Fortinet Security Fabric

Christian Barnes – Director Systems Engineering
South Central US

The Fortinet Security Fabric

An Integrated Security Architecture

April, 2018

Cyber Security and Education

A continuous process of identification, protection, testing, remediation and evaluation of the defenses deployed to protect network and information asset as related to the broader internet

Policy
Thou Shalt, Thou Shalt Not

Procedure
Carrying out the Thou Shalts

Regulation
Mandated Requirements

Standards
Agreed Upon Practices

People
End Users, Operations, Technologists

Processes
Means and Methods

Technology
Devices, Applications, and Systems

Partnerships
Key Contributors that Cover Gaps in the Afore Mentioned…

Common and unique challenges facing the education space for faculty, students and parents including leveling access to technology,

Environment
Classroom, sizes

Curricula Access
Content and Media

Regulation
Mandated Requirements in privacy and safety

Funding
Budget Cycle vs Technology Cycle

Threat Types
Common Threat Types in School Districts

Communication Flows
Operational vs Educational

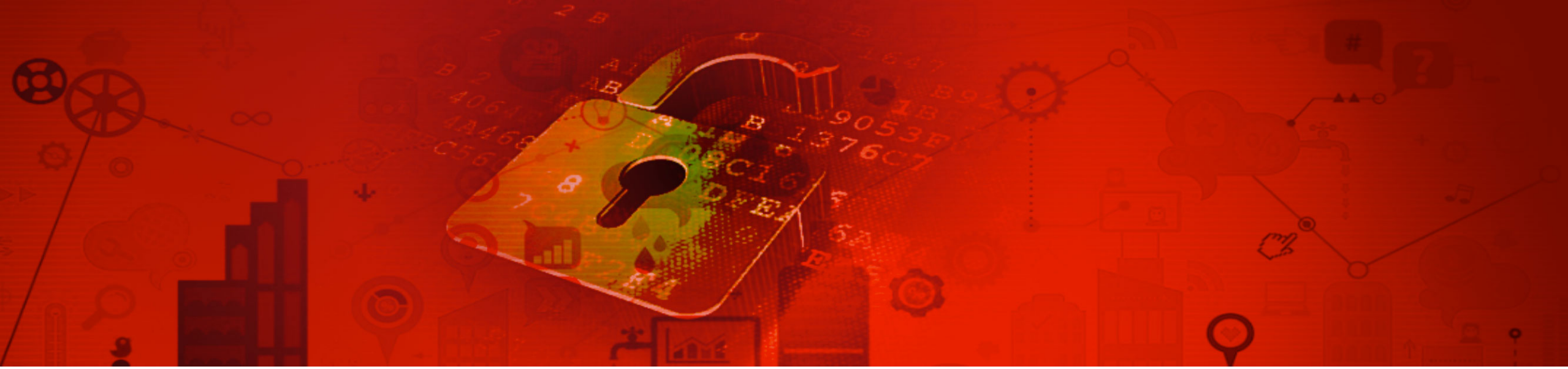
Technology
Devices, Applications, and Systems

Technologists
The practitioners within the School District

DX

is the integration of digital technology into all areas of the organization, resulting in fundamental operational changes and service value delivery

[Digital Transformation]



SX

is the integration of security into all areas of digital technology, resulting in a Security Architecture that provides a Continuous Trust Assessment

[Security Transformation]

Security Needs

The Analyst's View

Gartner

Scale to Support 100G

Expansion of network infrastructure to support new applications/services[1]

Gartner

Internal Segmentation

To contain attacks and limit the impact of a successful exploit[2]

Gartner

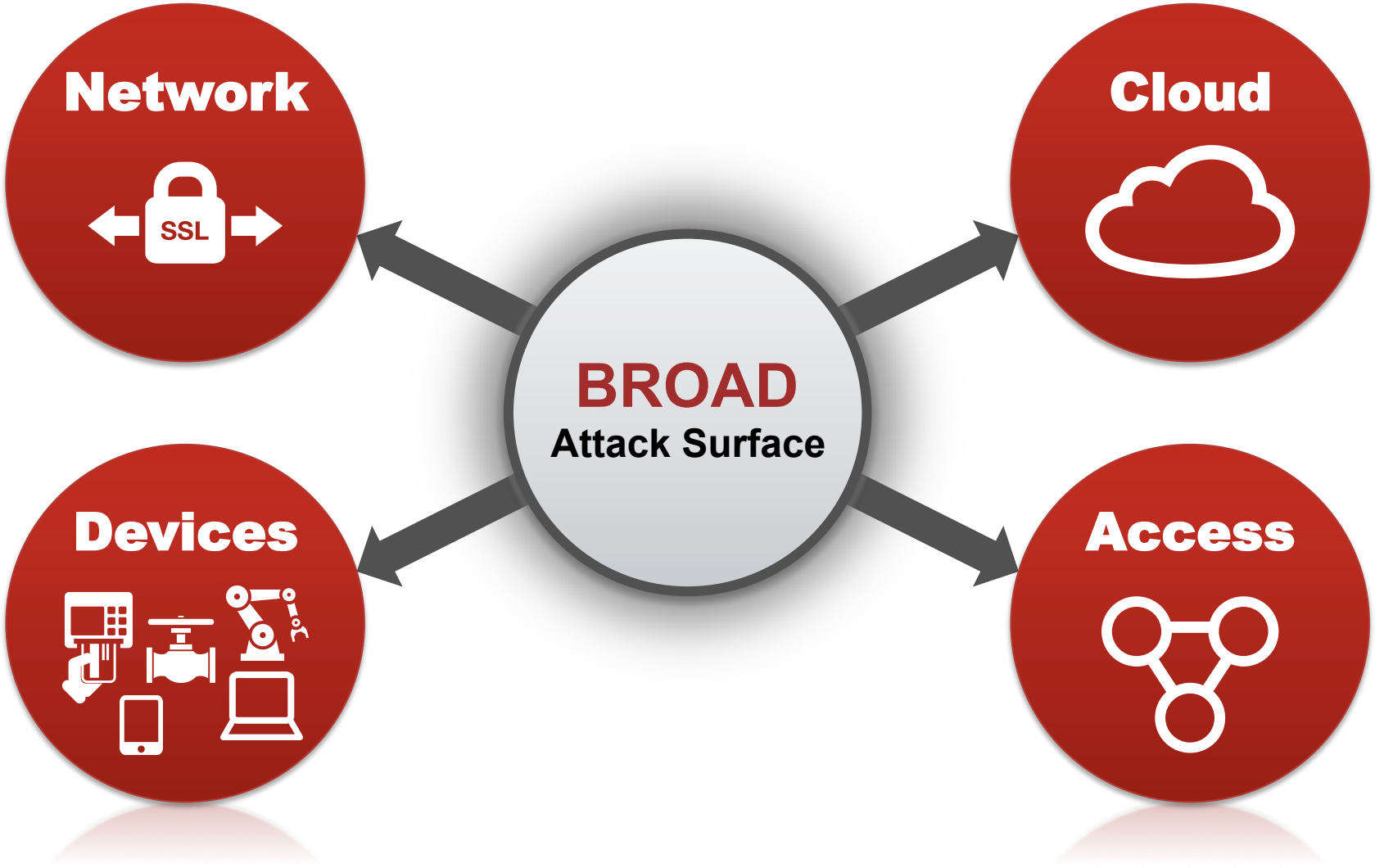
SSL Traffic Inspection

Growing number of malware attacks including Ransomware using HTTPS[3]

