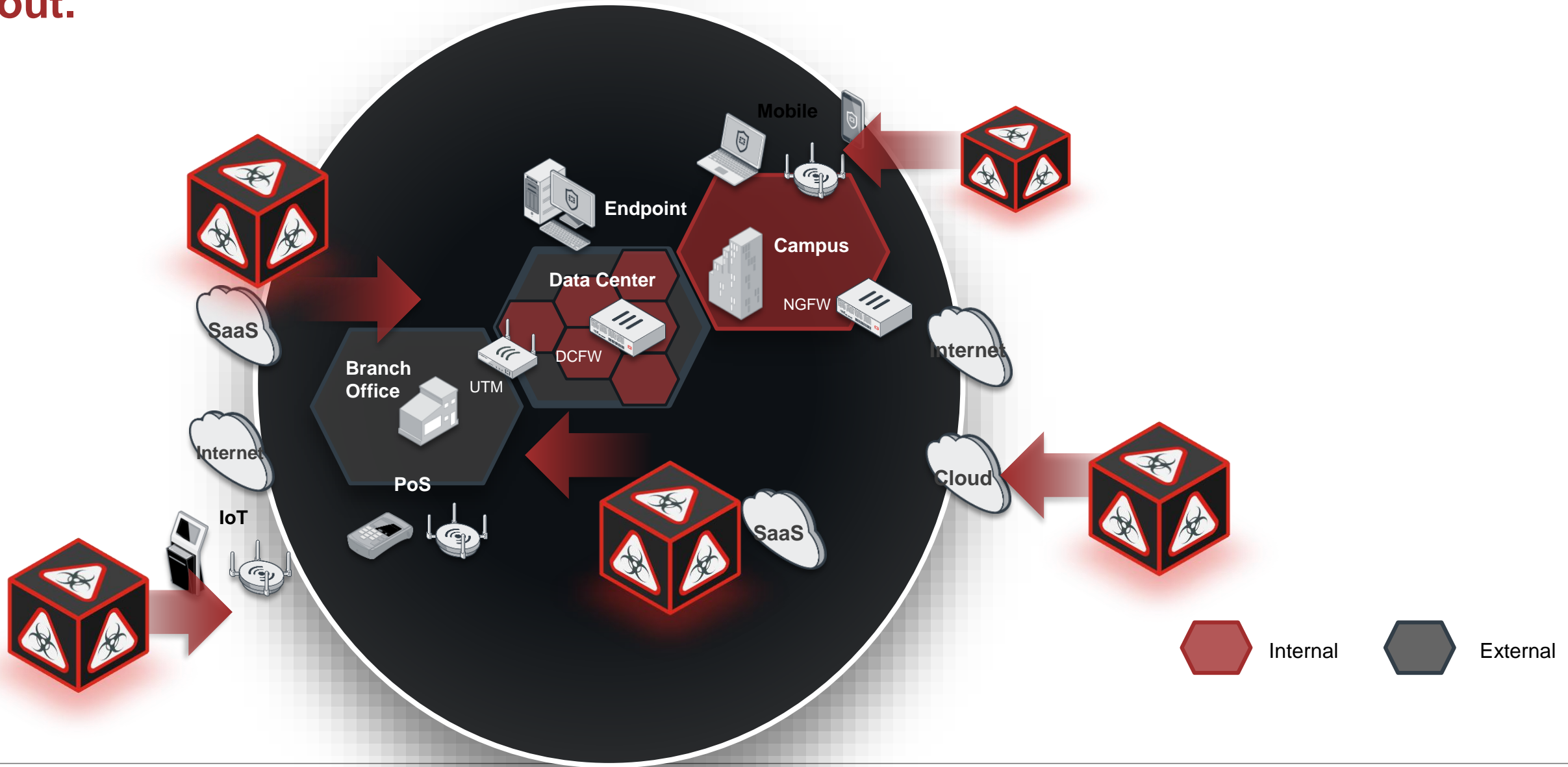
Infrastructure constantly changing



Malware is constantly changing

- Hard to catch by classical security engines
 - » HIPS usually bypassed by 0-day exploit kits
 - » URL filtering bypassed by using legit websites or random domain names
 - » Top 5 AV engines reach ~96% detection rate, repacked malware passes through
- Both massively deployed (ransomware) or targeted, specially developed for governments, SCADA & financial

The attack surface has increased **dramatically, everywhere, inside and out.**

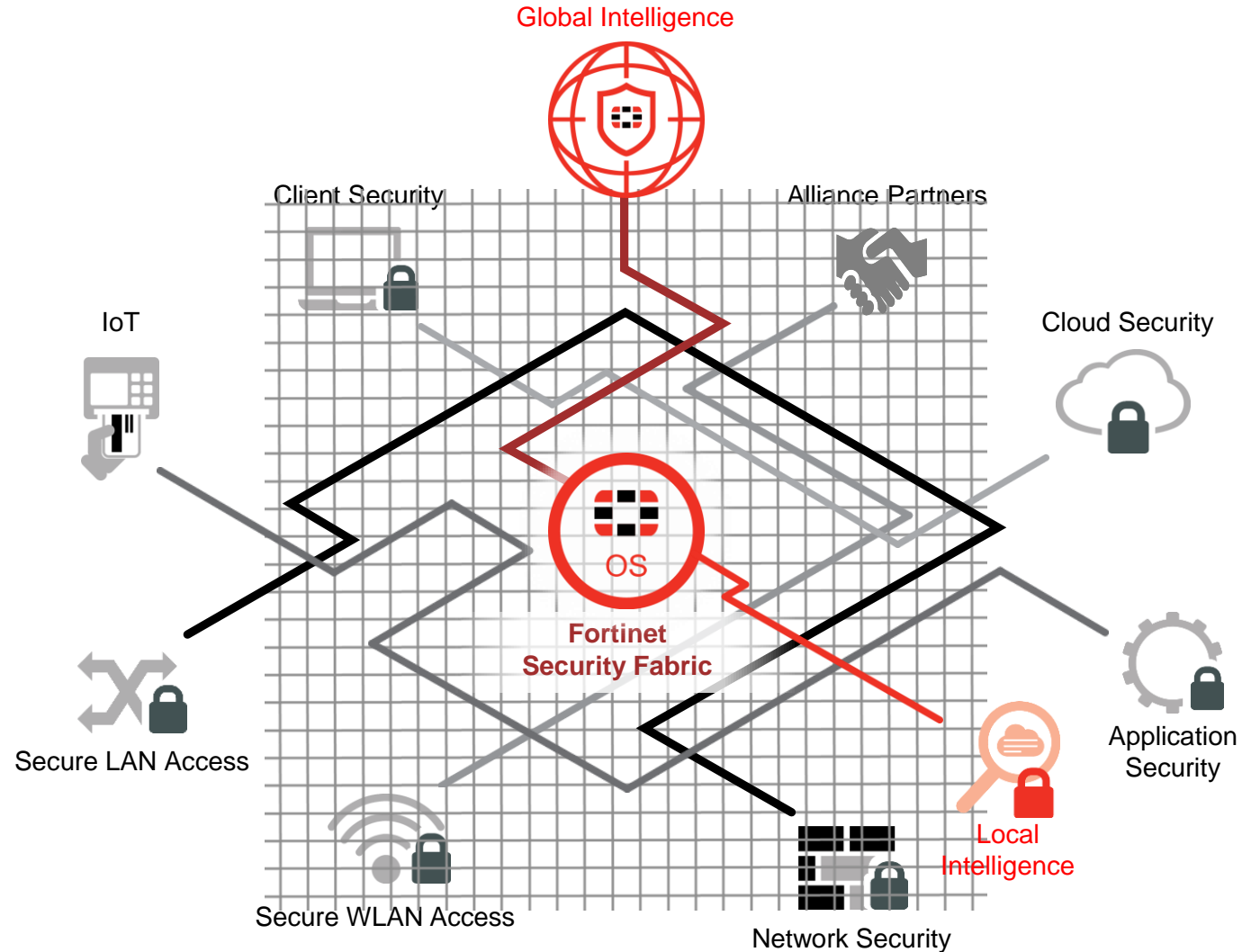




WHAT IS THE SECURITY FABRIC?

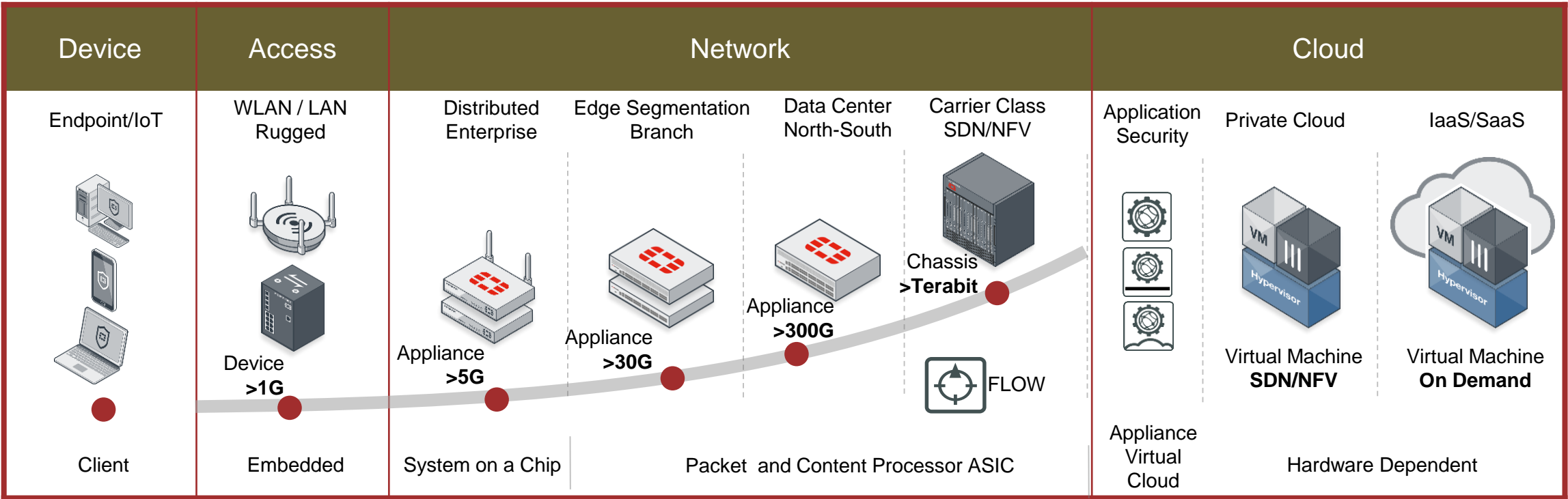
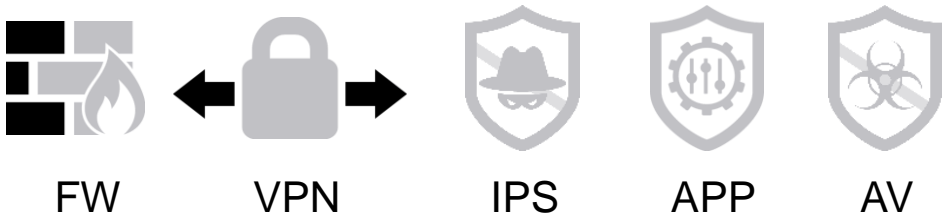
Fortinet Security Fabric – Integrated Security Architecture

Scalable
Aware
Secure
Actionable
Open

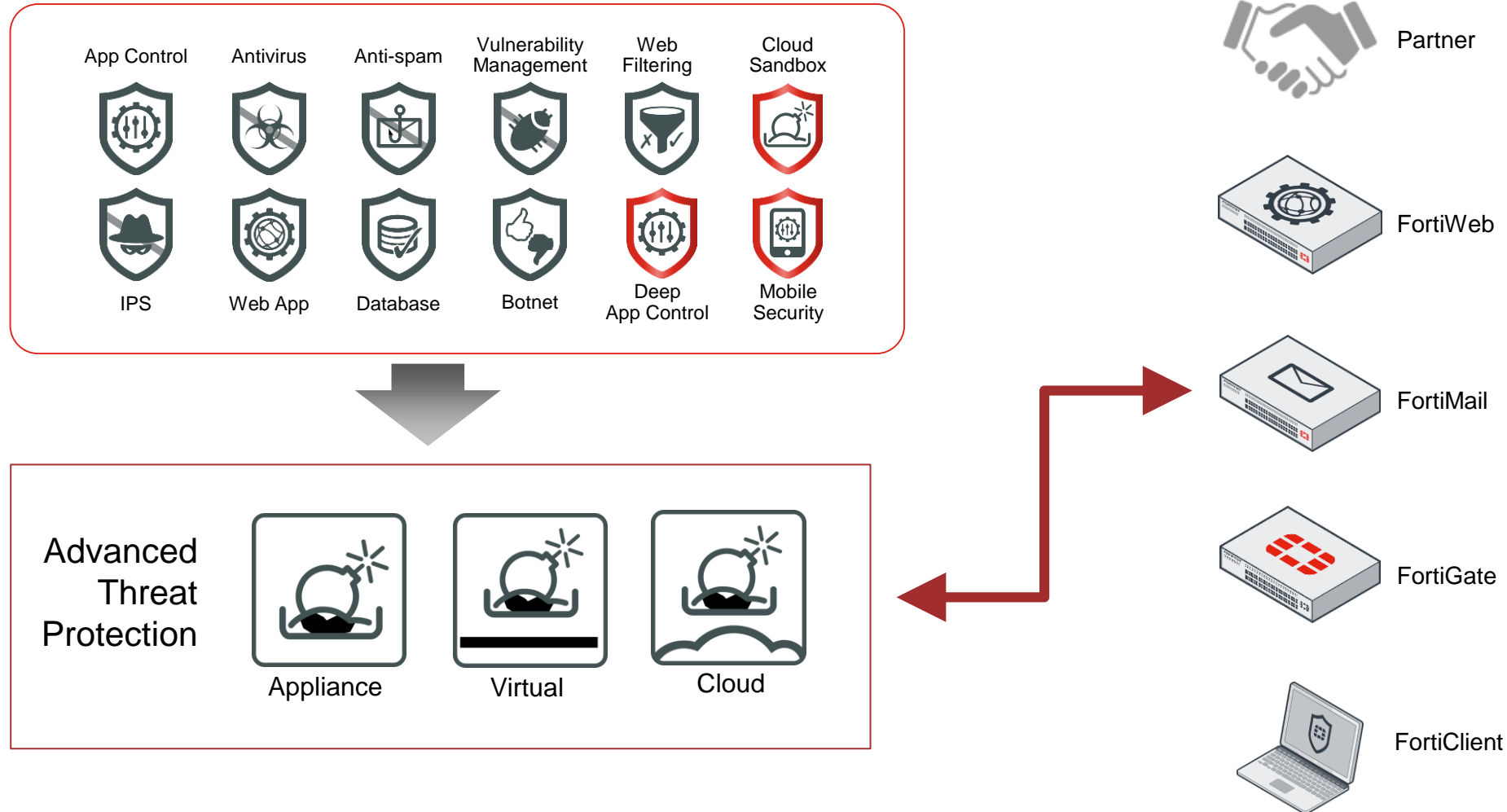


Secure – The Fabric cover all the possible attack vectors such as Network, Endpoint Access, Web, Email and Cloud

