31-03-22

FORTINET®

NLcom – Ontbijt Seminar

Roel Raaijmakers – Consultant

Programma

- Gartner CyberSecurty Mesh Architecture vs Fortinet Security Fabric
- Fortigate designed with Security Processing Unit (SPU)
- Fortinet Secure Driven Networking
- FortiGuard labs
- FortiClient ZTNA
- FortiAnalyzer as a SOC

© Fortinet Inc. All Rights Reserved.

Gartner CyberSecurty Mesh Architecture vs Fortinet Security Fabric

WHO IS FORTINET?

Fortinet is a global leader in cybersecurity, delivering a broad, integrated and automated security fabric to enable customers to accelerate their digital journey.

$3.09B
FY2020 Billing
Financially Stable

38.9B+ Market Cap (as of 7.31.21)
Nasdaq: FTNT
S&P 500

BBB+ Baa1
Security Investment Grade Rating
Leading the Cybersecurity Industry

50
Integrated Fabric Products
Broadest Attack Surface Coverage

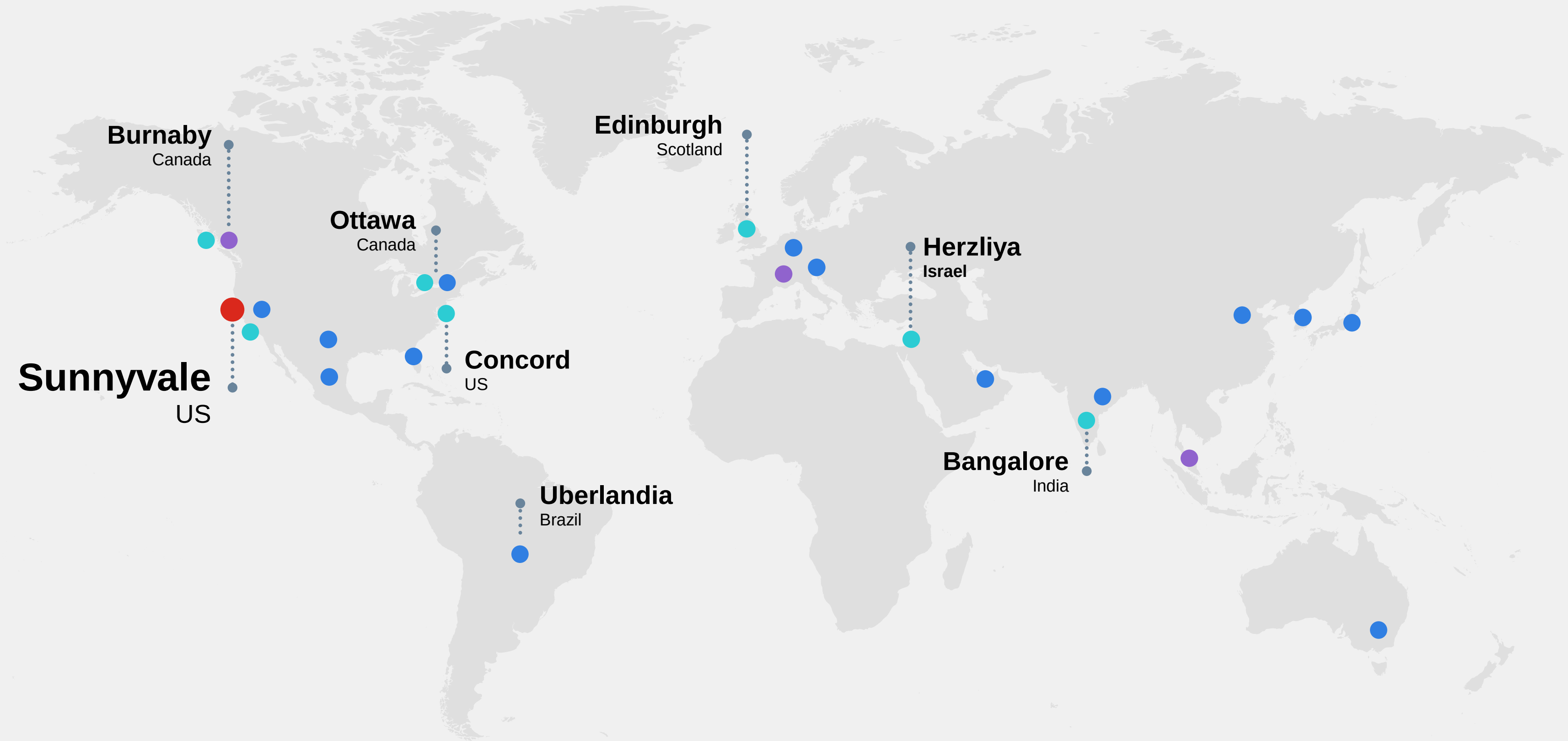
530,000+
Customers Worldwide
Massive Customer Input