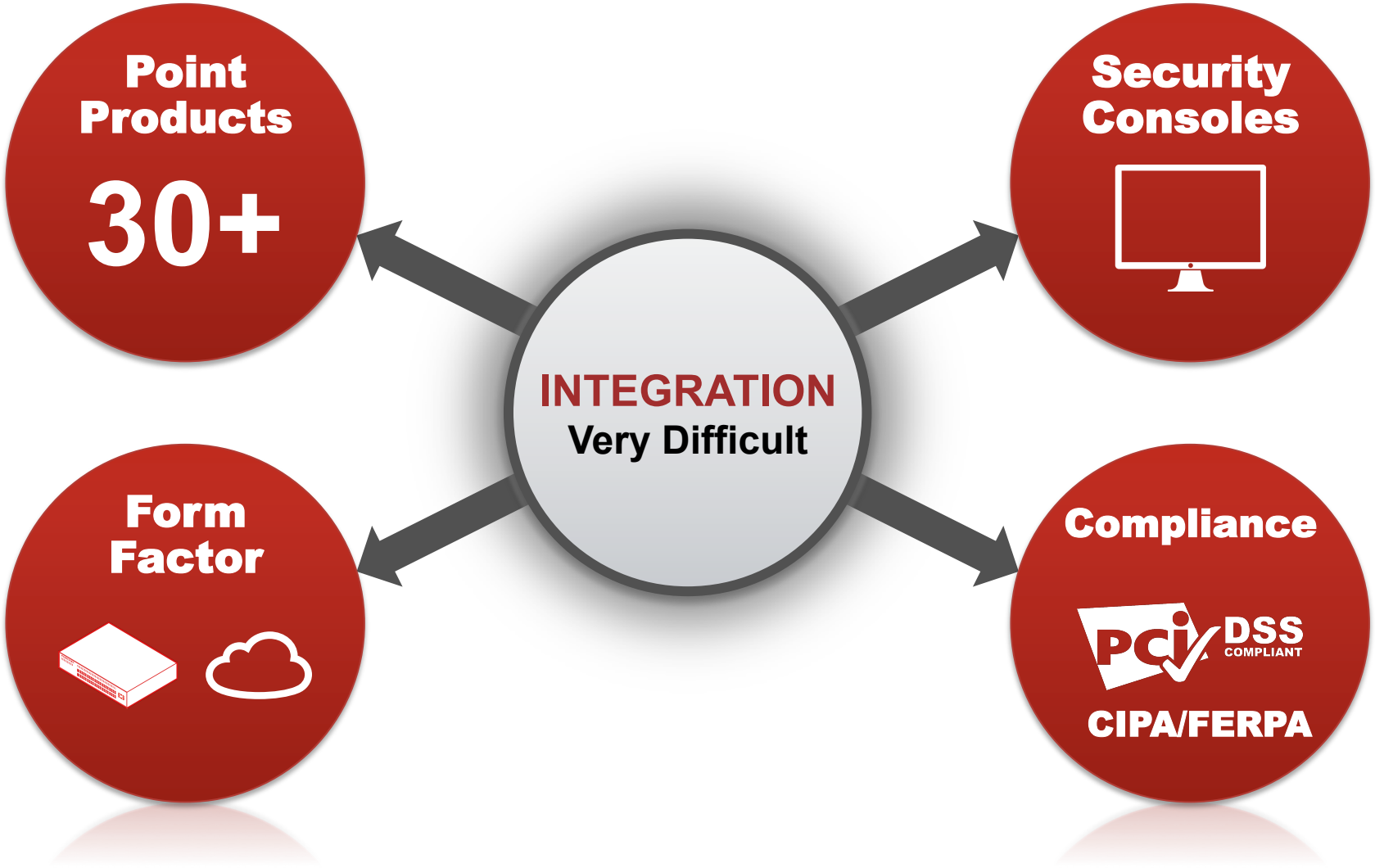
Notes/Sources:

1. Gartner Magic Quadrant for Data Center Networking July 2017
2. Gartner Best Practices in Network Segmentation for Security July 2016
3. Gartner Research Paper "Predicts 2017: Network and Gateway Security"

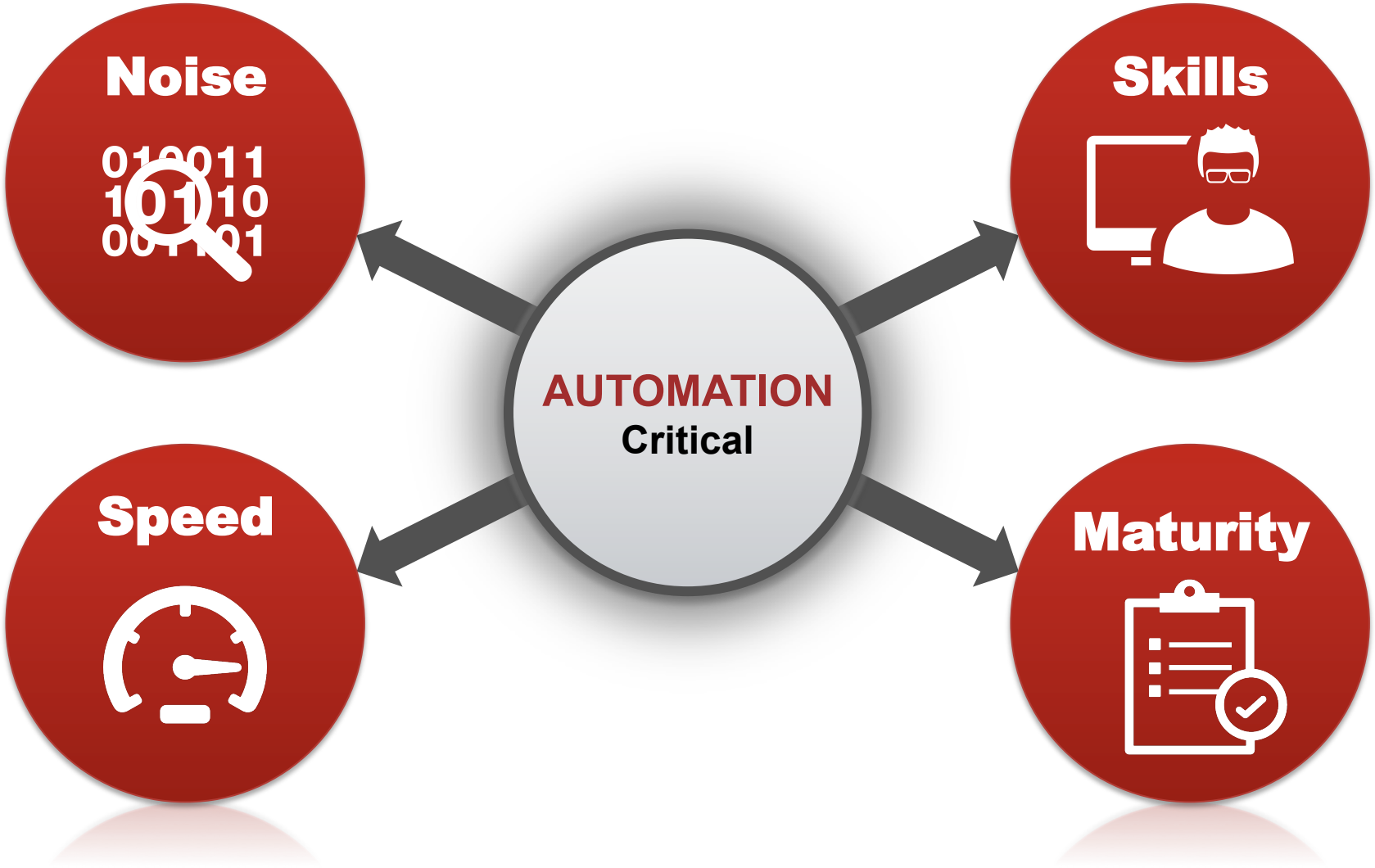
Digital Attack Surface Expanding and Becoming Invisible