Security Updates



Actionable – The Fabric cuts Time to Protect from hours to seconds



Open – The Fabric allows integration of existing security solutions



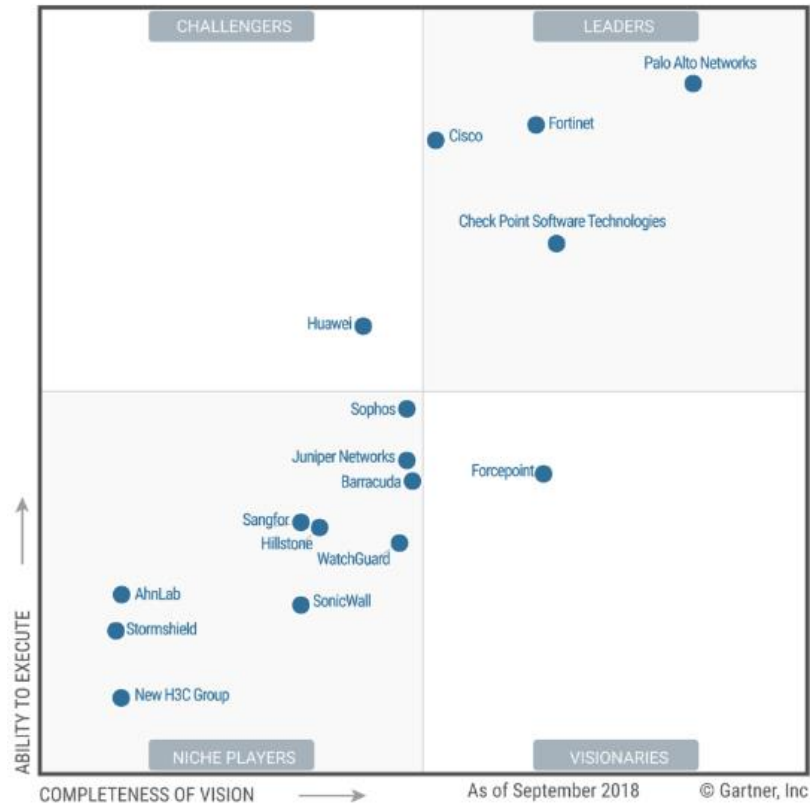
..and we mean open

- Cyber Threat Alliance:

- » Fortinet + Palo Alto Networks founded CTA – may 2014
- » Defined as Cyber Defense Consortium; goal is to have Automated Threat Intelligence Sharing Platform
- » Now it extended to
 - Intel Security Group, Intel Corporation;
 - Check Point;
 - Cisco Security;
 - Symantec;
 - McAfee
 - Telefonica
 - Zscaler
 - Barracuda

A Leader in Network Security

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (October 2018)

Figure 1. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

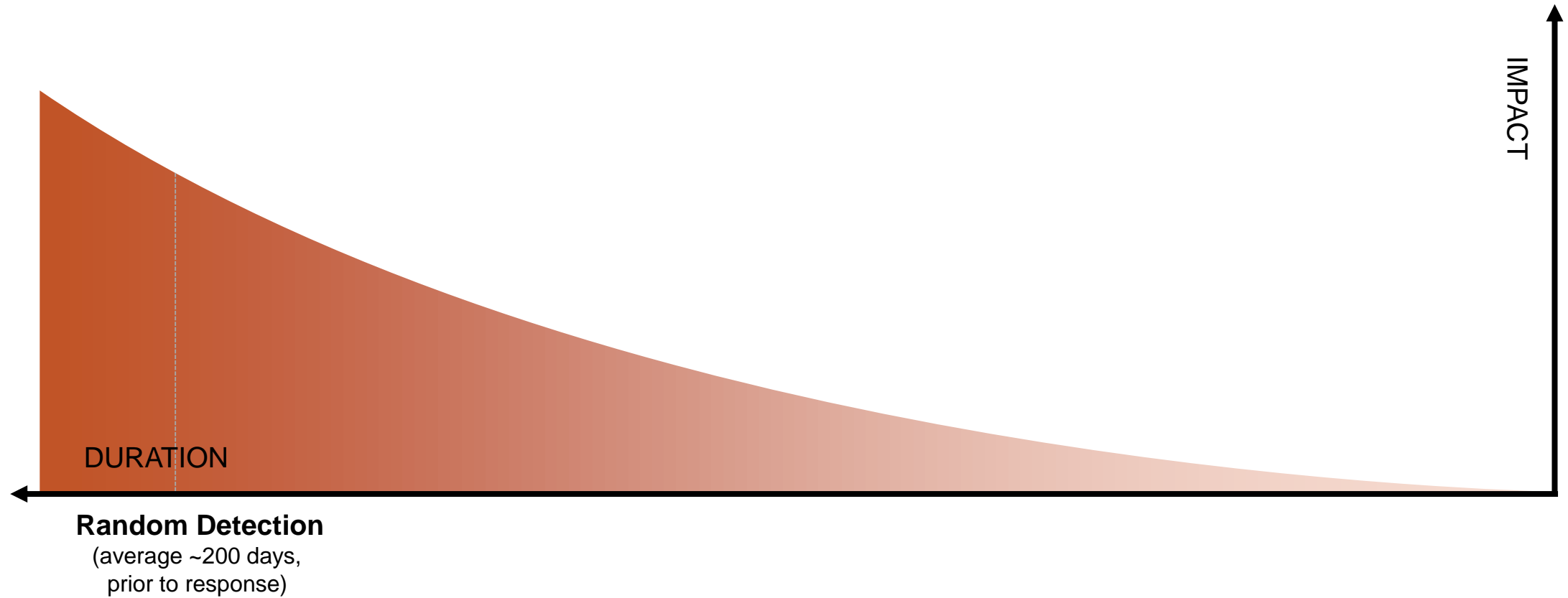


Source: Gartner (June 2017)

The background of the slide is a deep red color. It features a faint, white network diagram consisting of numerous interconnected dots and lines, resembling a molecular or data structure, spread across the upper half. In the lower right, there is a blurred image of a microscope. A cylindrical component of the microscope, likely the objective lens, is prominent and has the text "40X" printed on it in white. The overall aesthetic is scientific and technological.

ADVANCED THREAT PROTECTION

Time Malware Remains Undetected



How Does it Remain Undetected? Unique Code.

70-90%

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 signed files				Heuristics Reputation: File, IP, App, Email Generic Signatures	Blacklists Signatures

Sources:
Verizon 2016 Data Breach Investigations Report, April 2016

How Should We Address it? Sandboxing.

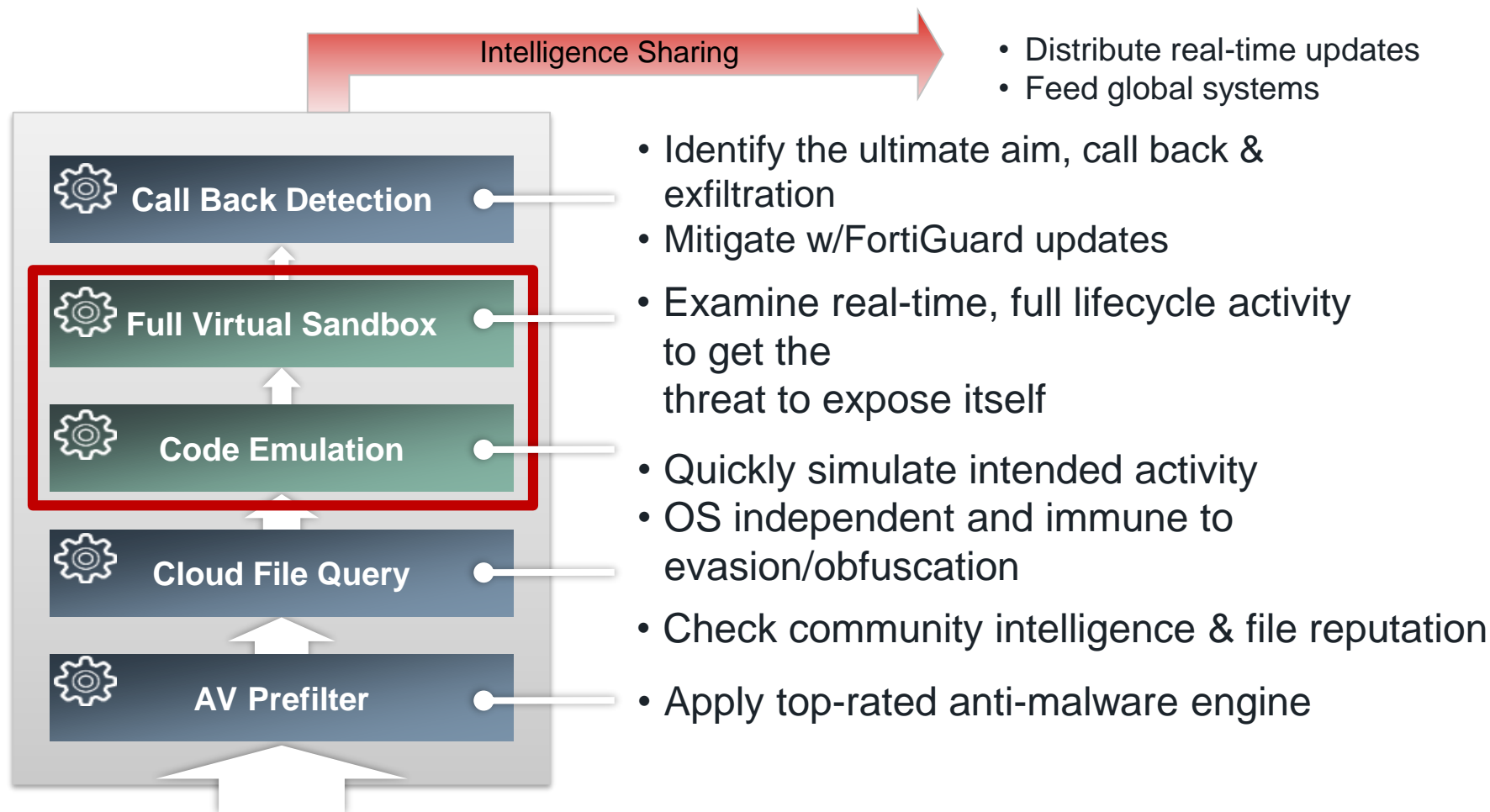
70-90%

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 signed files	Sandboxing 			Heuristics Reputation: File, IP, App, Email Generic Signatures	Blacklists Signatures

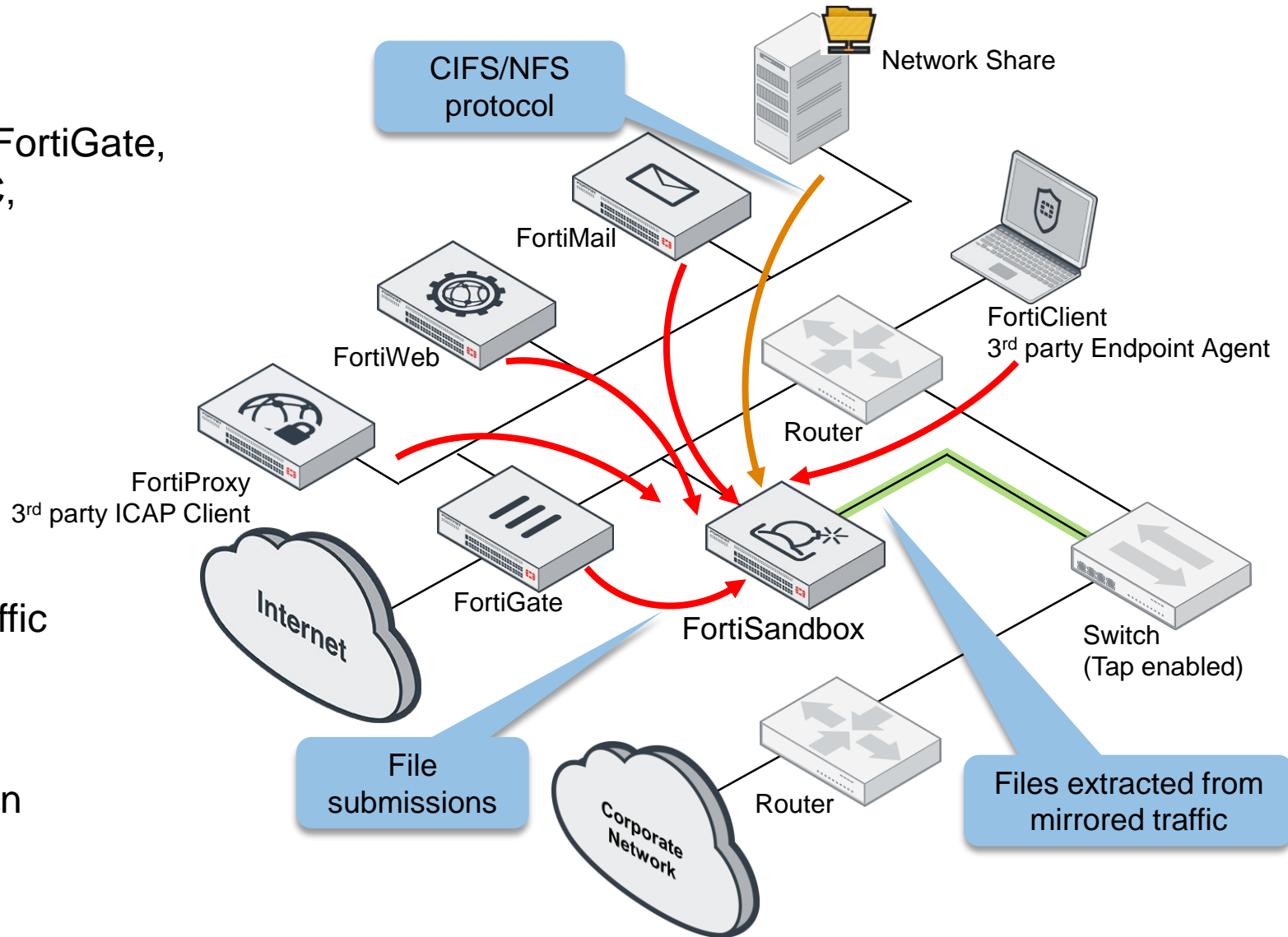
Sources:
Verizon 2016 Data Breach Investigations Report, April 2016