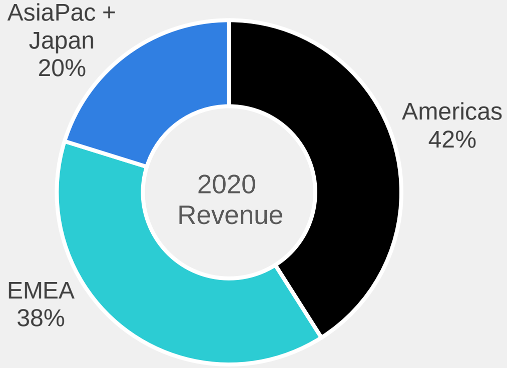
660,000+
NSE Certifications
WEF Cybersecurity Founders

© Fortinet Inc. All Rights Reserved.

Broad Global Footprint—Balanced Global Growth

Huge R&D investment to support organic growth





● Headquarters

● Dev Centers

FortiCare

● Support Centers

● Centers of Excellence

9,000+ employees

530,000+ customers worldwide

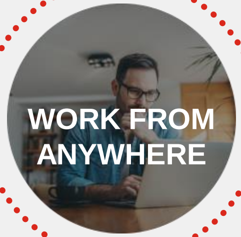
785 registered patents

© Fortinet Inc. All Rights Reserved.

Industry Landscape and Customer Challenges

Digital Innovation Impacts Every Business

Many business-critical trends are driving organizations to accelerate digital innovation to transform key growth areas of their business. However, these vital efforts also exponentially grow the organization's digital attack surface and increase cyber risk.


WORK FROM ANYWHERE

Massive increase in remote worker access

EDGE/CLOUD COMPUTING

Applications migrate to more compute platforms

IoT/OT

Proliferation of vulnerable, network enabled devices

COMPLIANCE

Growing data privacy and regulatory concerns, board level reporting

5G/LTE

New, more sophisticated business applications

EDGE EXPLOSION

More edges appearing across the network

THREAT LANDSCAPE

Zero day, supply chain, state sponsored, weaponized

DIGITAL EXPERIENCE

End-to-end performance becoming a critical differentiator

© Fortinet Inc. All Rights Reserved.

Digital Innovation is Also Causing Increased Risk

Cyber threats take advantage of the disruption

Sophisticated Threats	Breach and ransomware incidents continue to increase
Digital Attack Surface	As the perimeter expands, billions of “Security Edges” are formed
Ecosystem Complexity	Too many vendors and too many alerts, **not** enough skilled people
Compliance	Global, country, province, industry, and government regulation

© Fortinet Inc. All Rights Reserved.

Fortinet is recognized in 6 Gartner Magic Quadrants

Fortinet recognized as a Leader in **2** Magic Quadrants	Network Firewalls	WAN Edge Infrastructure
Fortinet recognized as a Visionary in **2** Magic Quadrants	Wired and WLAN	SIEM
Fortinet recognized as a Challenger or Niche in **2** Magic Quadrants	Web Application Firewall	Endpoint Protection Platforms*
Fortinet mentioned in **2** Magic Quadrants	Secure Web Gateway	Indoor Location Services