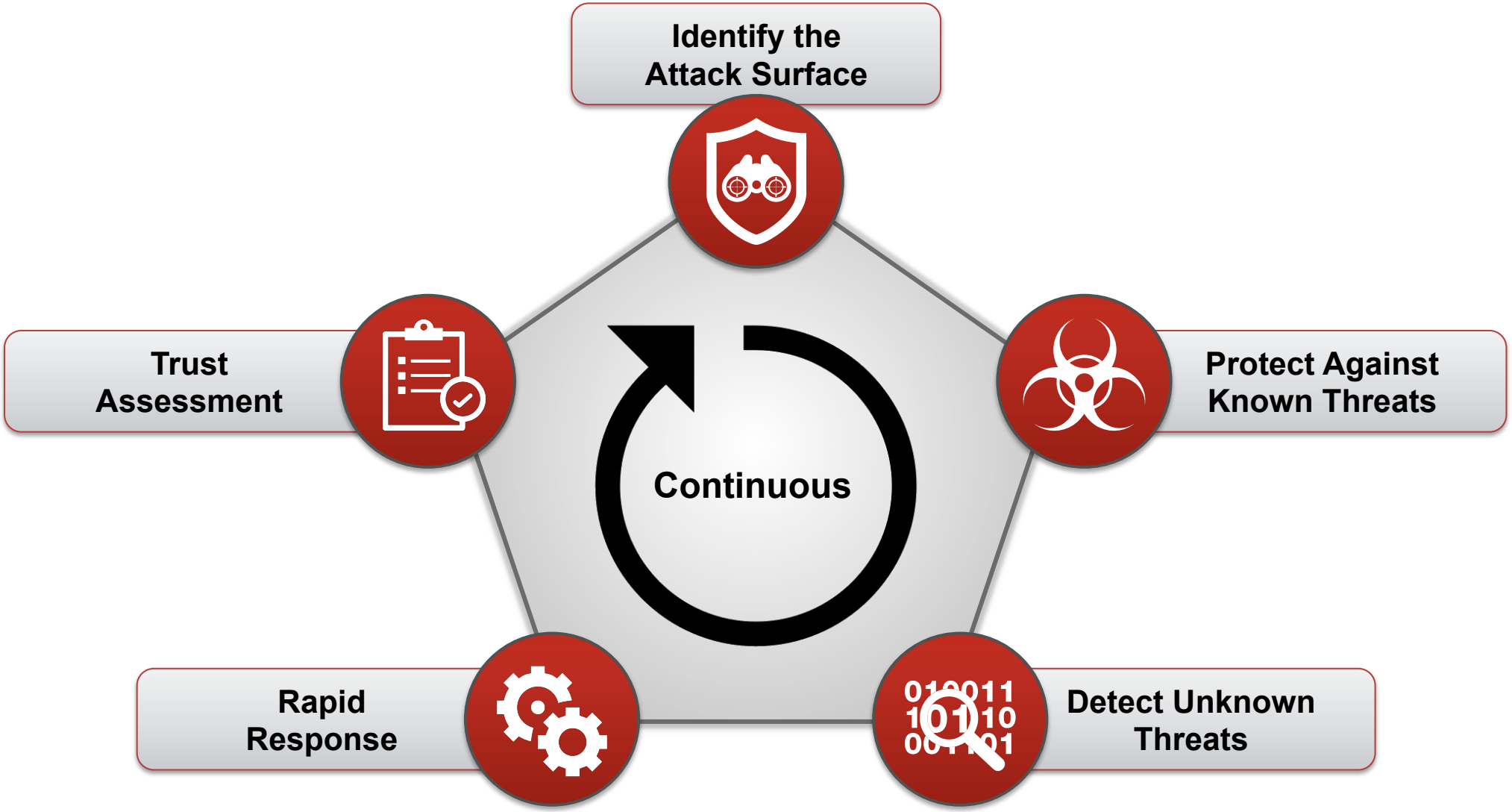
Too Many Point Solutions and New Regulations



Rapidly Changing Advanced Threats and Lack of Resources and Expertise



Security Framework for Digital Security



2018 Fortinet Security Fabric

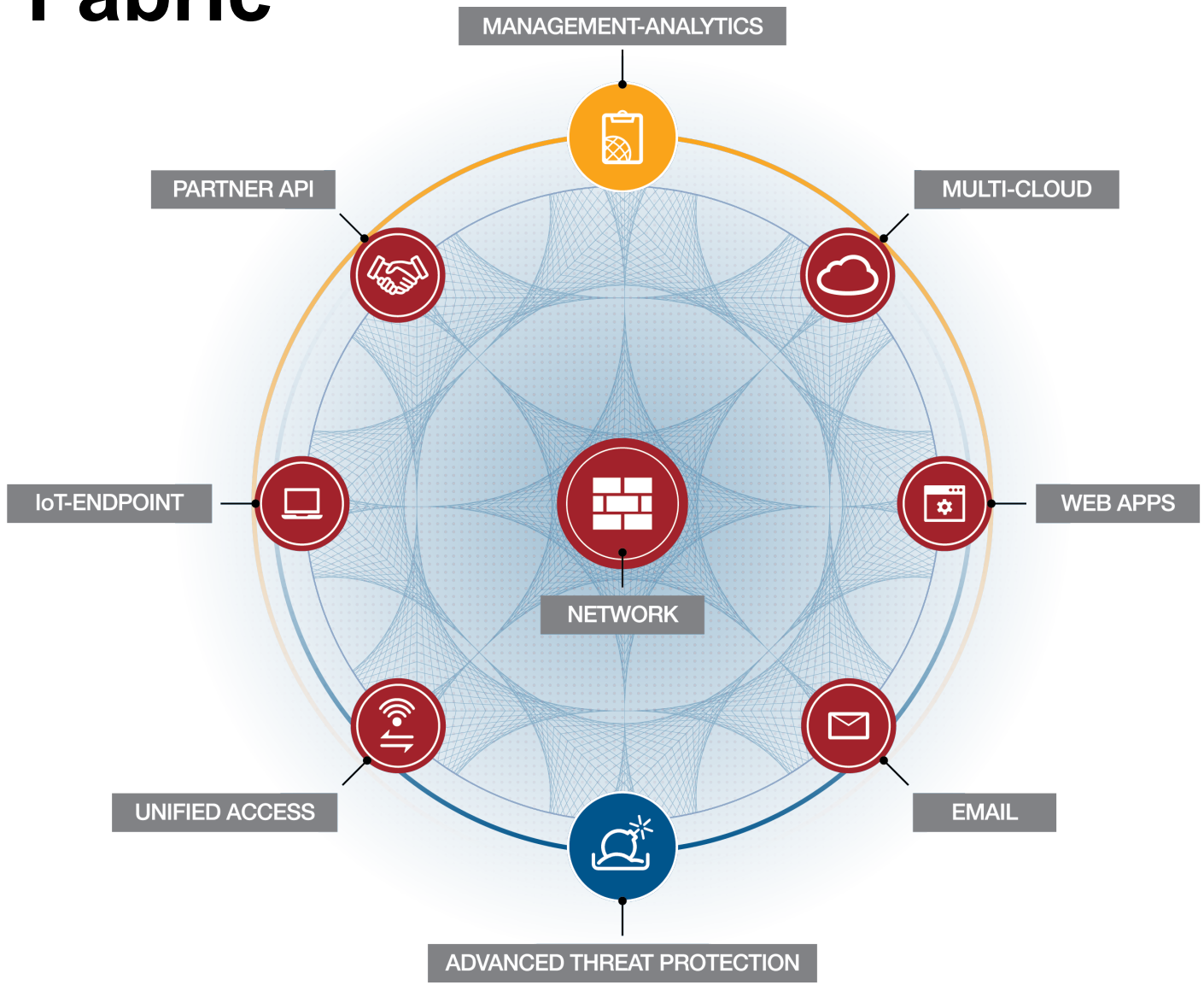
A Security Architecture that provides:

BROAD Visibility & Protection of the Digital Attack Surface

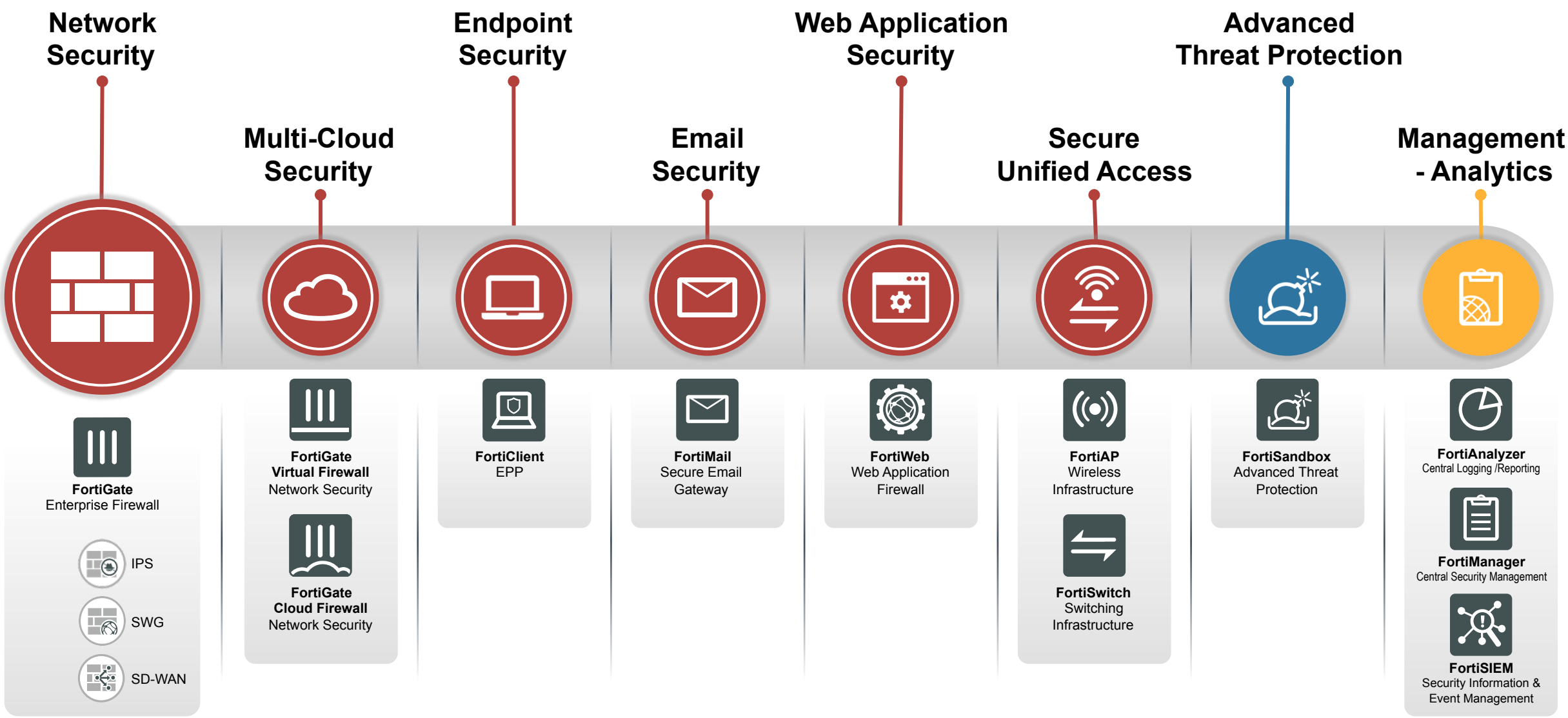
INTEGRATED Detection of Advanced Threats

AUTOMATED Response & Continuous Trust Assessment

Delivered as:



2018 Fortinet Solutions



Fabric Alliance Ecosystem

Partner
API

Cloud

- amazon web services
- Microsoft Azure
- ORACLE
- IBM Security
- HPE Helion

SDN

- CISCO
- nuagenetworks
- ADVA Optical Networking
- BROCADE
- openstack
- CLOUDIFY

Endpoint

- Symantec
- McAfee Together is power.
- SentinelOne
- Attivo NETWORKS
- CARBON BLACK ARM YOUR ENDPOINTS
- ziften

Management

- tufin
- algosec
- FIREMON
- servicenow

Vulnerability/SIEM

- WhiteHat SECURITY
- QUALYS Continuous Security
- Hewlett Packard Enterprise

IoT/OT/NAC

- NOZOMI NETWORKS
- ForeScout
- BRADFORD NETWORKS
- Pulse Secure

Identity

- Centrify
- CYBERARK

Technology

- intel
- VERISIGN
- ribbon communications

Third-Party Certifications

Product	2017
Firewall	Tested*
NGFW	Recommended
Data Center Security Gateway	Recommended
NGIPS	Recommended
Breach Detection	Recommended
Breach Prevention	Recommended
Web Application Firewall	Recommended
Adv. Endpoint Protection	Recommended