Key FortiSandbox Components



Modes of Operation

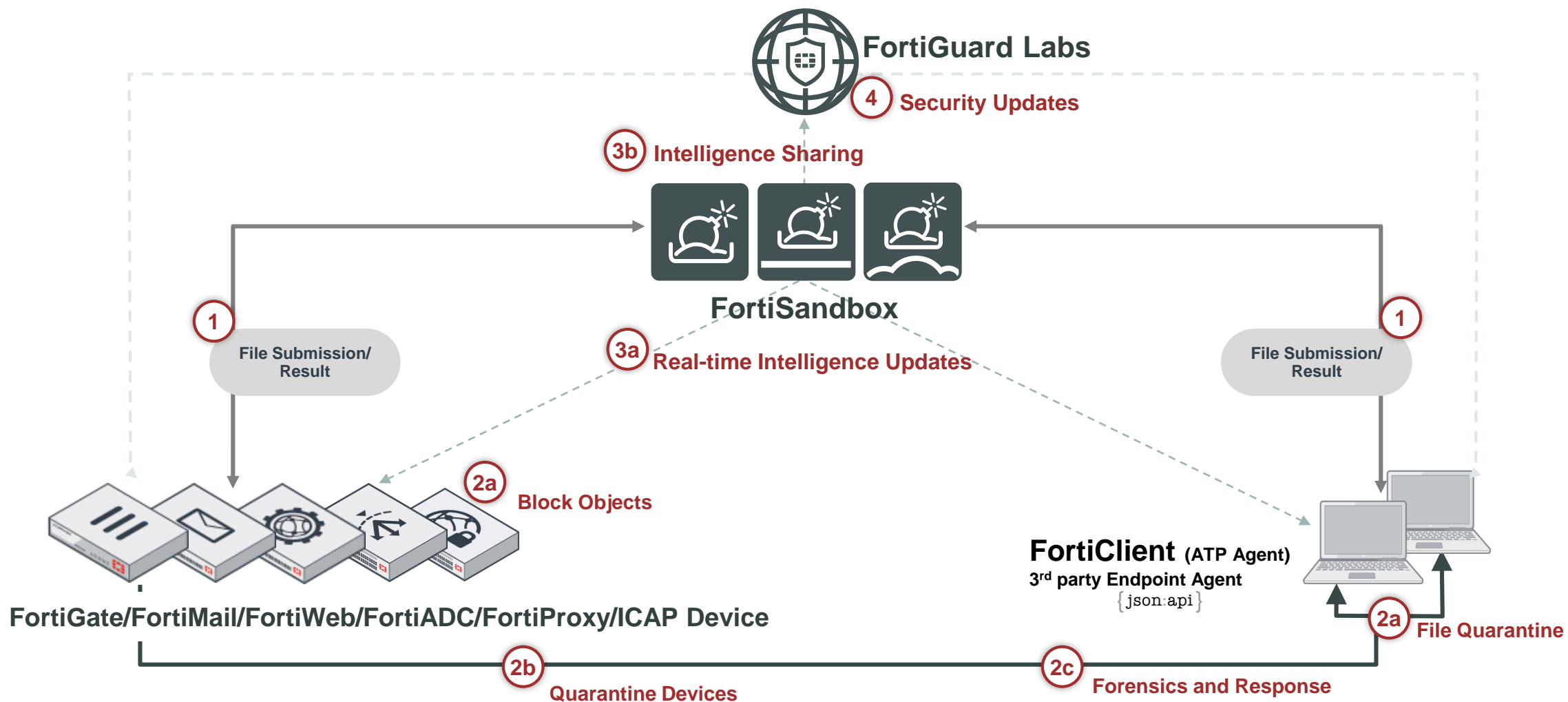
- Fabric Integration
 - » Files submitted directly from FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, and FortiClient
- 3rd Party Adapters
 - » Carbon Black/Bit9
 - » ICAP for SWG
 - » JSON API
- Sniffer
 - » Extract files from mirrored traffic to perform inspection
- On-demand
 - » Manual file or URL submission using management GUI
- Network share



That is Fully Automated

Automated Intelligence Sharing and Response

Animated



FortiGate / FortiSandbox in Security Fabric

FortiGate 1500D Demo-NGFW-PRI

demo

Favorites

Dashboard

FortiView

Network

System

Administrators

Admin Profiles

Settings

HA

SNMP

Replacement Messages

FortiGuard

Cooperative Security Fabric

Advanced

Feature Select

Certificates

Policy & Objects

Security Profiles

Cooperative Security Fabric

SMTP Service - FortiMail

Authentication

Sandbox inspection

FortiSandbox type

FortiSandbox Appliance

FortiSandbox Cloud

Server

10.88.23.8

Test Connectivity

Notifier Email

Applied Threat Intelligence

Dynamic Malware Detection version

2.3816 (signatures: 103)

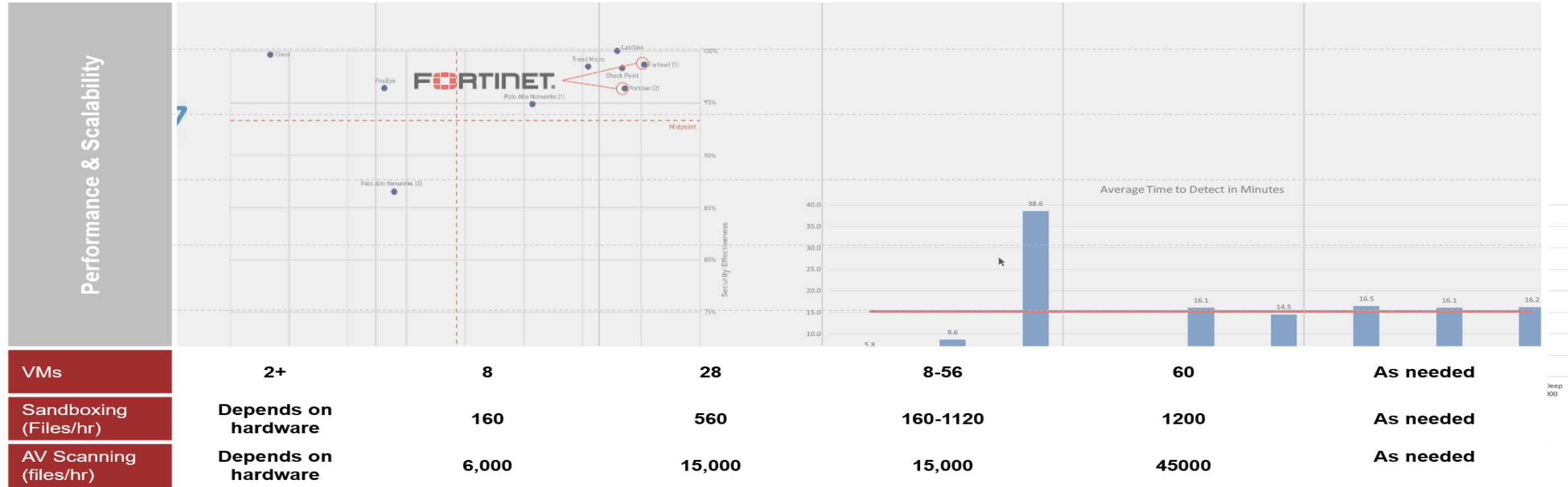
URL Threat Detection version

2.3722 (entries: 90)

FortiSandbox statistics (last 7 days)

File type	Detected
Total submitted	50
Critical (Malicious)	0
High Risk	0
Medium Risk	2
Low Risk	48
Clean	0

Independent Validation of FortiSandbox



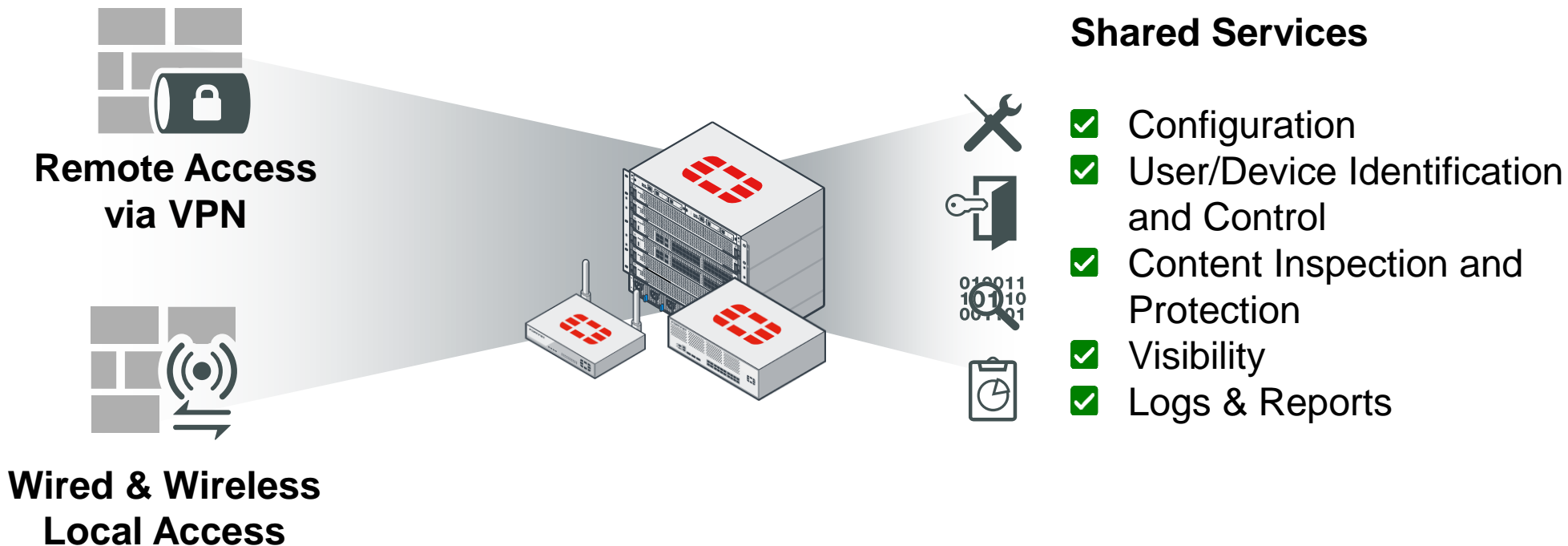
Product					Breach Detection Rate¹	NSS-Tested Throughput	3-Year TCO (List Price)	3-Year TCO (Street Price)
Fortinet FortiGate 500D v5.4.1 with FortiSandbox Cloud Service					99.4%	1,000 Mbps	\$22,300	\$17,960
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Offline Infections	Evasions	Stability & Reliability	
0.66%	100.0%	100.0%	99.6%	100.0%	76.9%	100.0%	PASS	

Product					Breach Detection Rate¹	NSS-Tested Throughput	3-Year TCO (List Price)	3-Year TCO (Street Price)
Fortinet FortiSandbox-3000D v2.1.3 with FortiClient v5.41.0840					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	

The background of the slide is a deep red color. It features a faint, white network diagram consisting of numerous nodes connected by thin lines, resembling a web or a molecular structure. In the lower right portion of the image, there is a blurred, high-contrast photograph of a microscope. A component of the microscope, likely an objective lens, is clearly visible and has the text "40X" printed on it in white. The overall aesthetic is technical and scientific.

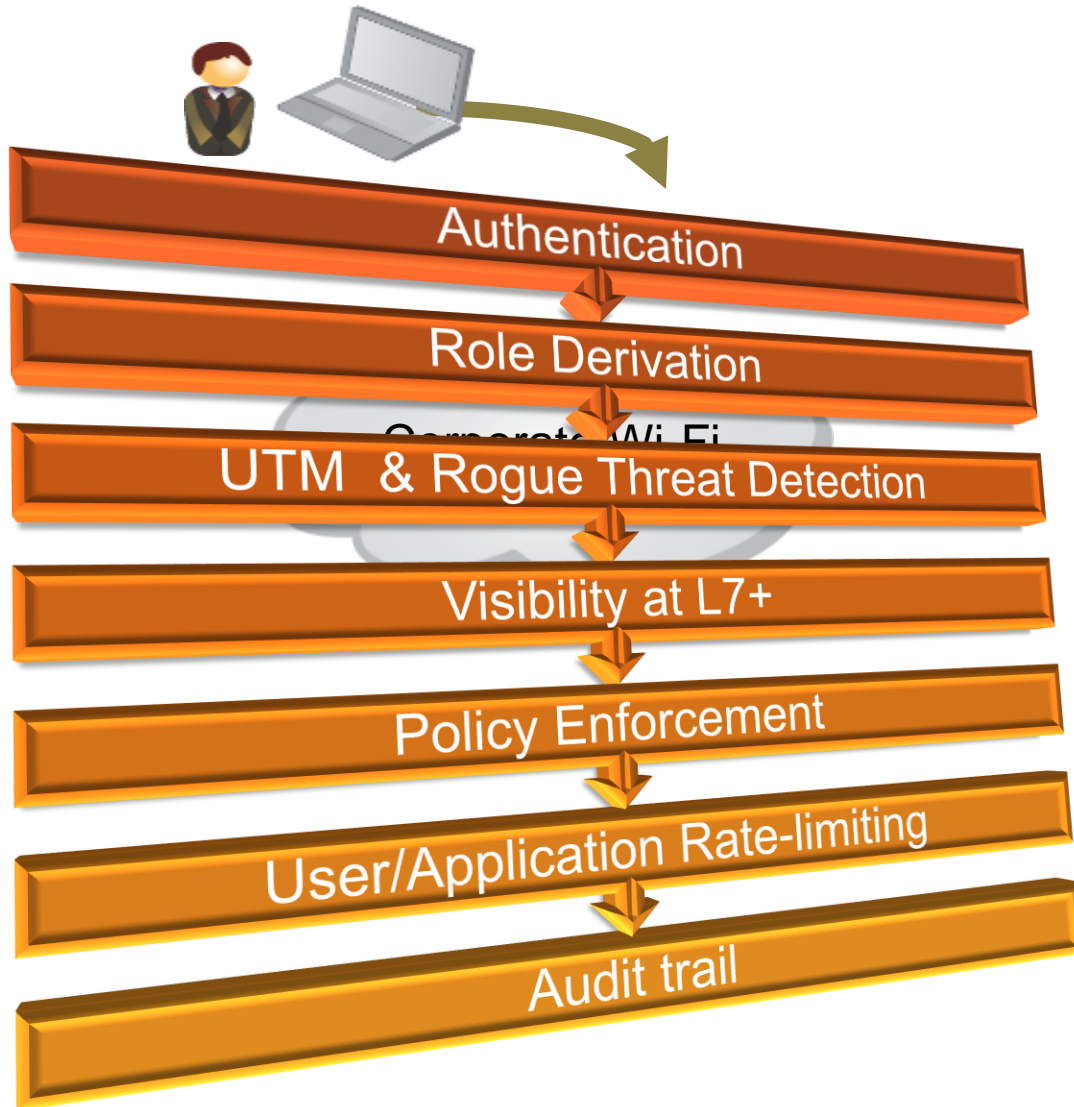
SECURE ACCESS

UNIFIED SECURE ACCESS



Integrated Connectivity Management with Security

WIRELESS CONTROLLER



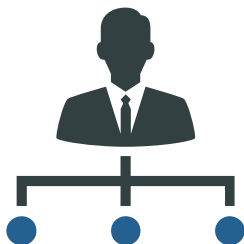
SECURE ACCESS APPROACH

1. Captive Portal, 802.1x—Radius /shared key
2. Assign users and devices to their role
3. Examine wireless traffic to remove threats
4. Identify applications and destinations
5. Apply policy to users and applications
6. Ensures Business traffic has priority
7. Reports on policy violations, application usage, destinations and PCI DSS