And Fortinet is listed in **8** Gartner Market Guides

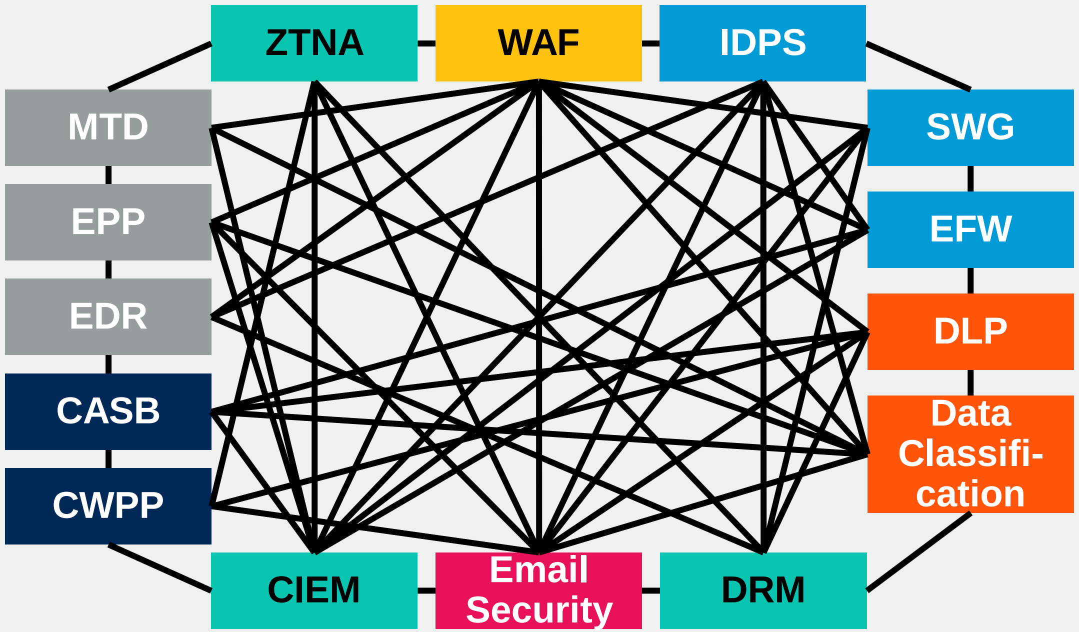
EDR	IDPS	Email	NAC
NDR	ZTNA	OT	SOAR

Gartner®

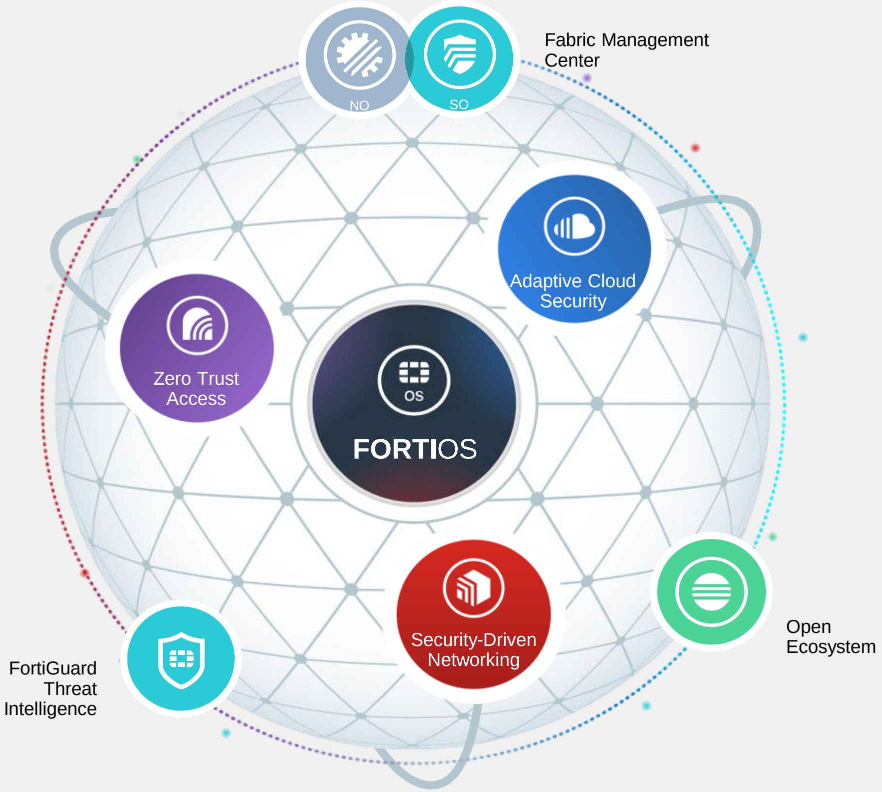
© Fortinet Inc. All Rights Reserved.