**NSS Labs Data Center Firewall test, April 2017. No SVM/recommendations published*

As of January, 2018

Core Fabric Technologies

FORTIOS

OS

FABRIC

USE CASES

CONNECTORS

API

AUTOMATION

FABRIC AGENT

CASB

ORCHESTRATION

FORTIGUARD

Security Rating

Threat Intelligence

Web Filtering

FortiSandbox Cloud

Intrusion Prevention

Antivirus

Application Control

IP Reputation

PARALLEL PROCESSING

SPU

NP6

CPU

CP9

Accelerates Network Traffic

Flexible Policy

Accelerates Content Inspection

SoC3

Optimized for entry-level form factors

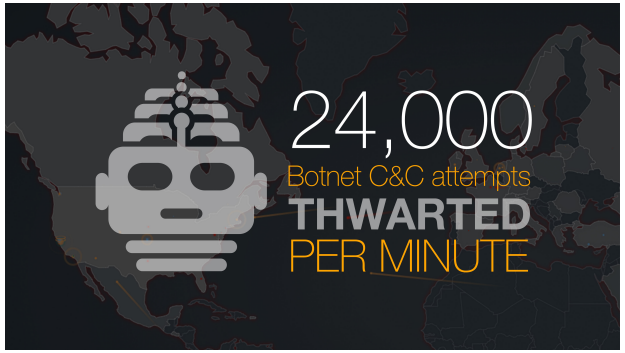
More Performance

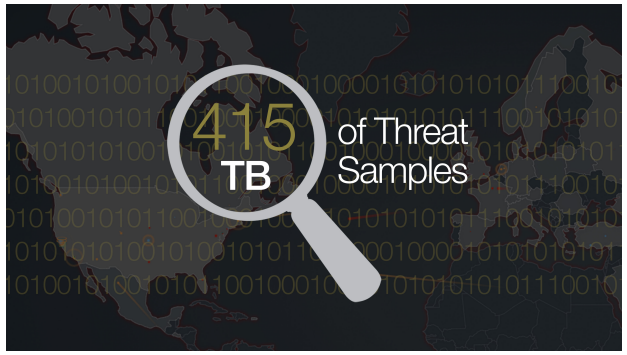
Less Latency

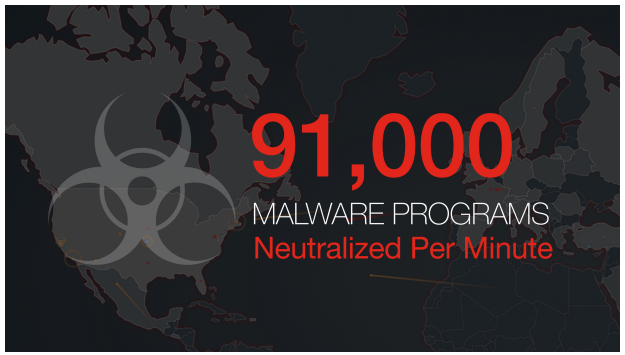
Less Power

Less Space

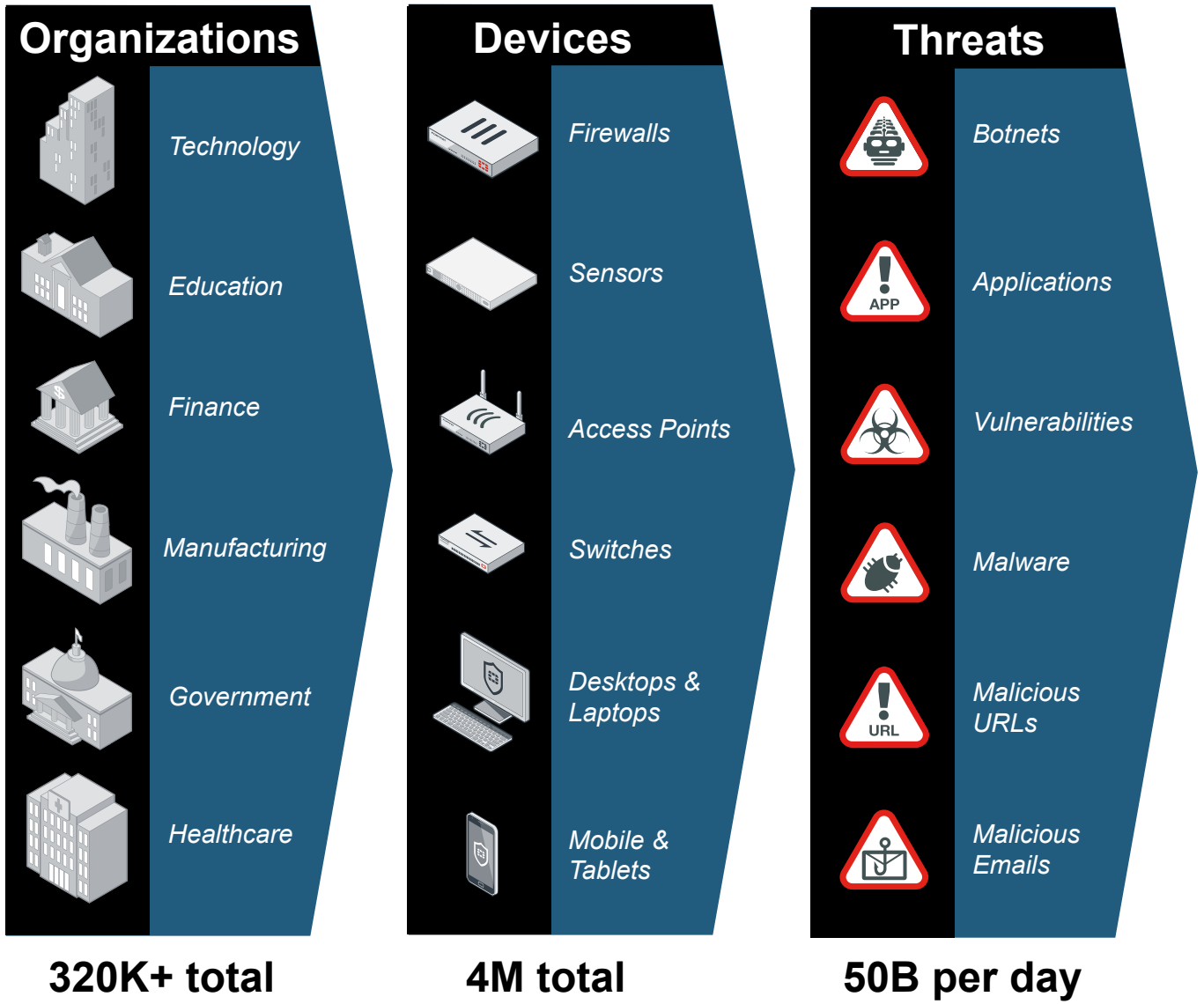
FortiGuard: By the Numbers