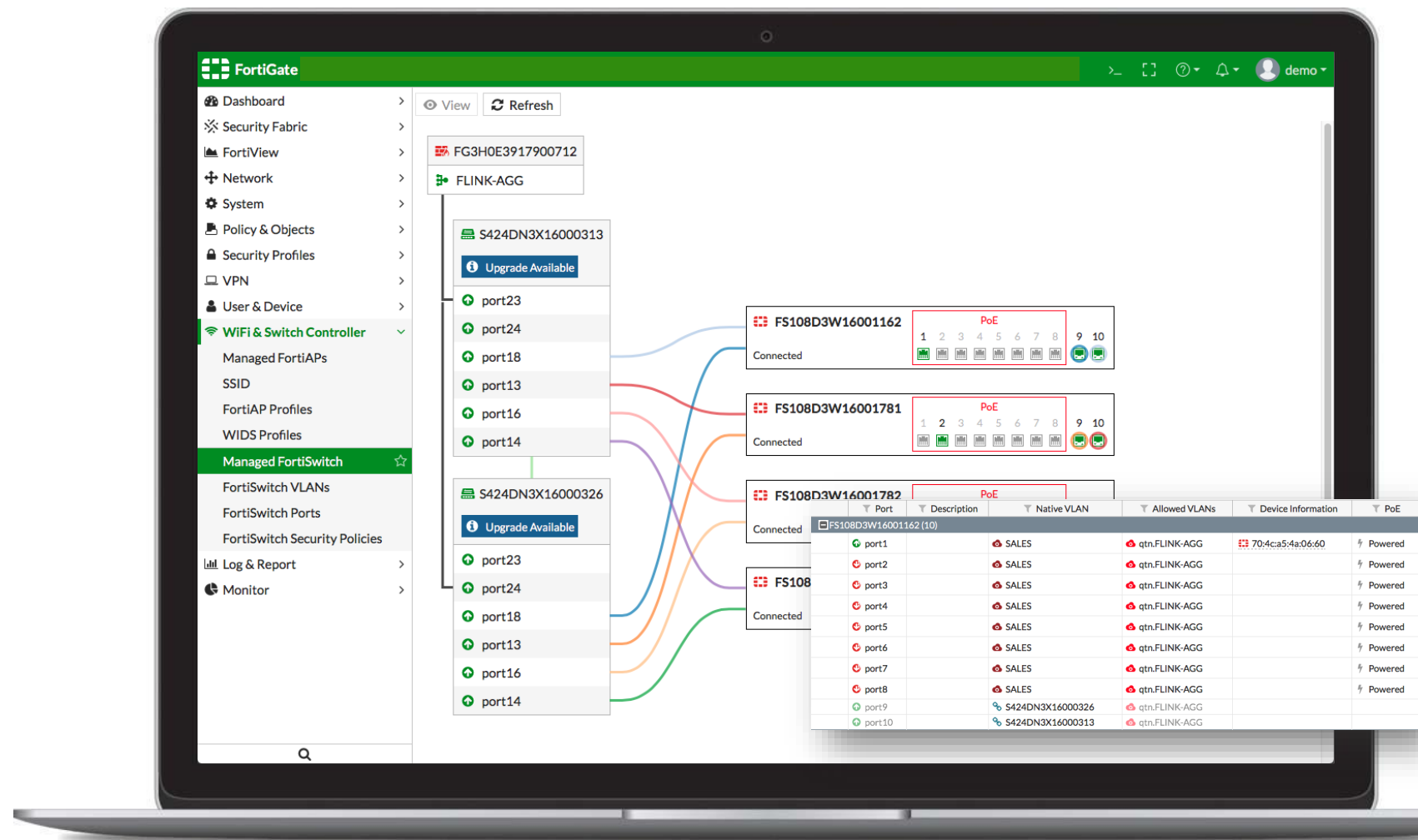
SECURITY FABRIC | NETWORKING

SWITCH CONTROLLER

INTEGRATED SWITCH MANAGEMENT



- Easily connects switches to FortiGate via FortiLink
- Setup stacks, configure and upgrade switches firmware with FortiOS
- Port level visibility – what is connected, plus contextual info on topology map and Device Inventory





Fabric extension to endpoints

FORTICLIENT

Fortinet's FortiClient Endpoint Protection Platform



Antivirus



Application Firewall



2-Factor Authentication



WAN Optimization



Web Filter



Vulnerability Scanning



Remote VPN



Part of Fortinet's ATP System (Sandbox Integration)



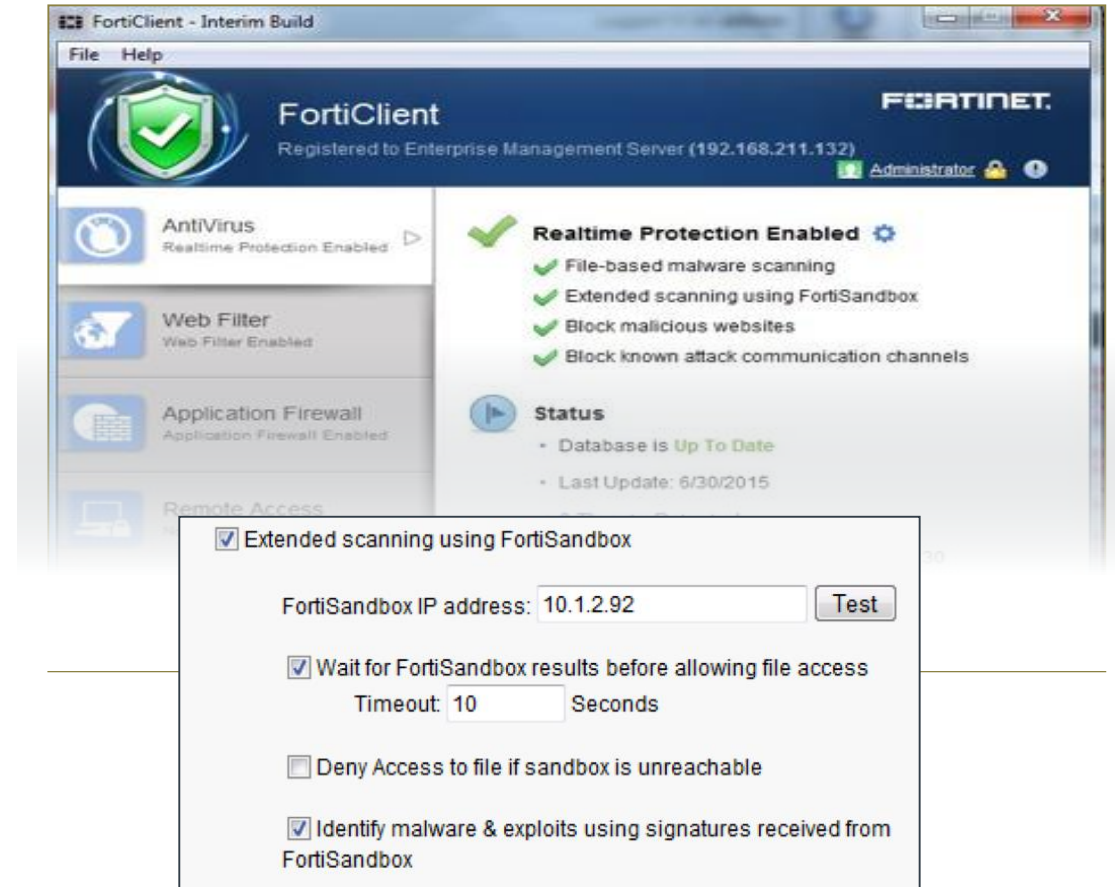
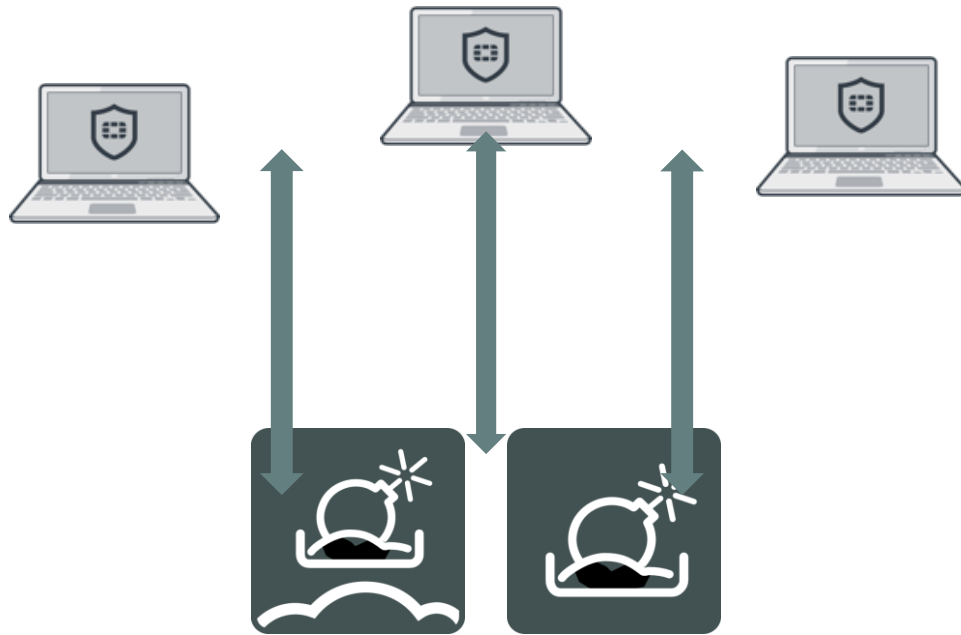
- ✓ Top rated protection
- ✓ Easy deployment
- ✓ Low TCO

Independent Validation



FortiClient Integration

- Hold For or Act Upon Result
- Dynamic, Local Threat Intelligence



The background of the slide is a deep red color. It features a faint, white network diagram consisting of numerous nodes connected by thin lines, resembling a web or a molecular structure. In the lower right portion of the background, there is a blurred image of a microscope. A specific part of the microscope, a cylindrical component, is clearly visible and has the text "40X" printed on it in white. The overall aesthetic is technical and scientific.

FABRIC BENEFITS

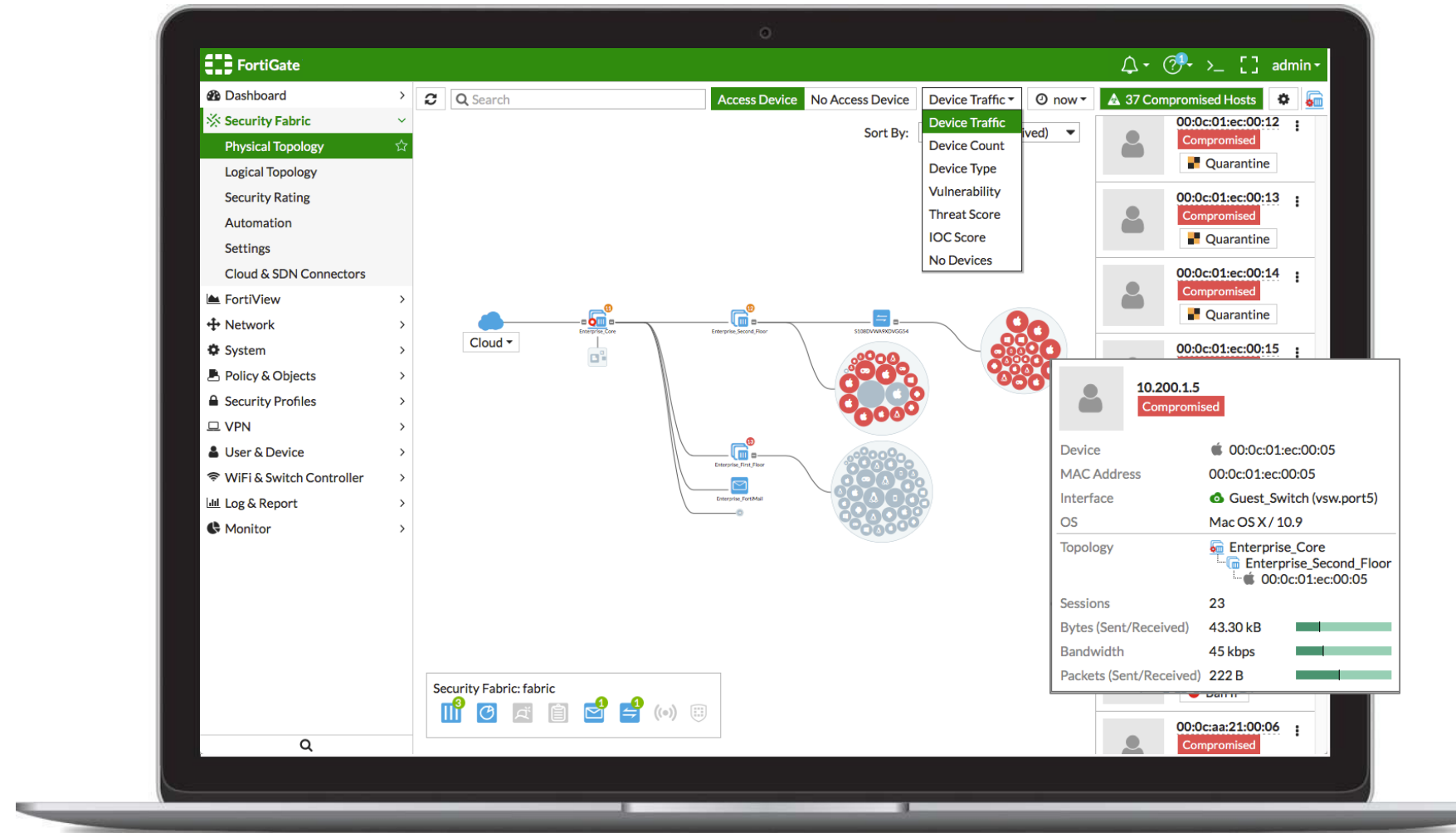
SECURITY FABRIC | OPERATION

VISIBILITY

TOPOLOGY MAPS



- Visualization of Security Fabric components from physical and logical connectivity perspective
- Mouse-over for endpoint contextual details
- Remote login to downstream FortiGate

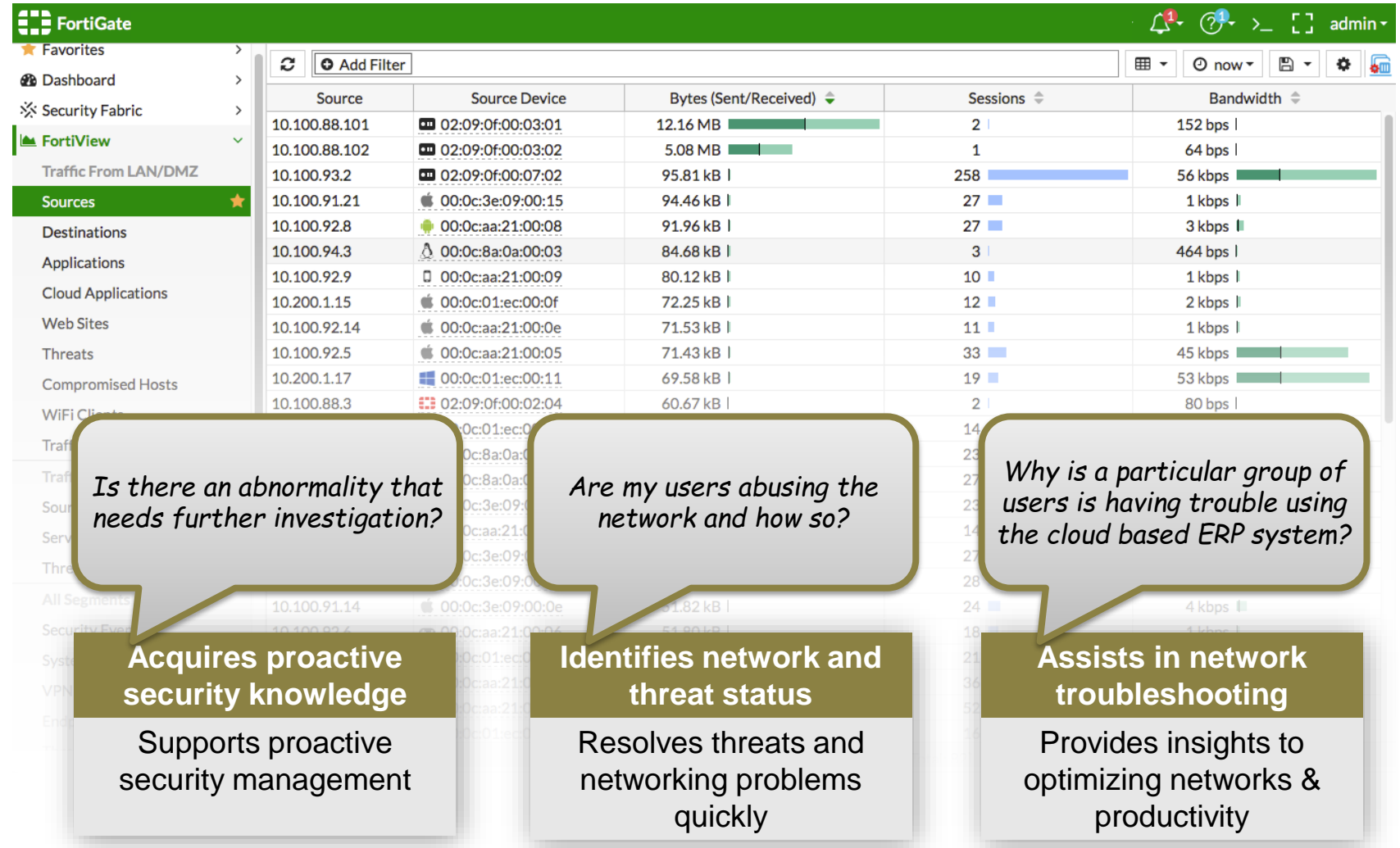


SECURITY FABRIC | OPERATION VISIBILITY

FORTIVIEW



- Powerful on-demand query tool that provides contextual results with drill down capabilities
- Presents in various viewers
- Uses real-time or historical data from FortiAnalyzer or FortiCloud
- Aggregated data from downstream FortiGates within the Security Fabric