Gartner Cybersecurity Mesh Architecture

Gartner®



FERTINET®



Executive Guide to Cybersecurity Mesh, 2022

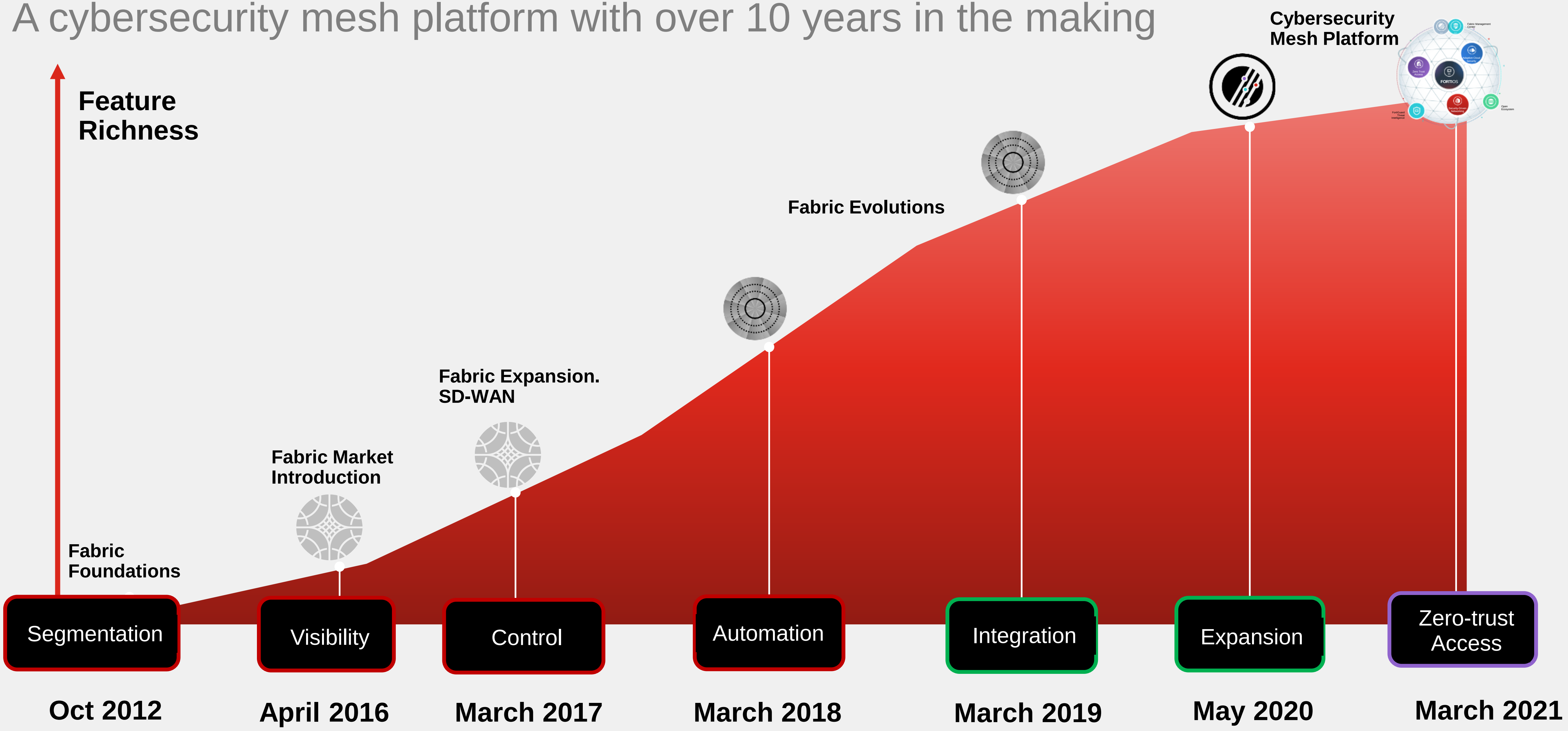
Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Evolution of the Fortinet Security Fabric

A cybersecurity mesh platform with over 10 years in the making



© Fortinet Inc. All Rights Reserved.