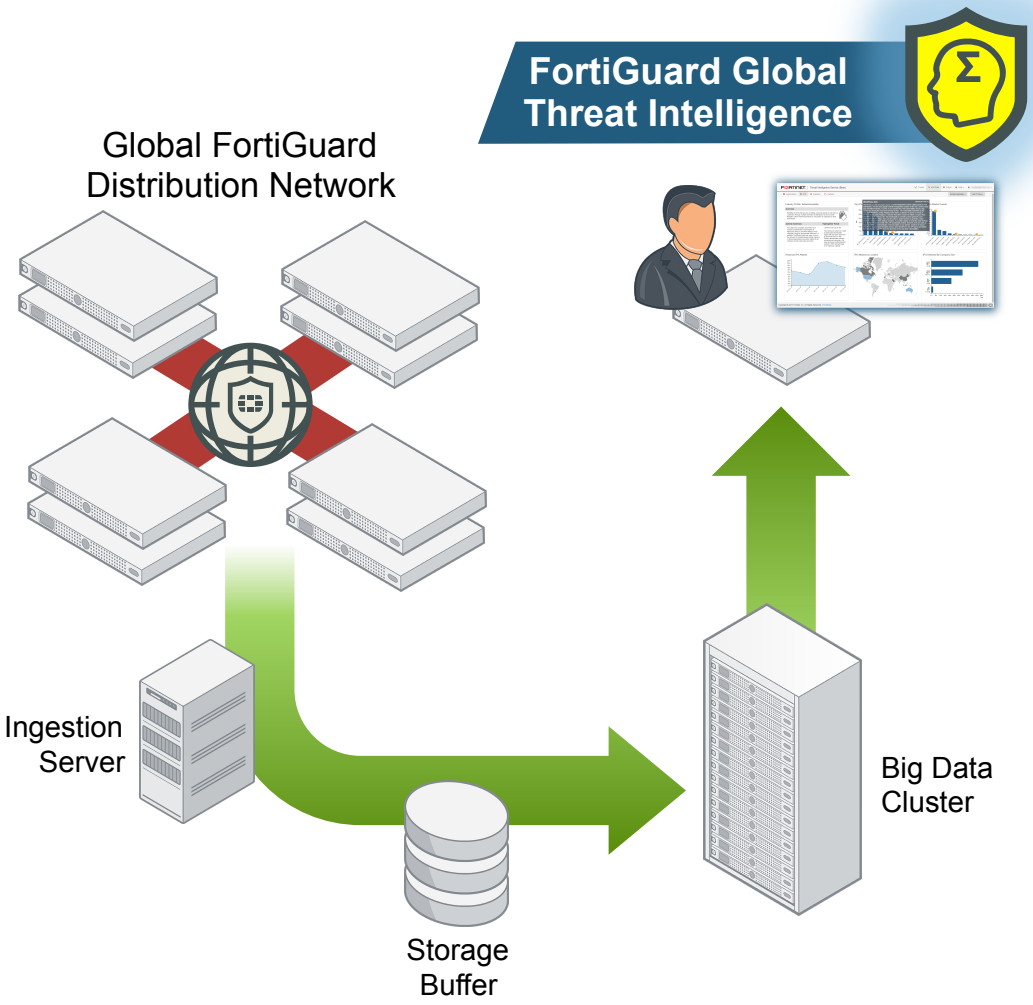






FortiGuard Global Threat Intelligence





SECURED BY FORTIGUARD®

Cloud/SDN

Private Hybrid Public

Scalable

CFW NGFW DEFW VFW ISFW DCFW

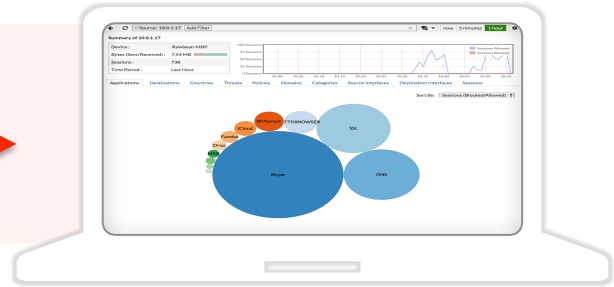
Application Security

Endpoint Protection

API

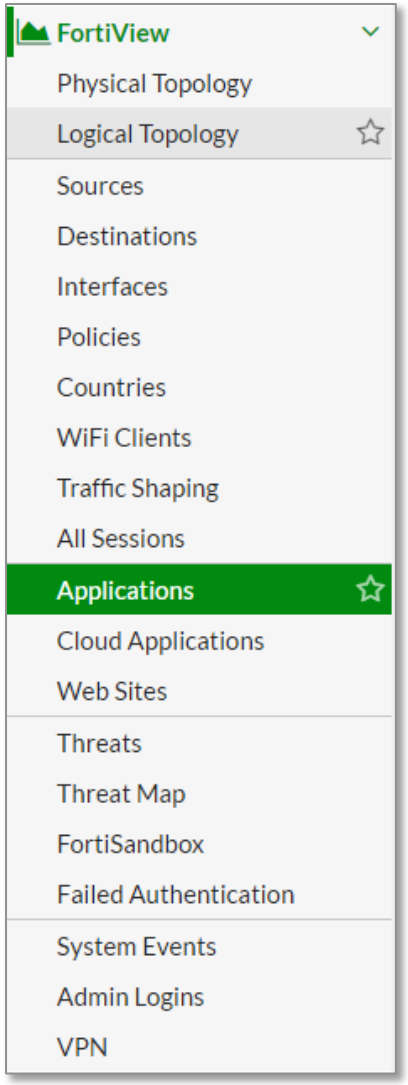
Secure Access Layer

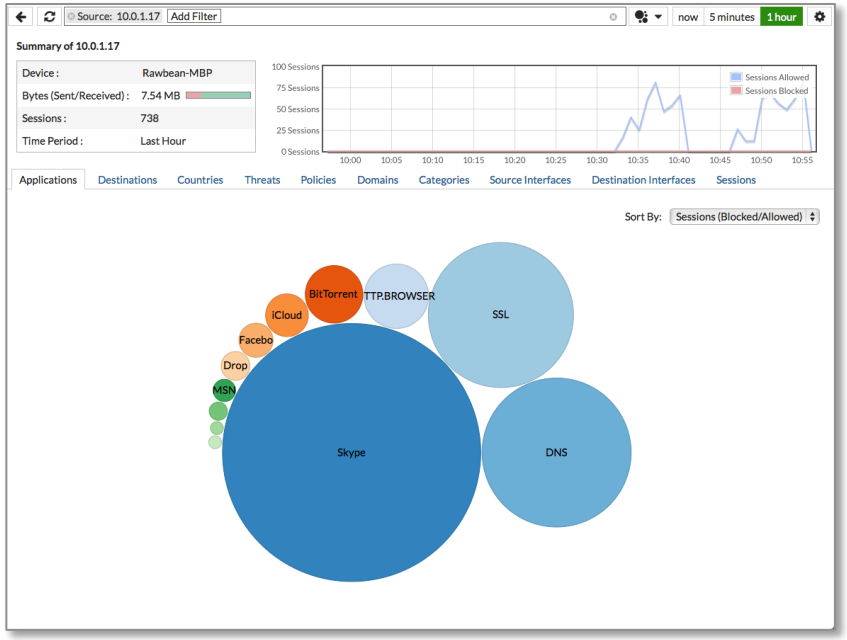
Advanced Threat Protection

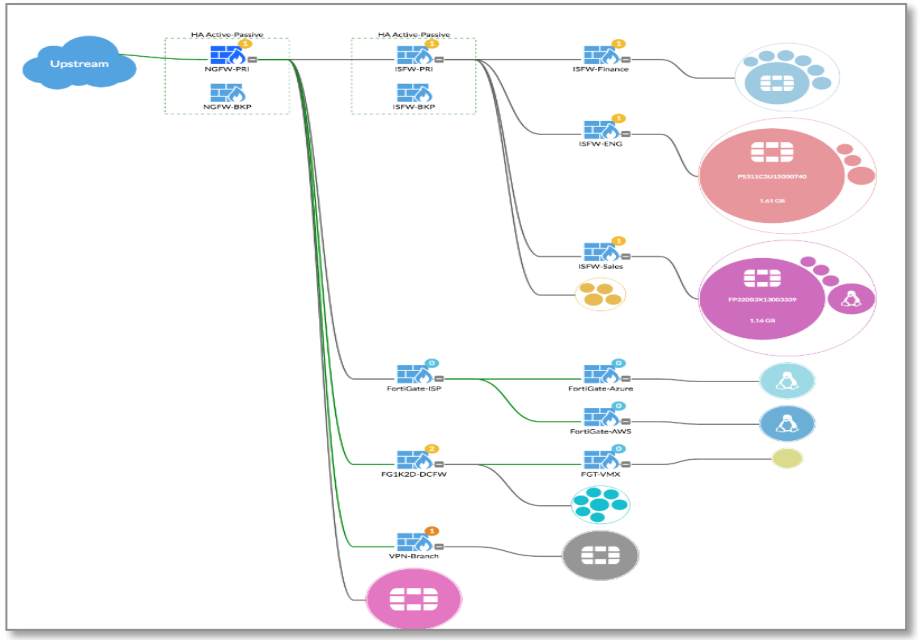


Single Pane of Glass Management & Analytics

Deep Visibility and Fabric View







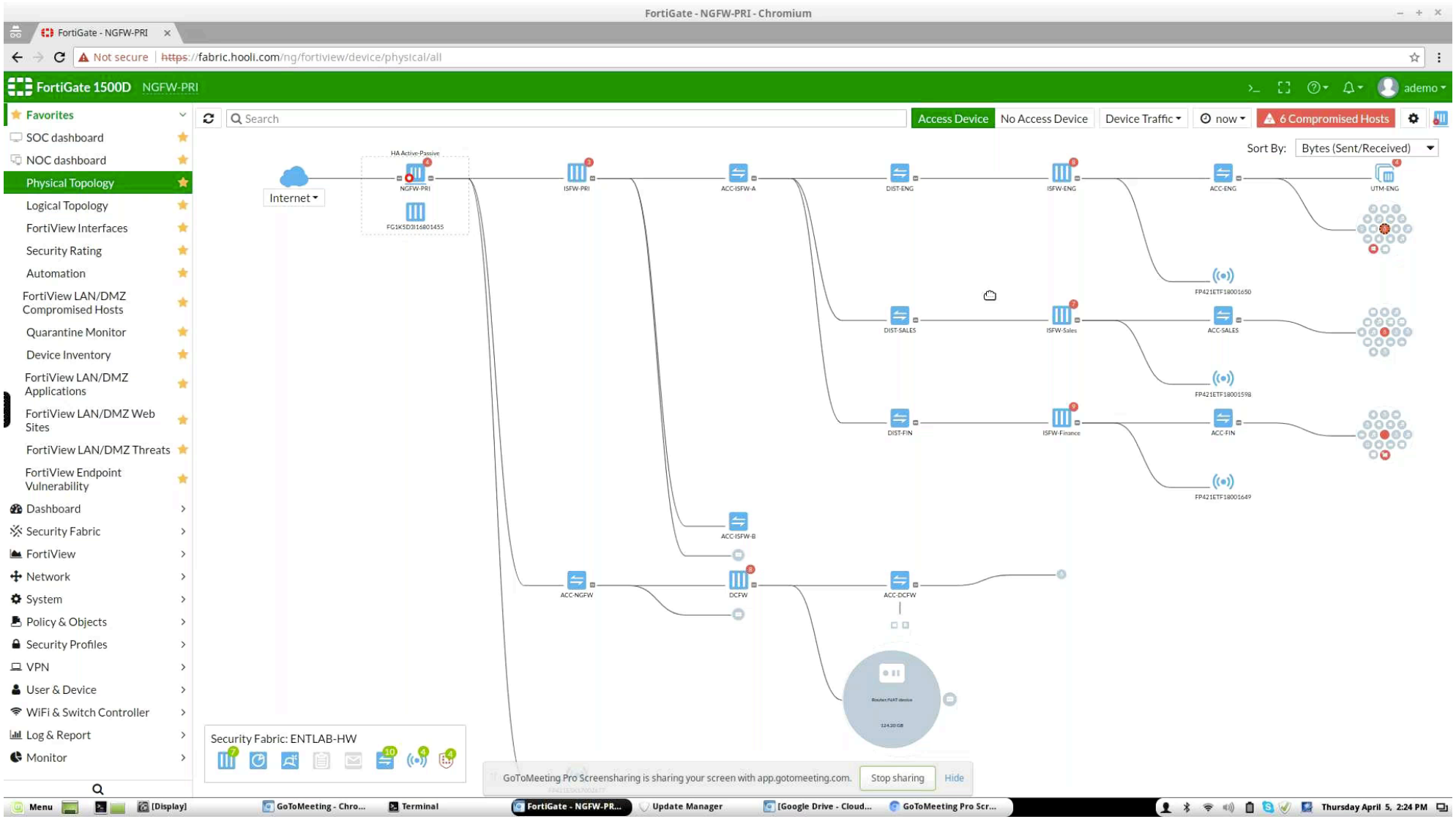
FortiView

- Top Applications and Threats
- Local Threat Map
- One Click Actions

Security Fabric View

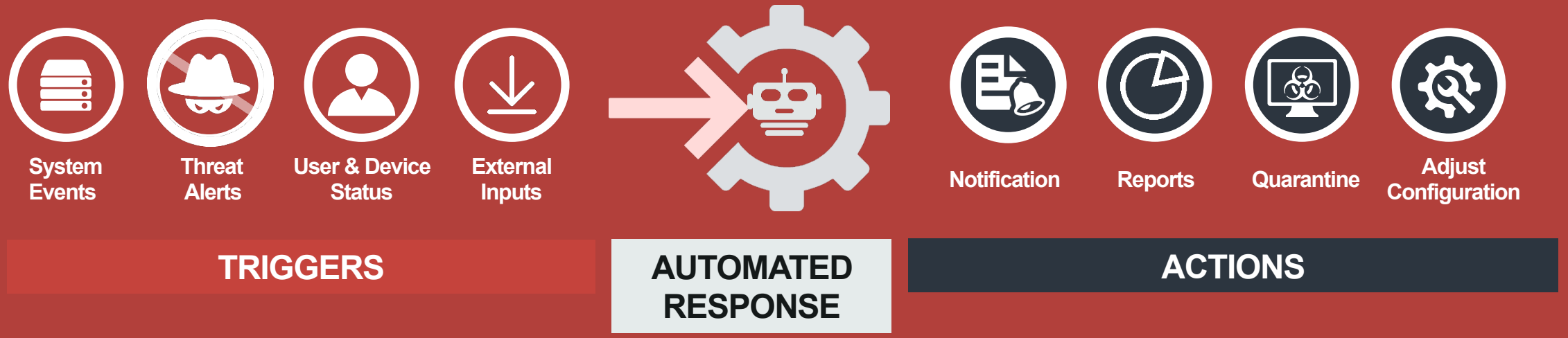
- Physical Topology
- Logical Topology
- Audit recommendation