FortiGate

Dashboard

Security Fabric

FortiView

Traffic From LAN/DMZ

Sources

Destinations

Applications

Cloud Applications

Web Sites

Threats

Compromised Hosts

WiFi Clients

Traffic From WAN

Sources

Servers

Threats

Source Interface:

Application

port2

port3

port4

ssl.root

toAWS

HTTPBROWSER

SMTPS

NTP

IMAPS

Android

HTTPS.BROWSER

Facebook

TCP 143

Unknown

Video/Audio

Web.Client

Video/Audio

Bytes (Sent/Received)

Sessions

Bandwidth

1.07 MB

970.85 kB

379.44 kB

307.57 kB

287.48 kB

268.74 kB

182.48 kB

29.89 kB

18.70 kB

14.90 kB

6.84 kB

6.32 kB

3.81 kB

3.06 kB

8

49

1133

49

37

2

19

2

5

2

13

1

3

1

251 kbps

9 kbps

528 bps

6 kbps

0 bps

0 bps

0 bps

2 kbps

0 bps

5 kbps

18 kbps

Sort rows to display
Top sessions

Setup query using
easy-to-use auto-
complete filters

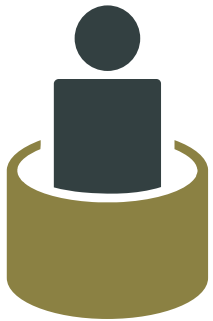
Examine real-time or
historical data

Select row for drill
down

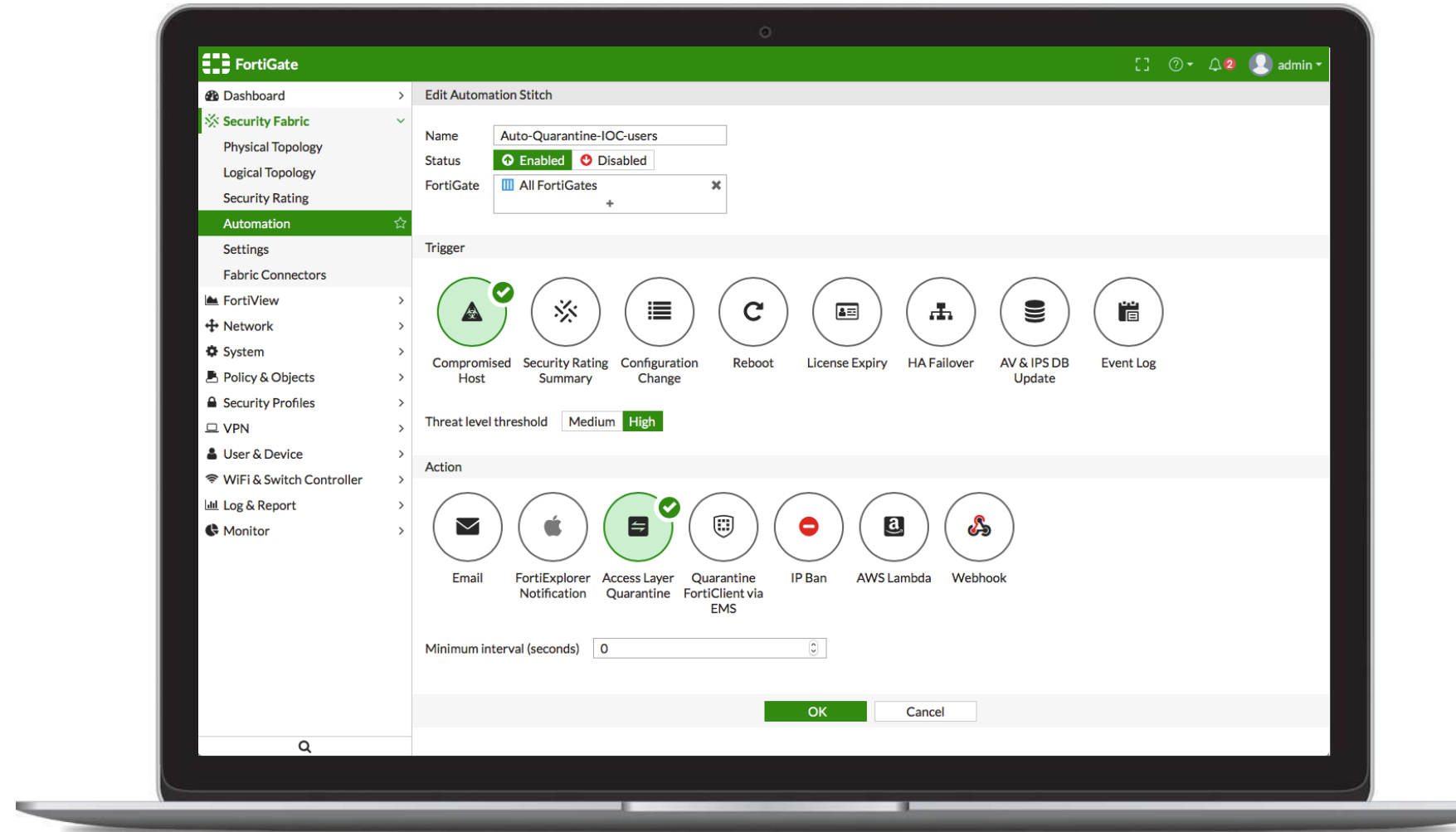
SECURITY FABRIC | OPERATION

AUTOMATION

QUARANTINE

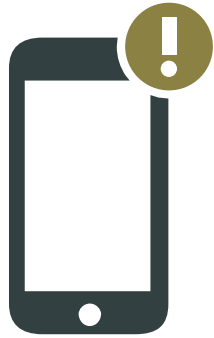


- Automatically quarantine compromised hosts via Stitch
- Option to do so using FortiClient via EMS or connection via FortiSwitch and FortiAP

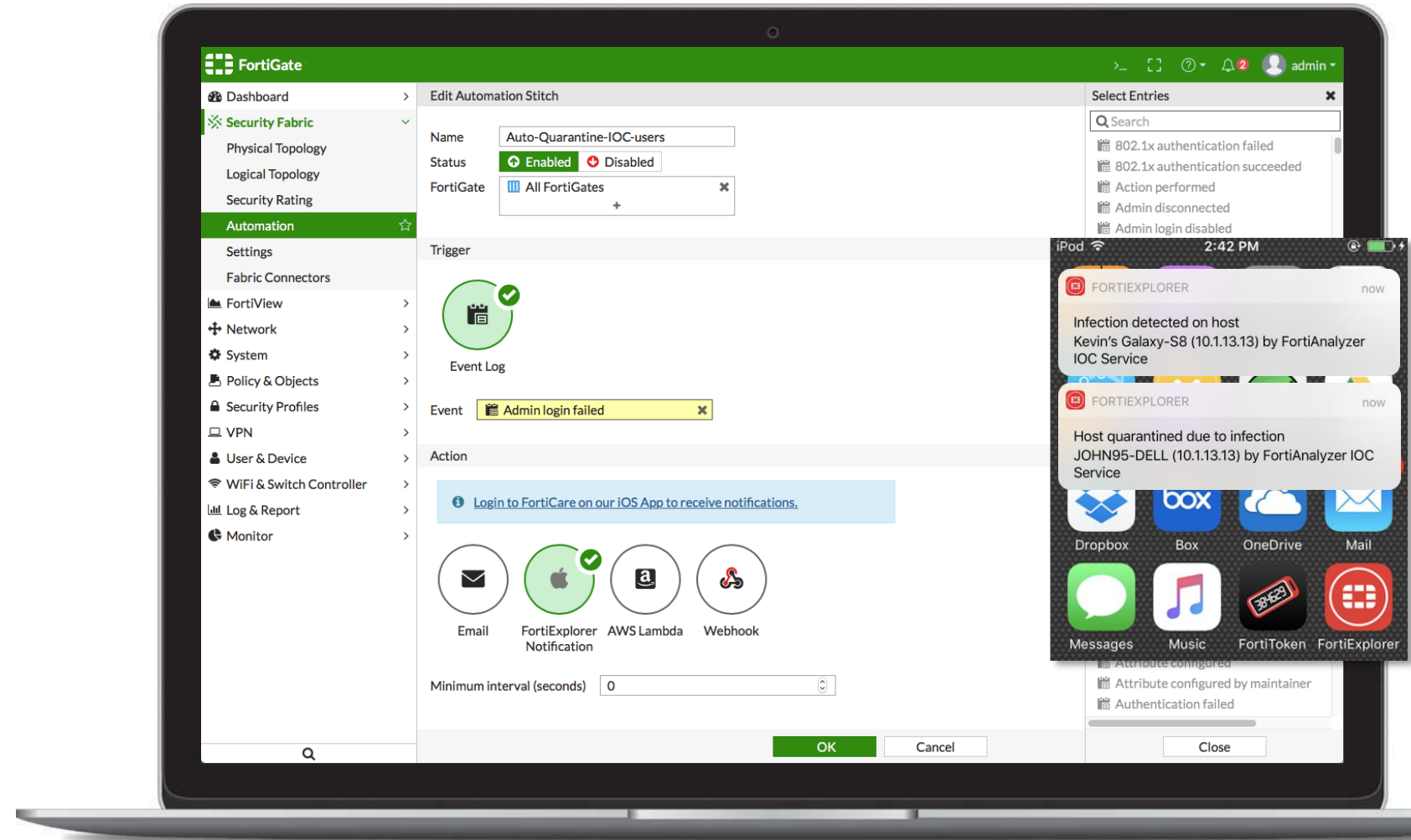


SECURITY FABRIC | OPERATION AUTOMATION

NOTIFICATIONS



- iOS Push notification via FortiExplorer

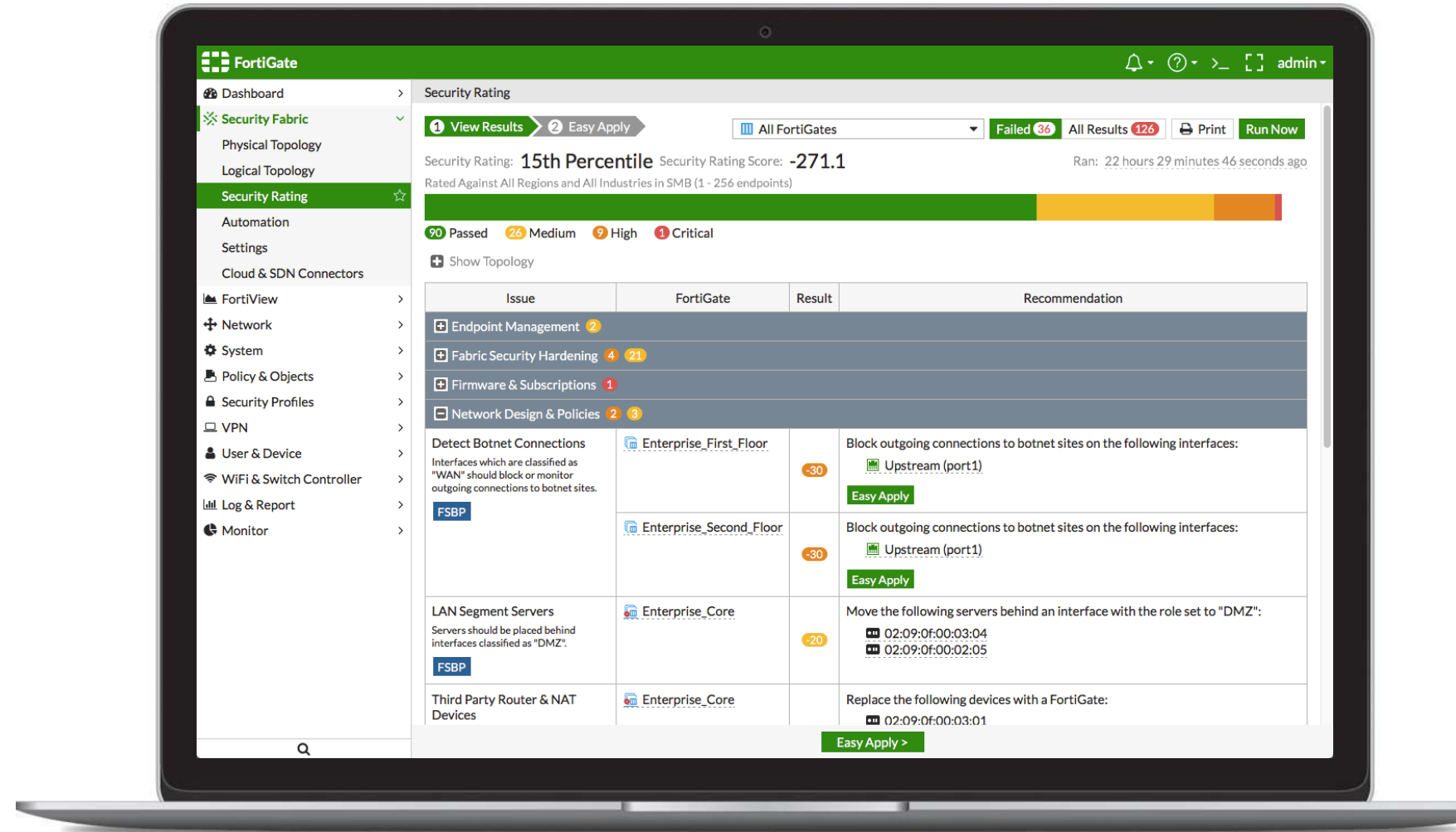


COMPLIANCE & SECURITY RATING

SECURITY RATING AUDIT



- Fabric-wide audit against
 - » Endpoint agent installation
 - » Configuration hardening
 - » Subscription status
 - » Network Design & Policies
 - » ATP implementation
- Provides recommendation or one-click fixes