Fortinet Security Fabric

Broad

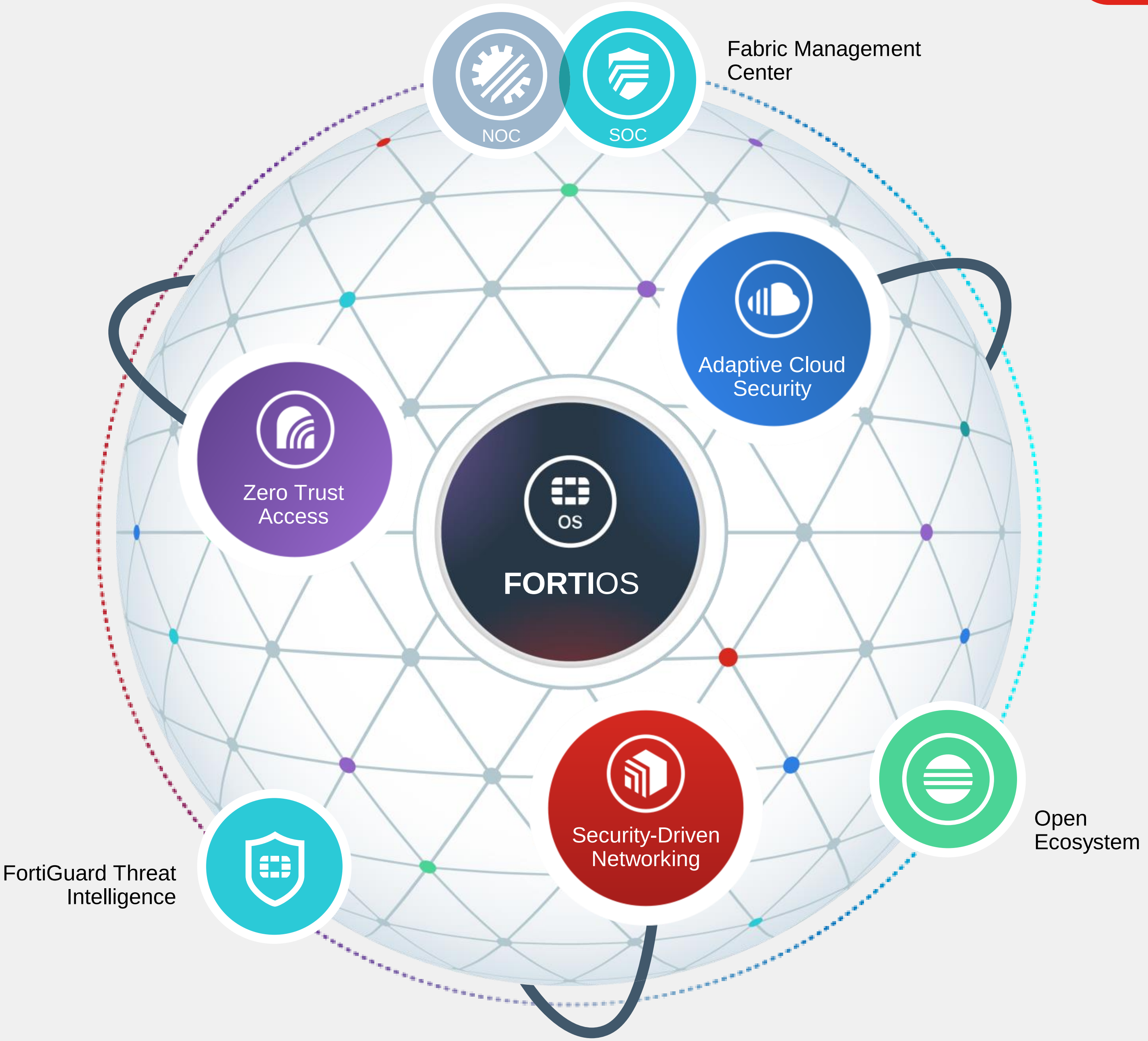
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations



© Fortinet Inc. All Rights Reserved.

Pillars of your security posture

Cybersecurity Platform Across Endpoint, Network and Cloud

Convergence of Networking and Security at New Network Edges

Security-driven Networking

More users off Network and more Devices IP Enabled (IoT/OT)

Zero Trust Access

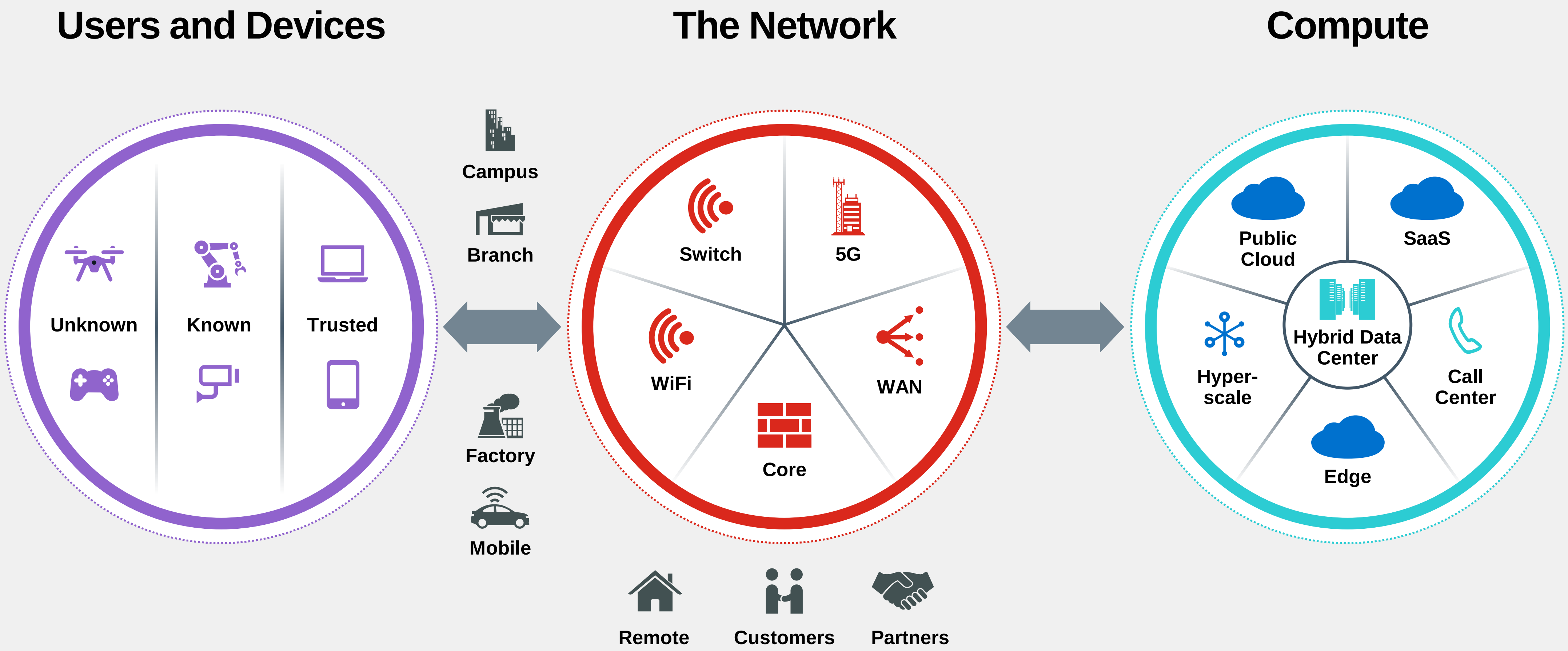
Applications continue to move across different Clouds