End to End Visibility & Control



WorkFlow Automation

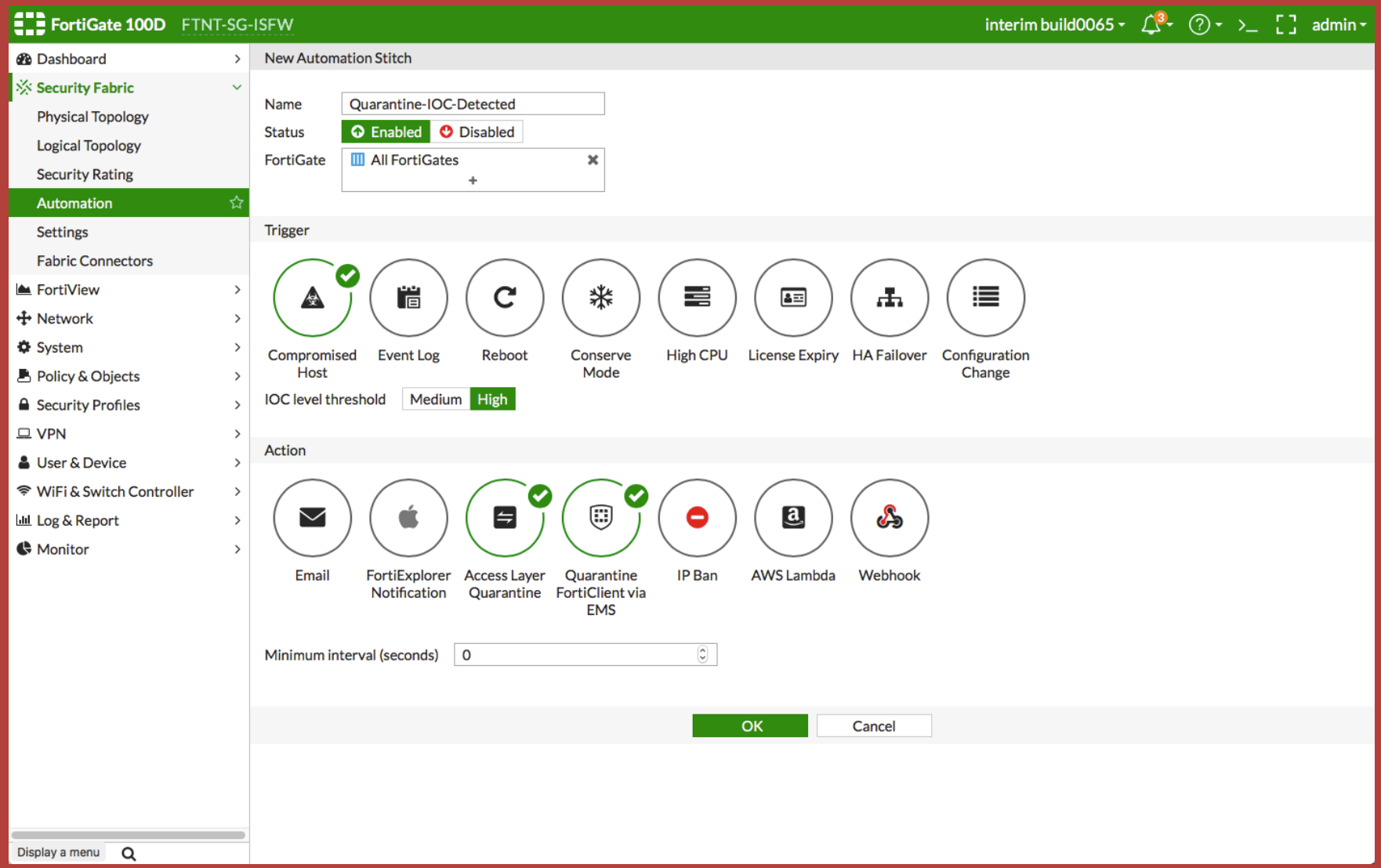
Automation



- Automated workflows (stitches) using triggers to deliver appropriate actions
  - » Easy creation using wizards
  - » Covers components within a security fabric

Automated Workflow

Automation



Audit for Compliance Best Practices

Visual Audit Indicator

Severity Level

- Critical
- High
- Medium
- Low
- Passed

Run Fabric Audit
(Priority-based)

Priority	Element	Severity	No.
1.	ISFW.2	Critical	
2.	ISFW.1	High	
3.	NGFW.1	Low	
4.	AWSFW.1	Low	

Apply Recommendations

- Common Compliance Areas
  - ✓ Secure the network
  - ✓ Secure the endpoints
  - ✓ Control access
  - ✓ Log and monitor activity
  - ✓ Enforce policy

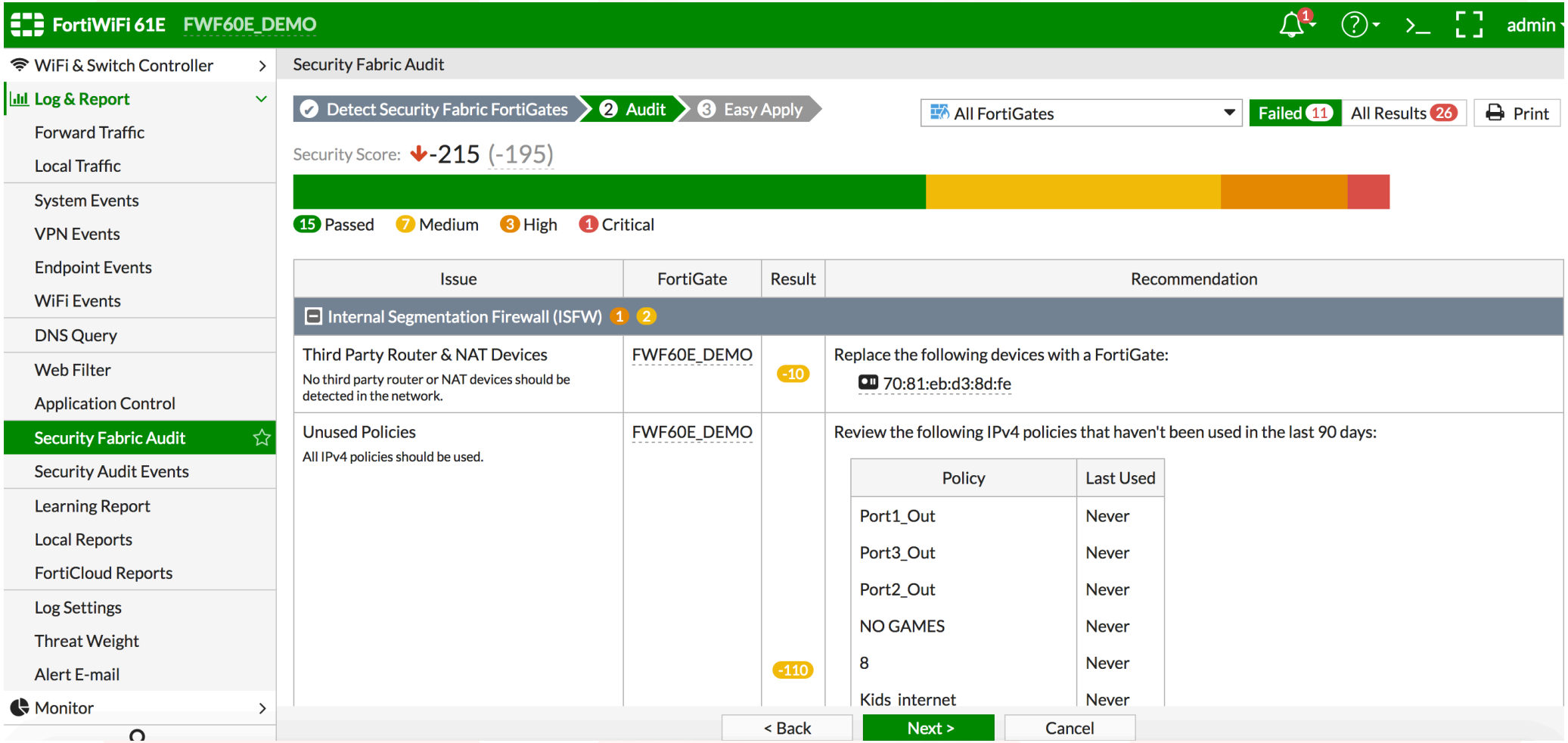
PCI · European Commission · NIST National Institute of Standards and Technology U.S. Department of Commerce · ISO ISO 27002