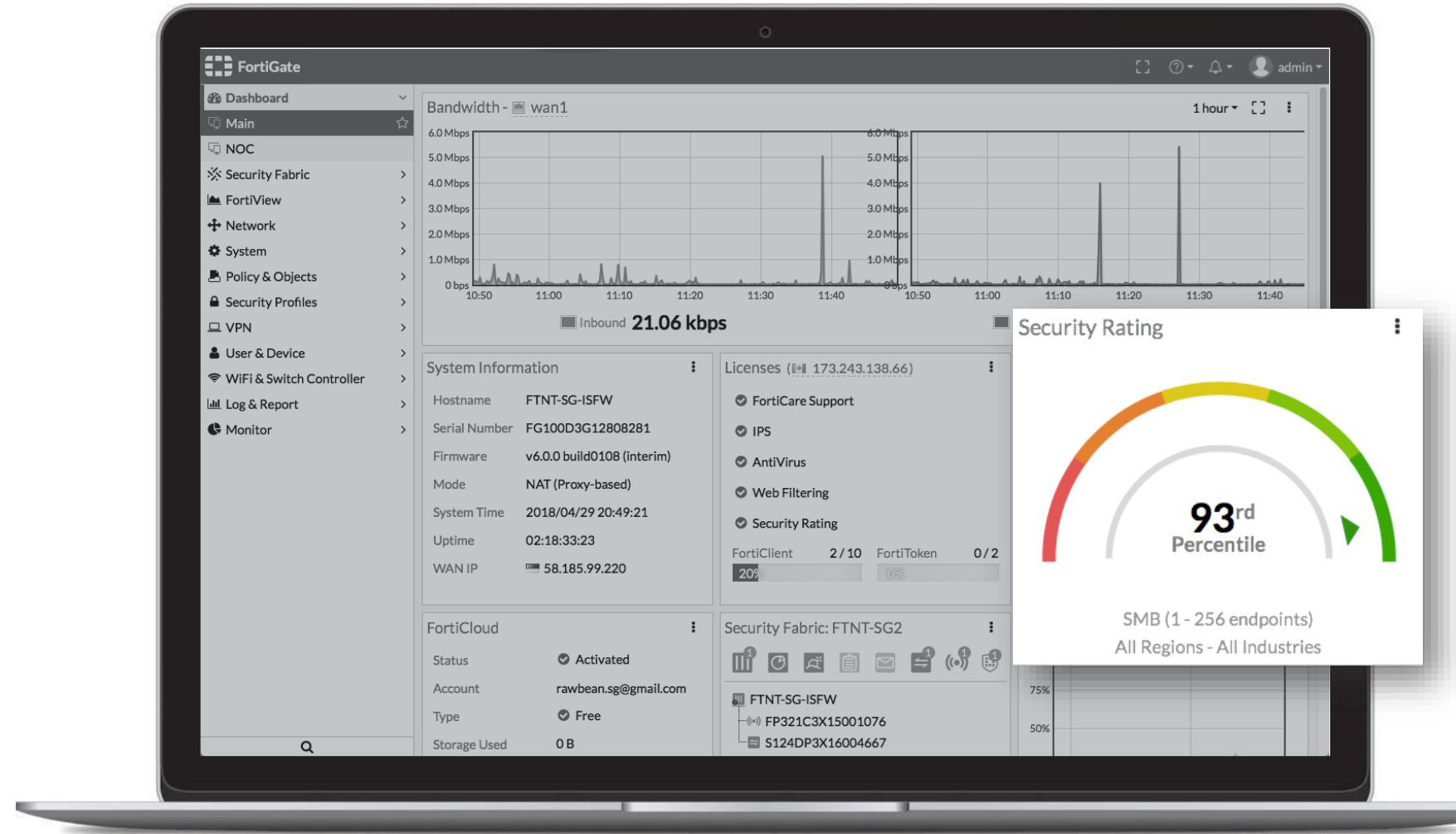


COMPLIANCE & SECURITY RATING

SECURITY RATING RANKING

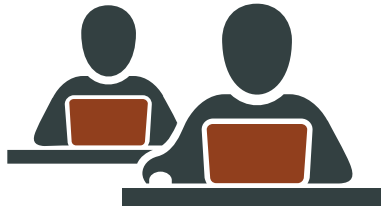


- Benchmark against peers
 - » Rank against similar organizations in term of size and industry by percentile
 - » Requires FortiGuard Security Rating subscription

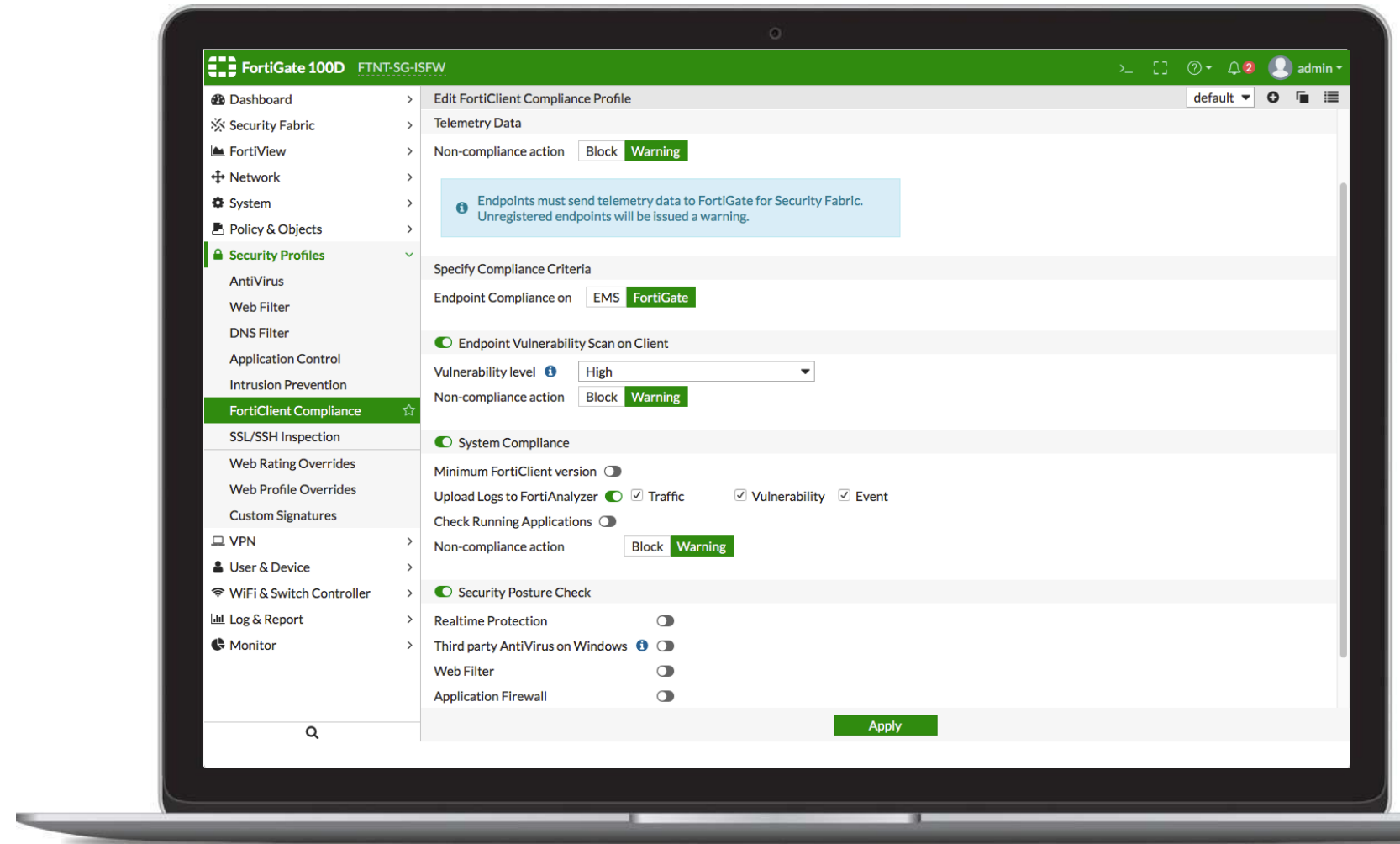


COMPLIANCE & SECURITY RATING

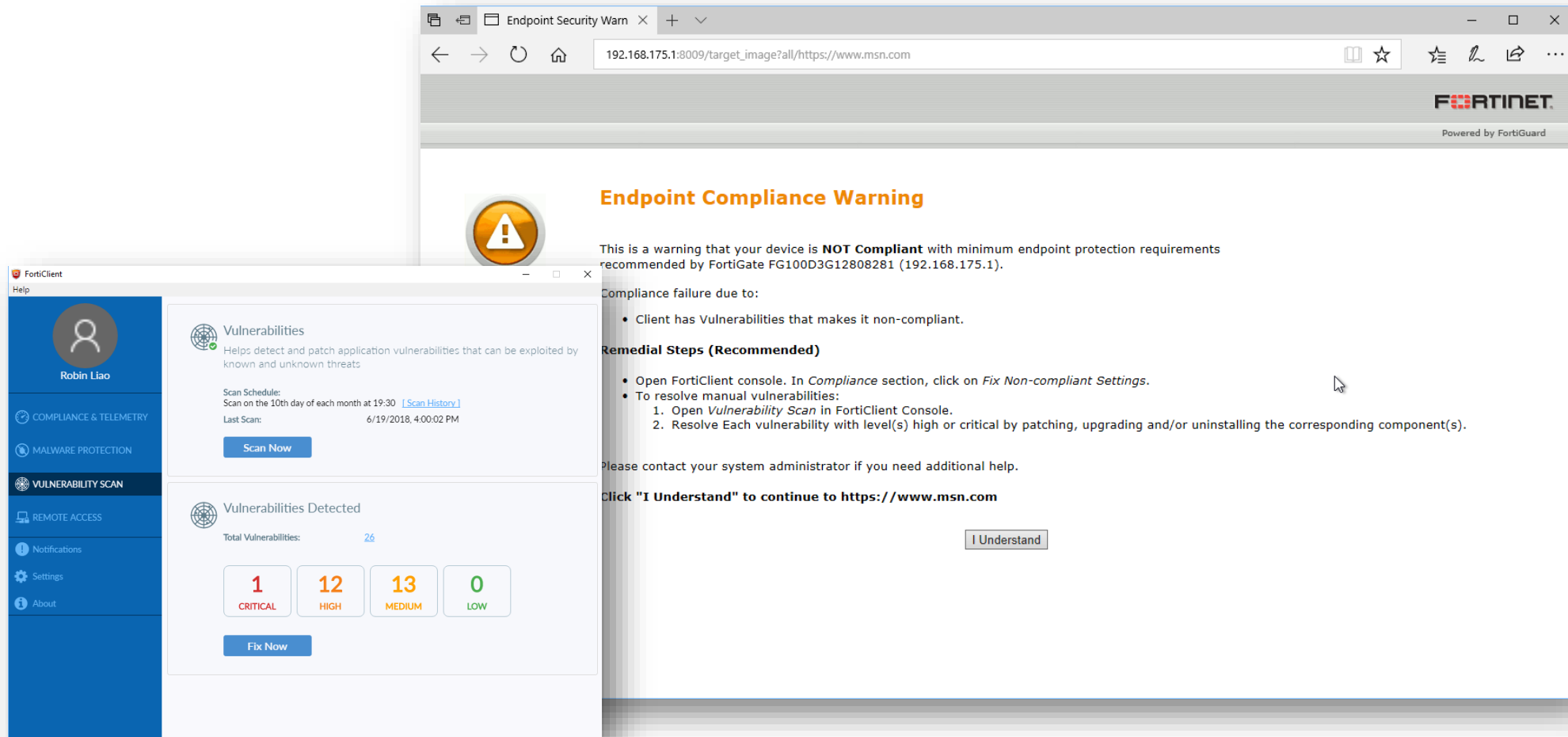
ENDPOINT COMPLIANCE



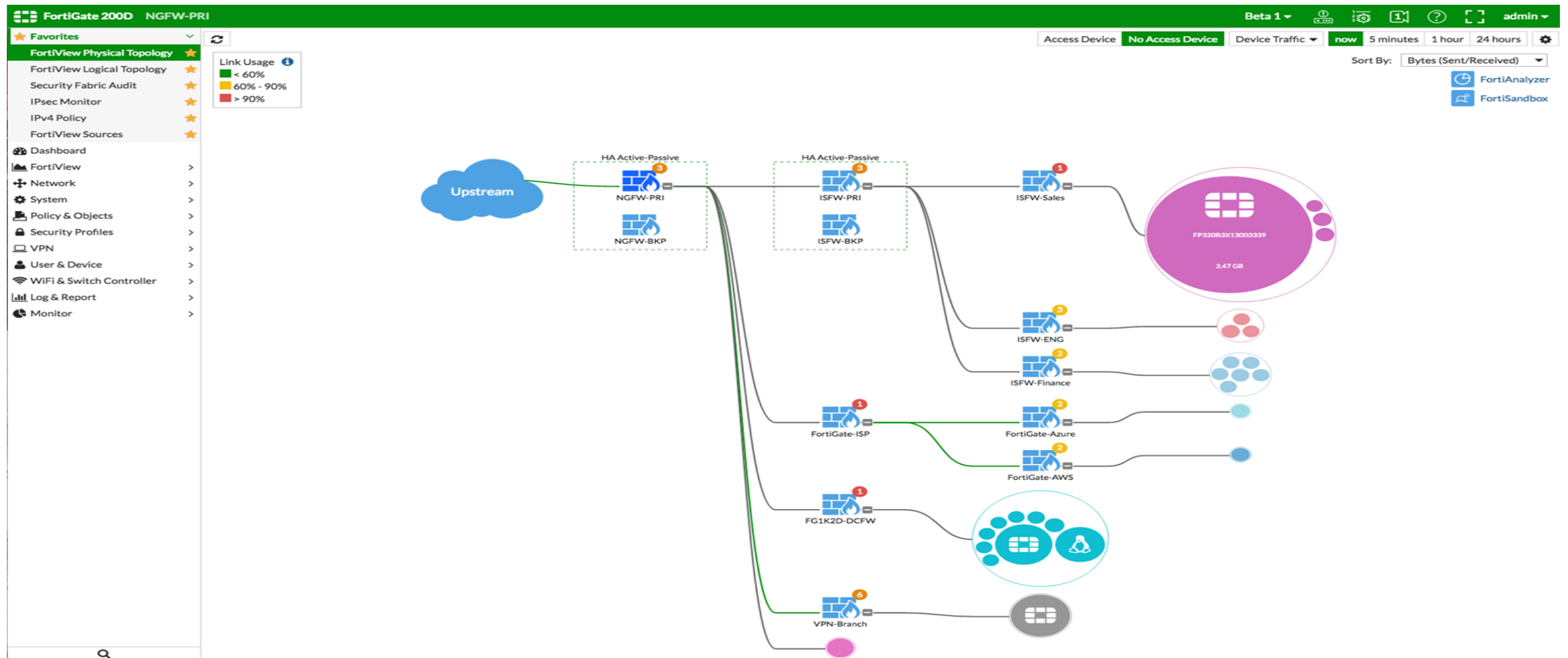
- Different profiles can be setup accordingly such as Location (Source IPs), User groups and/or Device types etc
- Compliance criteria includes Vulnerability scan status, Windows application/process presence and FortiClient configurations
- Warn or block clients if not compliant