Adaptive Cloud Security

© Fortinet Inc. All Rights Reserved.

Billions of “Edges” Expanding the Digital Attack Surface

The perimeter is everywhere



Digital Security, everywhere you need it.

FortiGuard Security Services

SOC & NOC

Content Security

Web Security

Advanced SOC/NOC

User Security

User Security

Device Security

Bundled Security

Fabric Management Center - SOC

Endpoint

FortiEDR

FortiXDR

Breach

FortiSandbox

FortiDeceptor

FortiAI

Incident Response

FortiAnalyzer

FortiSIEM

FortiSOAR

FortiGuard MDR Service

Fabric Management Center - NOC

FortiManager

FortiCloud

FortiMonitor

Open Ecosystem

Connector

Fabric API

DevOps

Extended Fabric Ecosystem

Zero Trust Access

FortiClient

FortiNAC

FortiVoice

FortiToken

FortiAuthenticator

FortiCamera

Security-Driven Networking

LAN Edge

FortiAP

FortiSwitch

WAN Edge

FortiGate SD-WAN

FortiExtender

DC Edge

FortiGate

FortiProxy

Cloud Edge

FortiSASE

FortiIsolator

Adaptive Cloud Security

Network

FortiGate VM

Cloud Networking

FortiDDos

FortiSegment

Platform

FortiCASB

FortiCWP

AWS Native

Azure Native

Applications

FortiWeb

FortiMail

FortiADC

FortiGSLB

Appliance

VM

Hosted

Cloud

Software

Container

© Fortinet Inc. All Rights Reserved.

Platform Integration and Services

Open Ecosystem

450+ Best-in-class integrated solutions for comprehensive protection

Fabric Connectors

Fortinet-developed deep integration automating security operations and policies

aws · aruba (a Hewlett Packard Enterprise company) · cisco · Google Cloud · IBM Cloud · Microsoft Azure · ORACLE · servicenow · Symantec.

Fabric APIs

Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions

ARISTA · ASAVIE · DELL · DRAGOS · EQUINIX · intel · SIEMENS Ingenuity for life · splunk> · TIGERA · tufin

Fabric DevOps

Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration

aws · Google Cloud · HashiCorp · Microsoft Azure · openstack. · ORACLE · RED HAT ANSIBLE Automation · refactr · vmware

Extended Ecosystem

Integrations with threat sharing initiatives and other vendor technologies

CYBER THREAT ALLIANCE · MITRE · STIX · INTERPOL · OT CSA · Firewalls · Switching · Wireless · Endpoint Security