- Security Best Practices
  - ✓ Strong administrative access
  - ✓ Current firmware & subscriptions

Audit Support

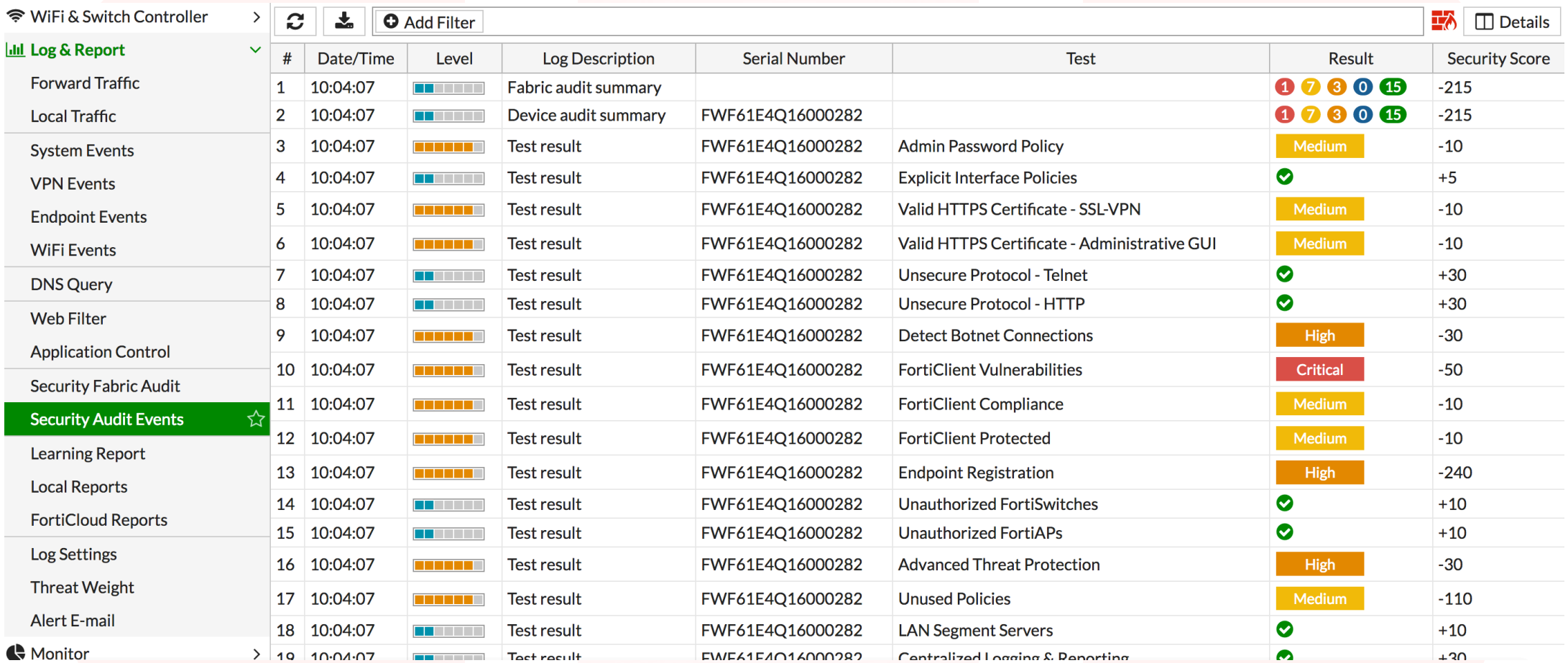
FORTINET SECURITY FABRIC

SECURED BY FORTIGUARD®



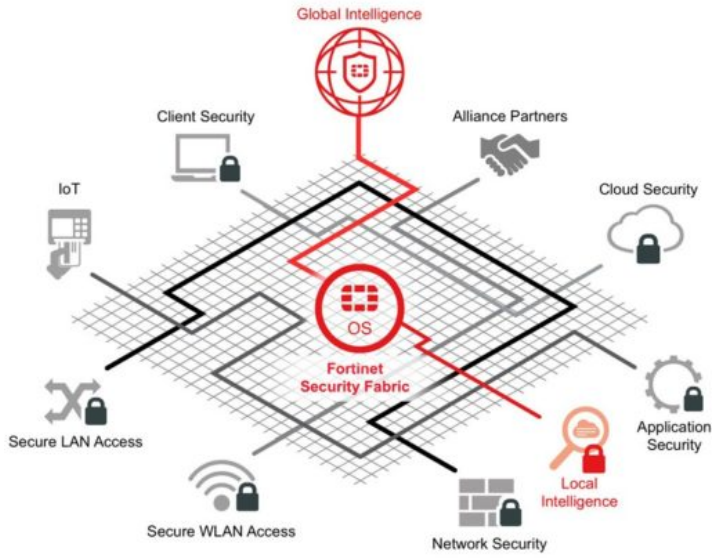
Audit Support

SECURED BY FORTIGUARD®



#	Date/Time	Level	Log Description	Serial Number	Test	Result	Security Score
1	10:04:07		Fabric audit summary			1 7 3 0 15	-215
2	10:04:07		Device audit summary	FWF61E4Q16000282		1 7 3 0 15	-215
3	10:04:07		Test result	FWF61E4Q16000282	Admin Password Policy	Medium	-10
4	10:04:07		Test result	FWF61E4Q16000282	Explicit Interface Policies	✓	+5
5	10:04:07		Test result	FWF61E4Q16000282	Valid HTTPS Certificate - SSL-VPN	Medium	-10
6	10:04:07		Test result	FWF61E4Q16000282	Valid HTTPS Certificate - Administrative GUI	Medium	-10
7	10:04:07		Test result	FWF61E4Q16000282	Unsecure Protocol - Telnet	✓	+30
8	10:04:07		Test result	FWF61E4Q16000282	Unsecure Protocol - HTTP	✓	+30
9	10:04:07		Test result	FWF61E4Q16000282	Detect Botnet Connections	High	-30
10	10:04:07		Test result	FWF61E4Q16000282	FortiClient Vulnerabilities	Critical	-50
11	10:04:07		Test result	FWF61E4Q16000282	FortiClient Compliance	Medium	-10
12	10:04:07		Test result	FWF61E4Q16000282	FortiClient Protected	Medium	-10
13	10:04:07		Test result	FWF61E4Q16000282	Endpoint Registration	High	-240
14	10:04:07		Test result	FWF61E4Q16000282	Unauthorized FortiSwitches	✓	+10
15	10:04:07		Test result	FWF61E4Q16000282	Unauthorized FortiAPs	✓	+10
16	10:04:07		Test result	FWF61E4Q16000282	Advanced Threat Protection	High	-30
17	10:04:07		Test result	FWF61E4Q16000282	Unused Policies	Medium	-110
18	10:04:07		Test result	FWF61E4Q16000282	LAN Segment Servers	✓	+10
19	10:04:07		Test result	FWF61E4Q16000282	Centralized Logging & Reporting	✓	+30

What is the Fabric?



Application: From IoT to Cloud broad coverage of the attack surface.

Instrumentation: Cost reduction in identifying risk across the infrastructure.

Automation: Reduction in exposure from breach detection to remediation.


FORTINET®