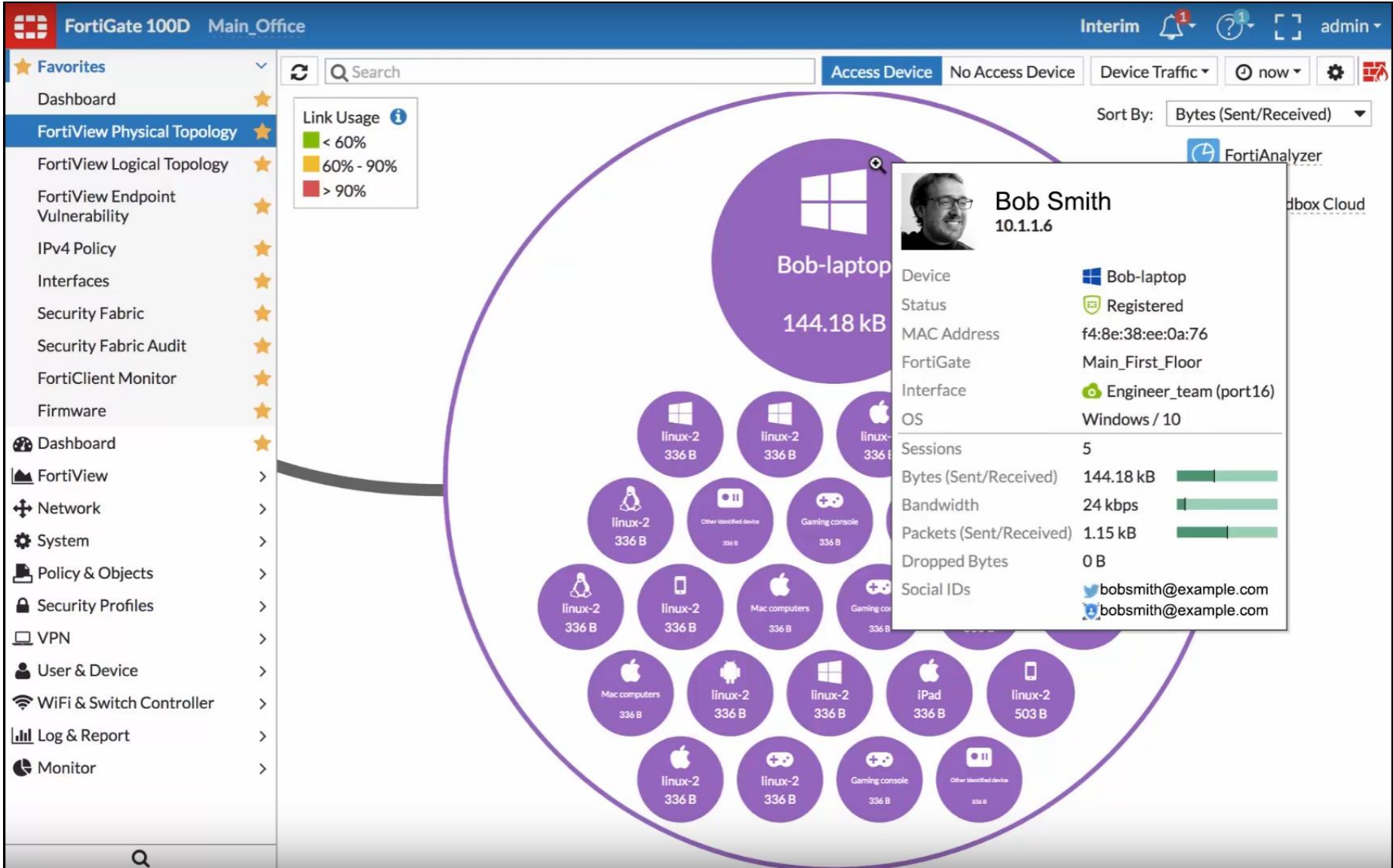
COMPLIANCE & SECURITY RATING



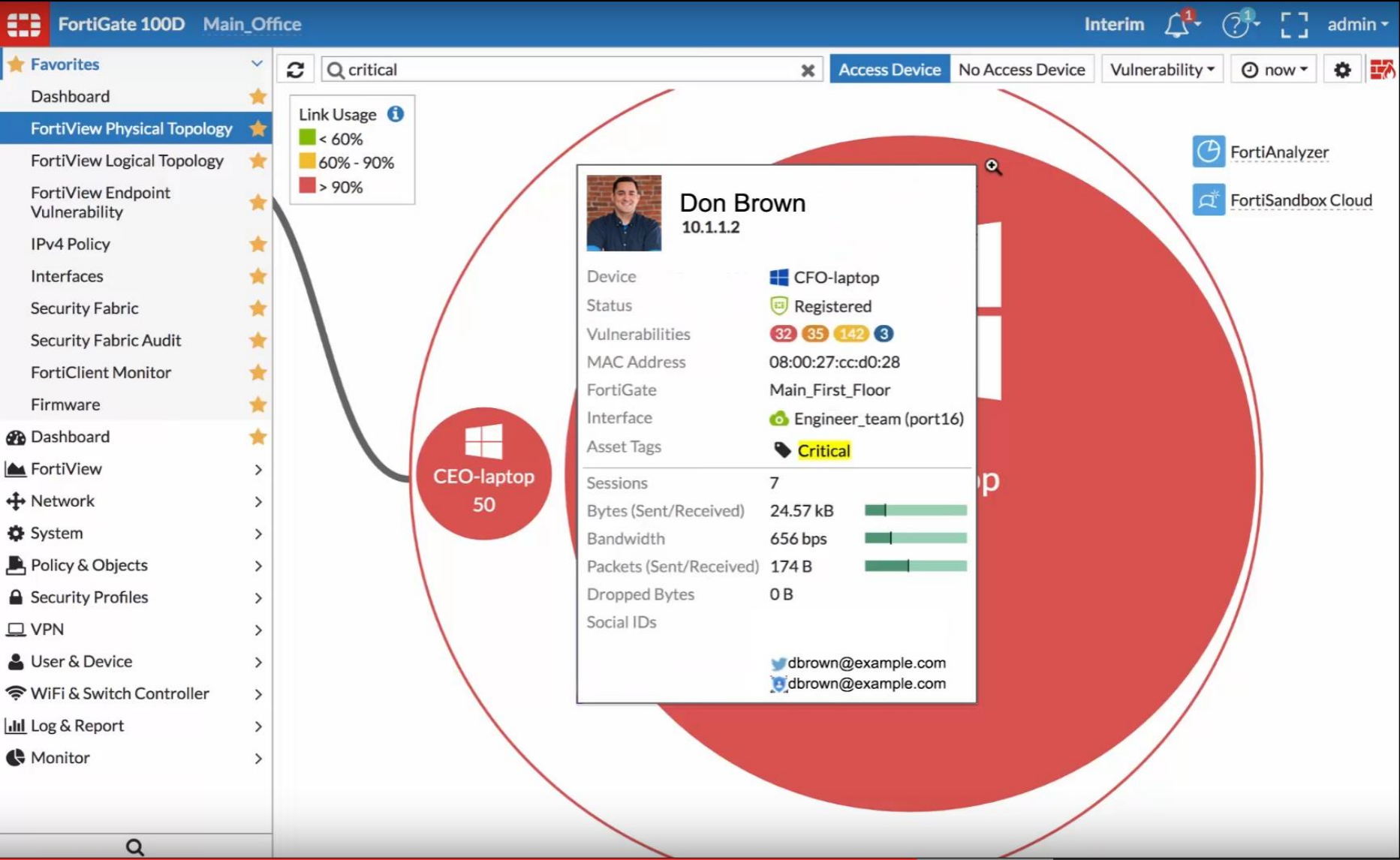
Visibility



More visibility



Asset tagging



Easy apply

FortiGate 100DMain_Office

Interim1

admin

★ Favorites

Dashboard★

FortiView Physical Topology★

FortiView Logical Topology★

FortiView Endpoint Vulnerability★

IPv4 Policy★

Interfaces★

Security Fabric★

Security Fabric Audit★

FortiClient Monitor★

Firmware★

Dashboard★

FortiView>

Network>

System>

Policy & Objects>

Security Profiles>

VPN>

User & Device>

WiFi & Switch Controller>

Log & Report>

Monitor>

Security Fabric Audit

Unauthorized FortiSwitches

All discovered FortiSwitches should be authorized or disabled.

Main_Second_Floor

Medium

Authorize or disable the following FortiSwitches:

FAP28C3X13000146

S124DN3W15000797

Security Best Practices

Detect Botnet Connections

Interfaces which are classified as "WAN" should block or monitor outgoing connections to botnet sites.

Main_Office

High

Block outgoing connections to botnet sites on the following interfaces:

wan1

Main_First_Floor

High

Block outgoing connections to botnet sites on the following interfaces:

wan2

Main_Second_Floor

High

Block outgoing connections to botnet sites on the following interfaces:

wan2

Main_Office

High

Enable HTTPS redirection globally in order to force HTTP to HTTPS on 1 interfaces(s).

Main_First_Floor

High

Enable HTTPS redirection globally in order to force HTTP to HTTPS on 1 interfaces(s).

Main_Second_Floor

High

Enable HTTPS redirection globally in order to force HTTP to HTTPS on 1 interfaces(s).

Main_Second_Floor

High

Disable Telnet access on the following interfaces:

wan2

Main_Office

Medium

Enable a simple password policy for system administrators.

Main_First_Floor

Medium

Enable a simple password policy for system administrators.

< Back

Apply Recommendations

Cancel

The background of the slide is a deep red color. It features a faint, white network diagram consisting of numerous interconnected dots and lines, resembling a molecular structure or a data network, spread across the upper half. On the right side, there is a blurred image of a microscope. A specific part of the microscope, a cylindrical component, is clearly visible and has the text "40X" printed on it in white. The overall aesthetic is scientific and technological.