Figures as of March 31, 2021

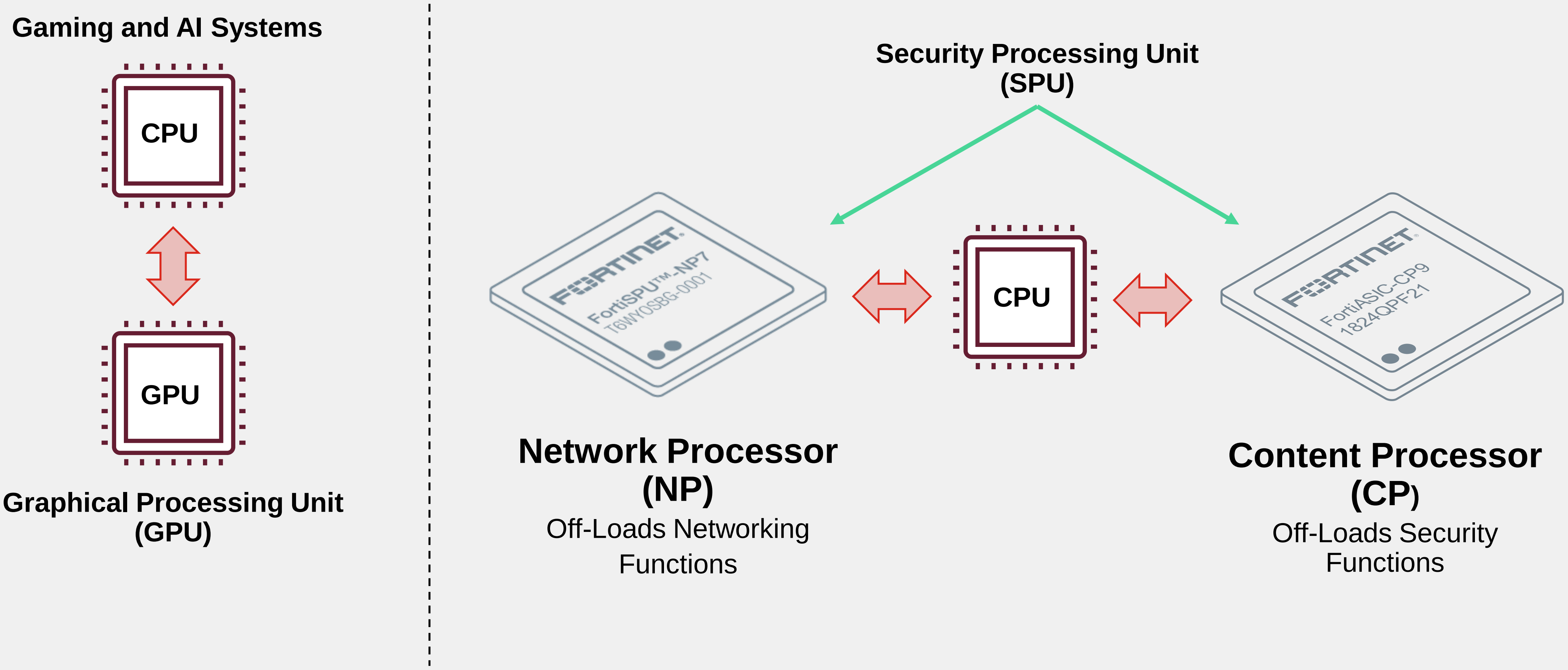
© Fortinet Inc. All Rights Reserved.

Note: Logos are a representative subset of the Security Fabric Ecosystem

FortiGate designed with Security Processing Unit (SPU)

Fortinet Designed Security Processing Unit (SPU)

Industry Leading Hyperscale Security with NP7



Gaming and AI Systems

Graphical Processing Unit (GPU)

Security Processing Unit (SPU)

Network Processor (NP)

Off-Loads Networking Functions

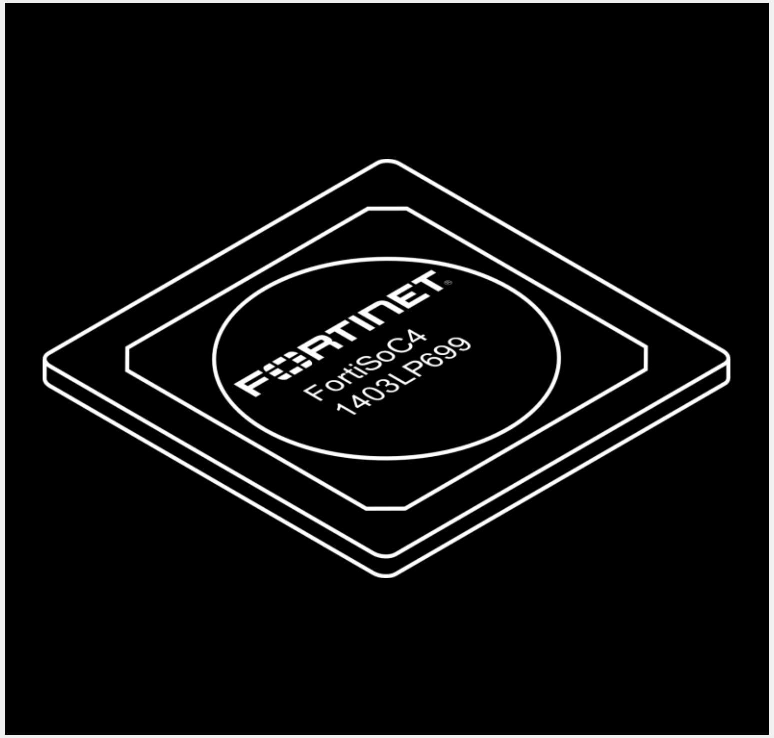
Content Processor (CP)

Off-Loads Security Functions

© Fortinet Inc. All Rights Reserved.