WHERE DO WE GO FROM HERE

EXPAND



Cloud

SDN

CASB

SD-WAN

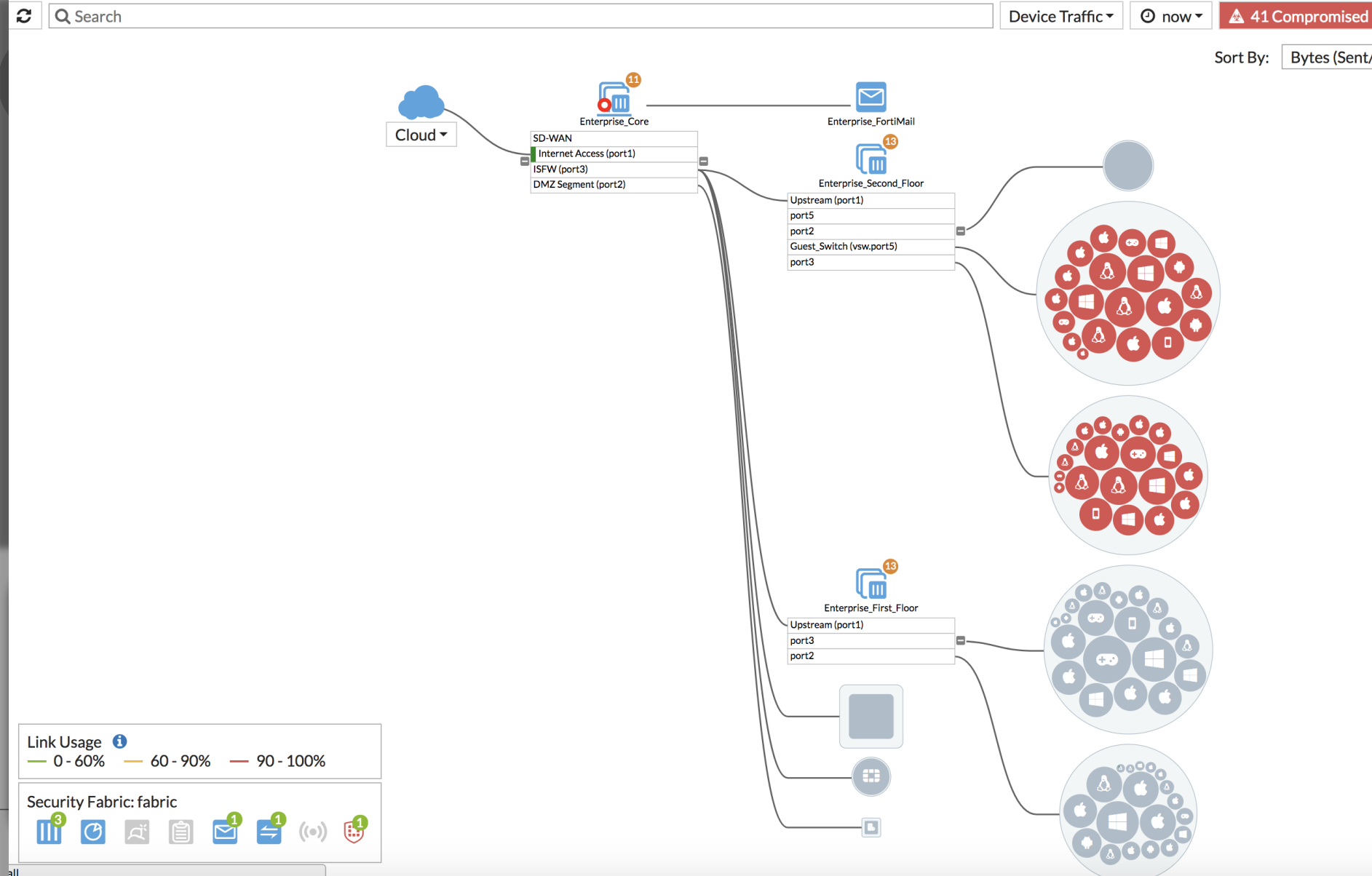
UEBA

Single Pane

AWS
Azure
Google
Oracle
VMWare
KVM

Acceleration

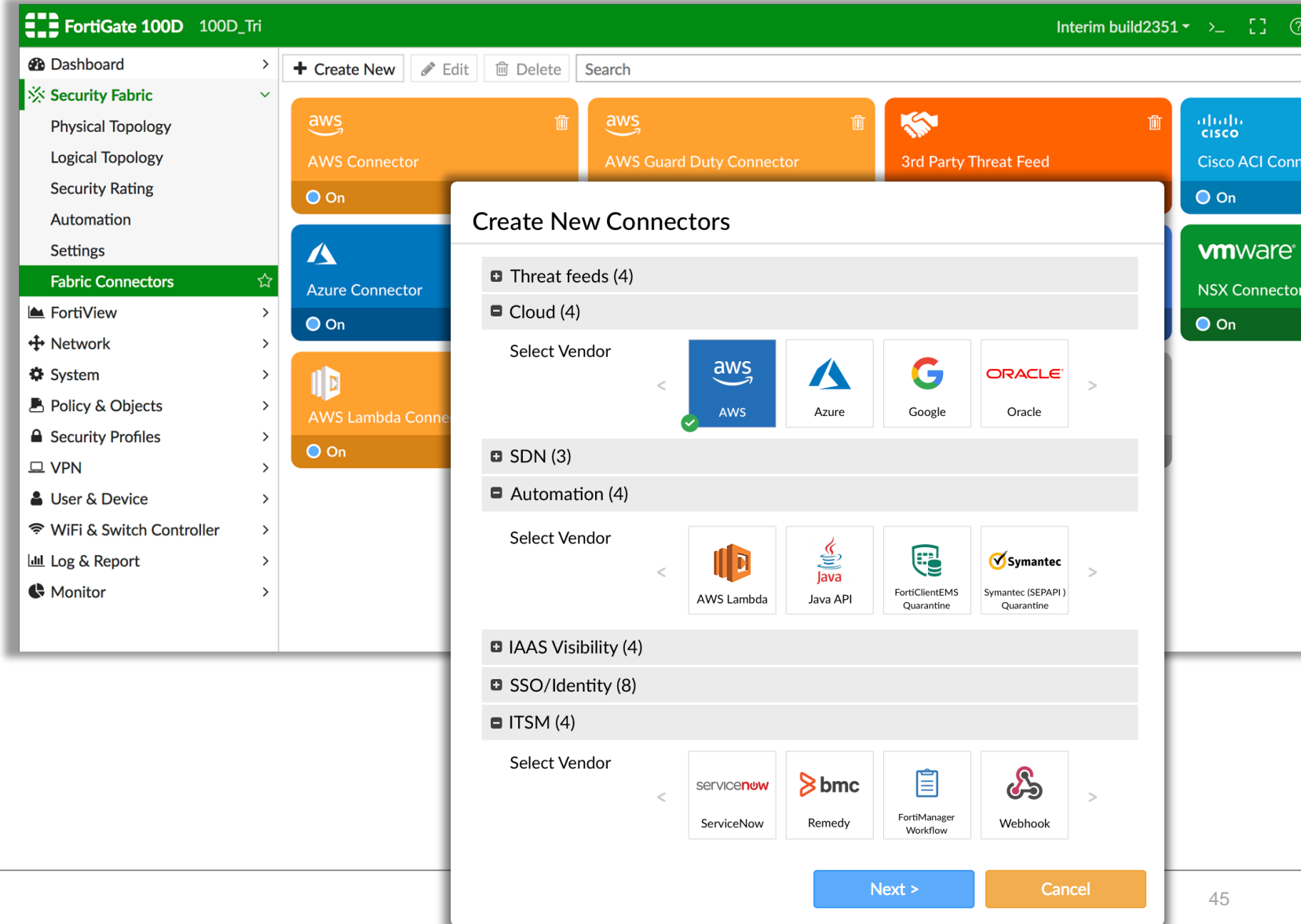
Dynamic
Policies



INTEGRATE

Fabric Connectors

Threat Feeds
Dynamic Policy
Automation /
Remediation
IAAS
SSO
ITSM
Endpoint CVE



The screenshot displays the FortiGate 100D management interface. The left sidebar shows the navigation menu with 'Fabric Connectors' highlighted. The main panel shows a list of existing connectors: AWS Connector, AWS Guard Duty Connector, 3rd Party Threat Feed, Azure Connector, and AWS Lambda Connector. A 'Create New Connectors' modal window is open, showing categories and vendor selection options.

Create New Connectors

- Threat feeds (4)**
- Cloud (4)**
 - Select Vendor: AWS (selected), Azure, Google, Oracle
- SDN (3)**
- Automation (4)**
 - Select Vendor: AWS Lambda, Java API, FortiClientEMS Quarantine, Symantec (SEAPI) Quarantine
- IAAS Visibility (4)**
- SSO/Identity (8)**
- ITSM (4)**
 - Select Vendor: ServiceNow, BMC Remedy, FortiManager Workflow, Webhook

Buttons: Next >, Cancel

MEASURE



Integrated Measurement

Fabric-wide Reporting

Multi-product

**Industry, Region & Size
Comparison**

How Secure Am I?



Map

DETECT



APT

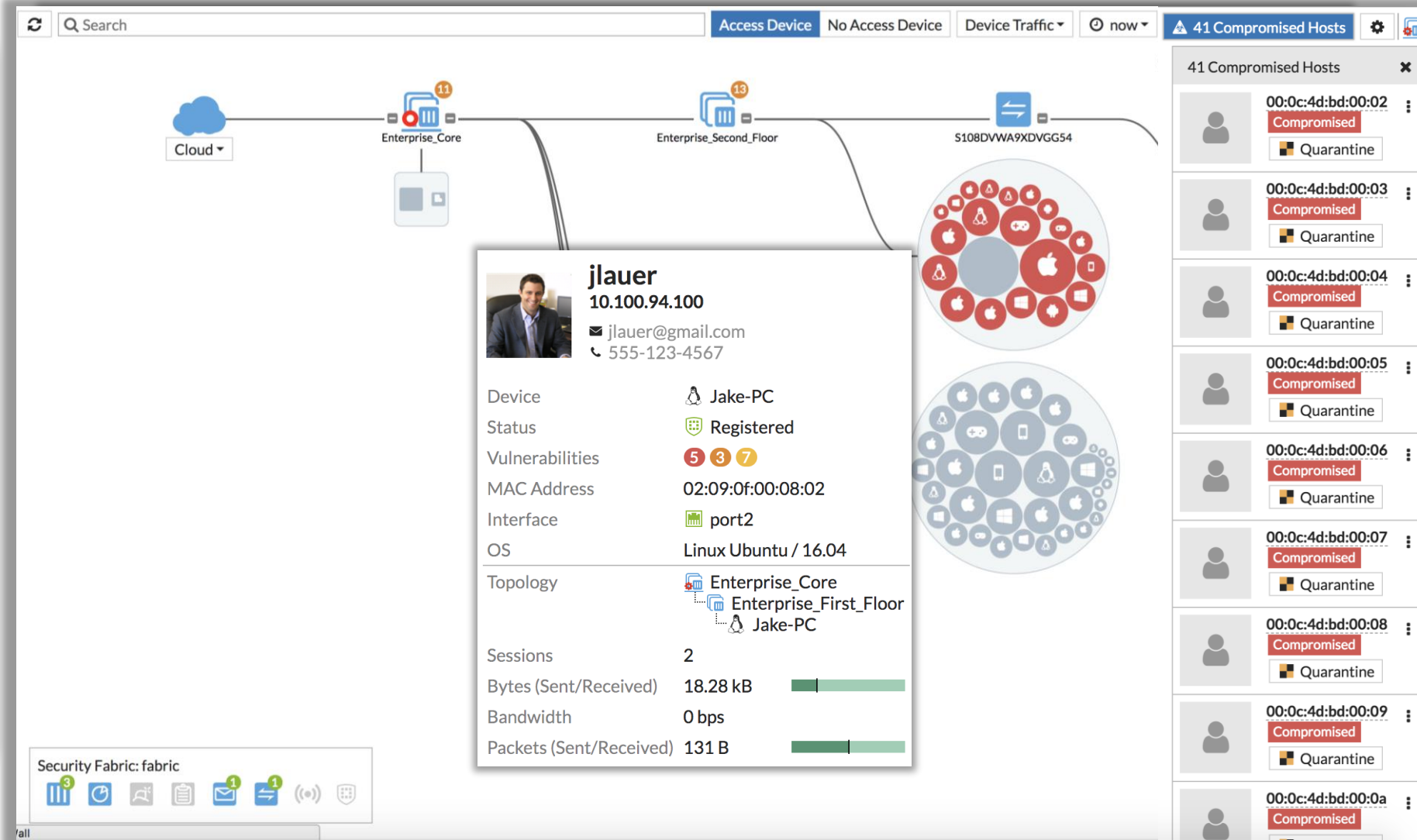
IOC

3rd Party

Vulnerability

UEBA

Weakness



AUTOMATE



Remediation

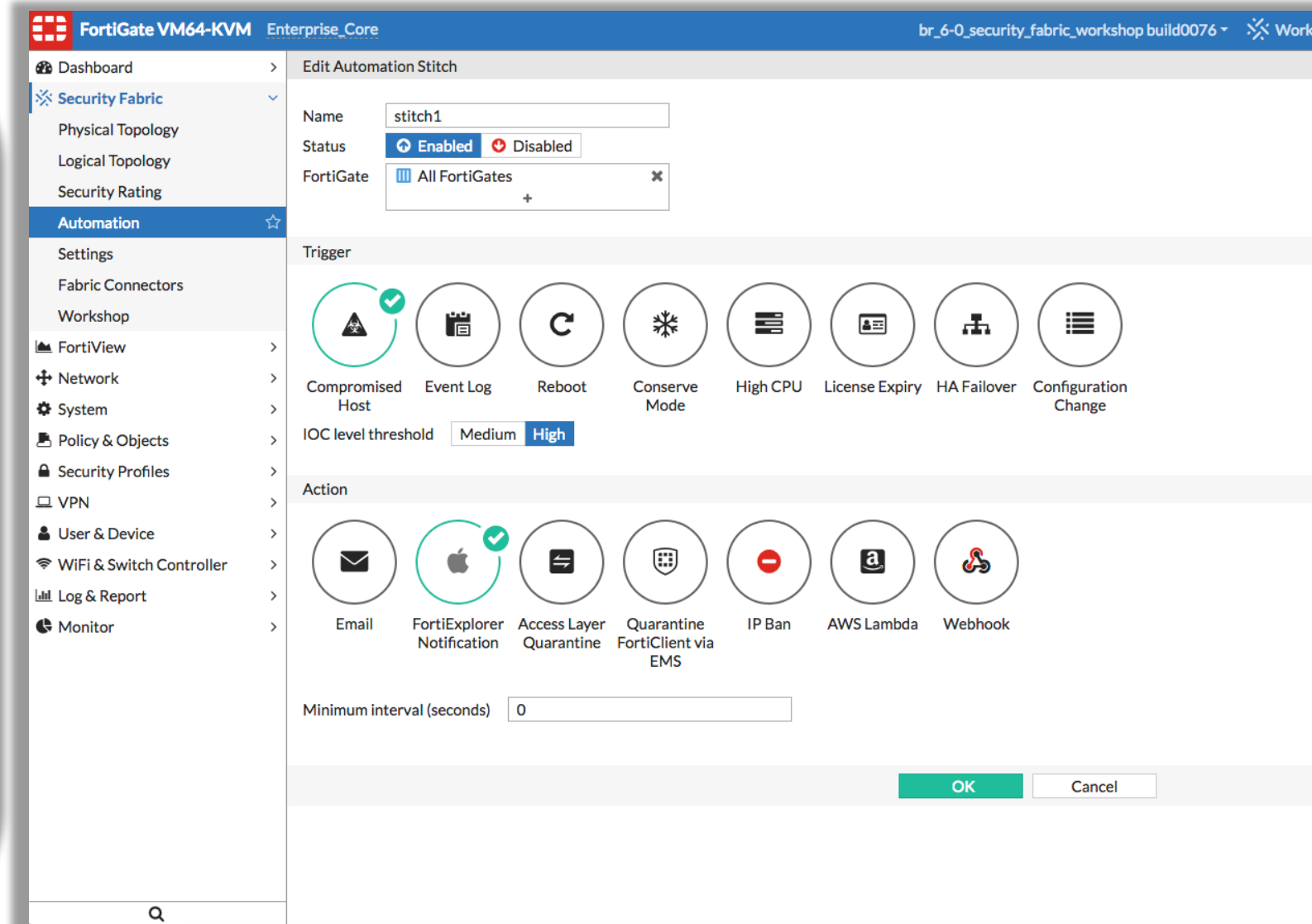
Framework (Stitches)

Fabric Inputs

Fabric Outputs

IFTTT

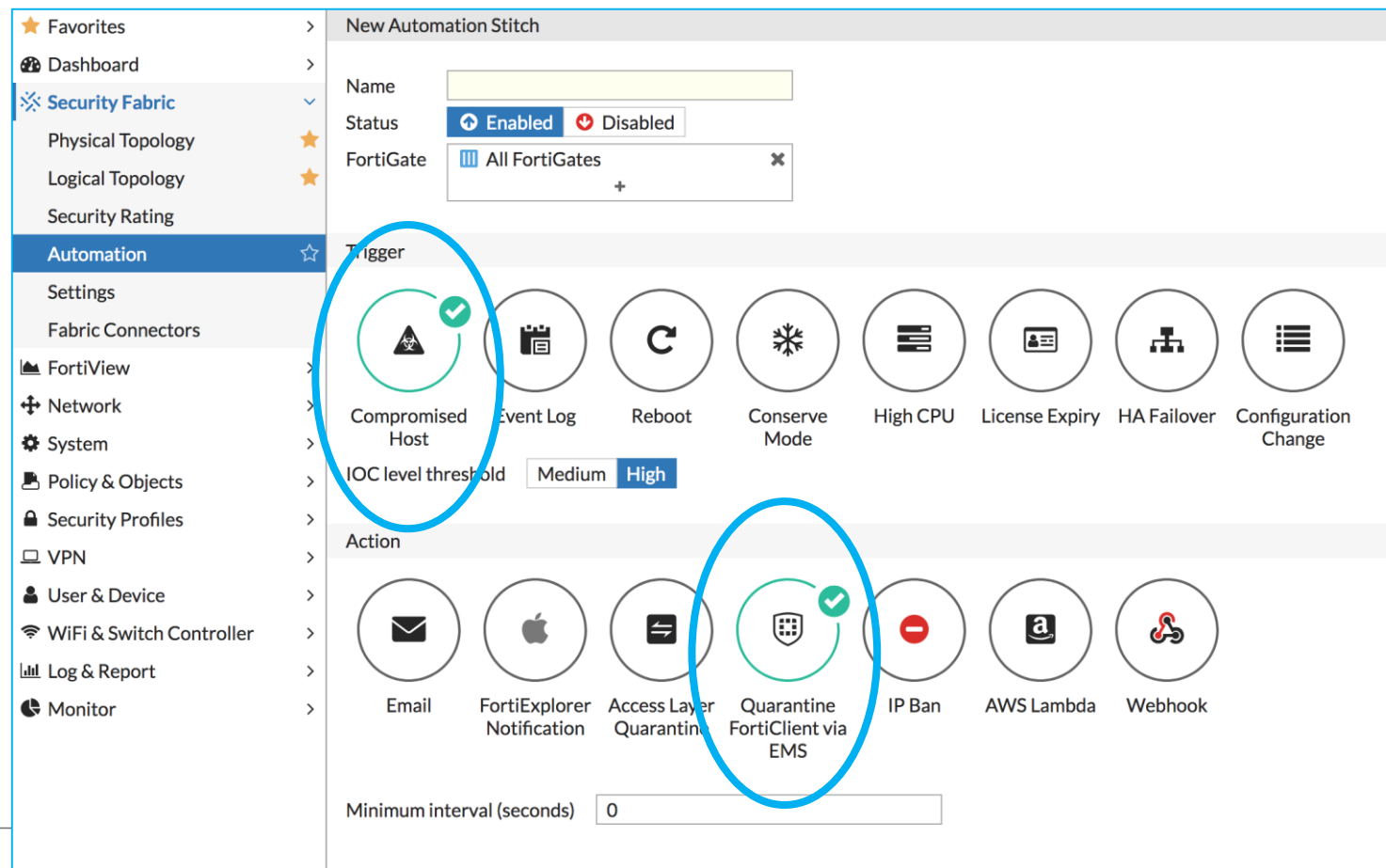
Endless



FortiClient Automatic Quarantine (FOS 6.0.0)

FOS 6.0.0

- Based on IOC level (medium/high)
- Automatic FortiClient quarantine via EMS



Wireless user quarantine

- Quarantine Host option to quarantine devices that are connected in Tunnel-mode
- Host gets an IP address from the quarantine VLAN

The image features the FORTINET logo in white, bold, sans-serif capital letters. The logo is centered horizontally and slightly above the vertical center. The background is a solid red color. Overlaid on the red background are several faint, white, hexagonal patterns. These patterns consist of concentric hexagons and some hexagons connected by thin lines, resembling a network or molecular structure. The patterns are scattered across the image, with some being larger and more prominent than others. The overall aesthetic is technical and modern.

FORTINET®