SPU - System on Chip (SoC4)

Powers SD-WAN Branch Performance



NP6 Lite

Firewall – 10 Gbps
Networking – 9 Mpps
IPsec – 3 Gbps

Quad Core CPU

All FortiOS Features

CP9 Lite

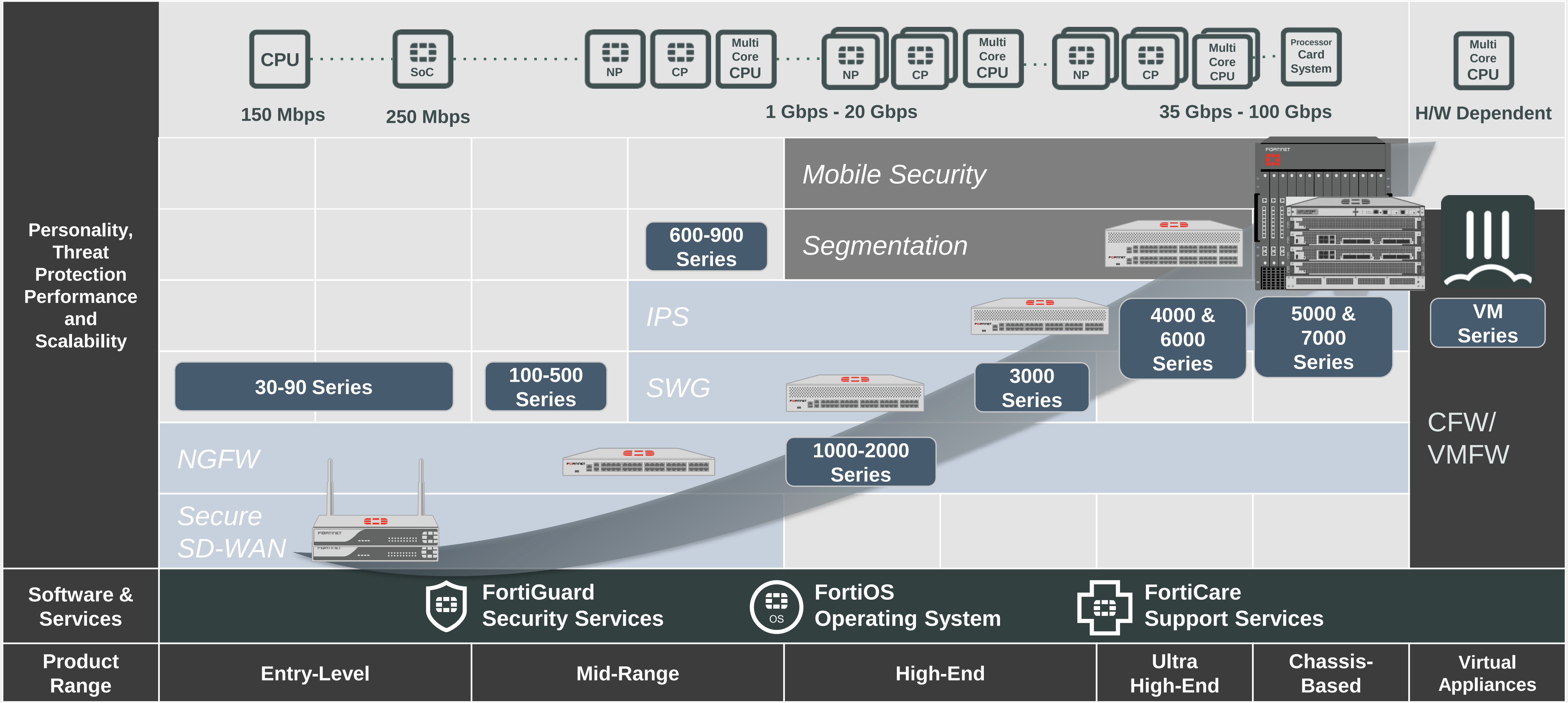
Flow Engine - IPS
Flow Engine - AV
Encryption Engine - SSL

Green

Low cost
Low power

© Fortinet Inc. All Rights Reserved.

FortiGate Product Range



CPU · SoC · NP CP Multi Core CPU · NP CP Multi Core CPU · NP CP Multi Core CPU Processor Card System · Multi Core CPU

150 Mbps · 250 Mbps · 1 Gbps - 20 Gbps · 35 Gbps - 100 Gbps · H/W Dependent

Personality, Threat Protection Performance and Scalability

Mobile Security

Segmentation

IPS

SWG

NGFW

Secure SD-WAN

30-90 Series

100-500 Series

600-900 Series

1000-2000 Series

3000 Series

4000 & 6000 Series

5000 & 7000 Series

VM Series

CFW/ VMFW

Software & Services: FortiGuard Security Services · FortiOS Operating System · FortiCare Support Services

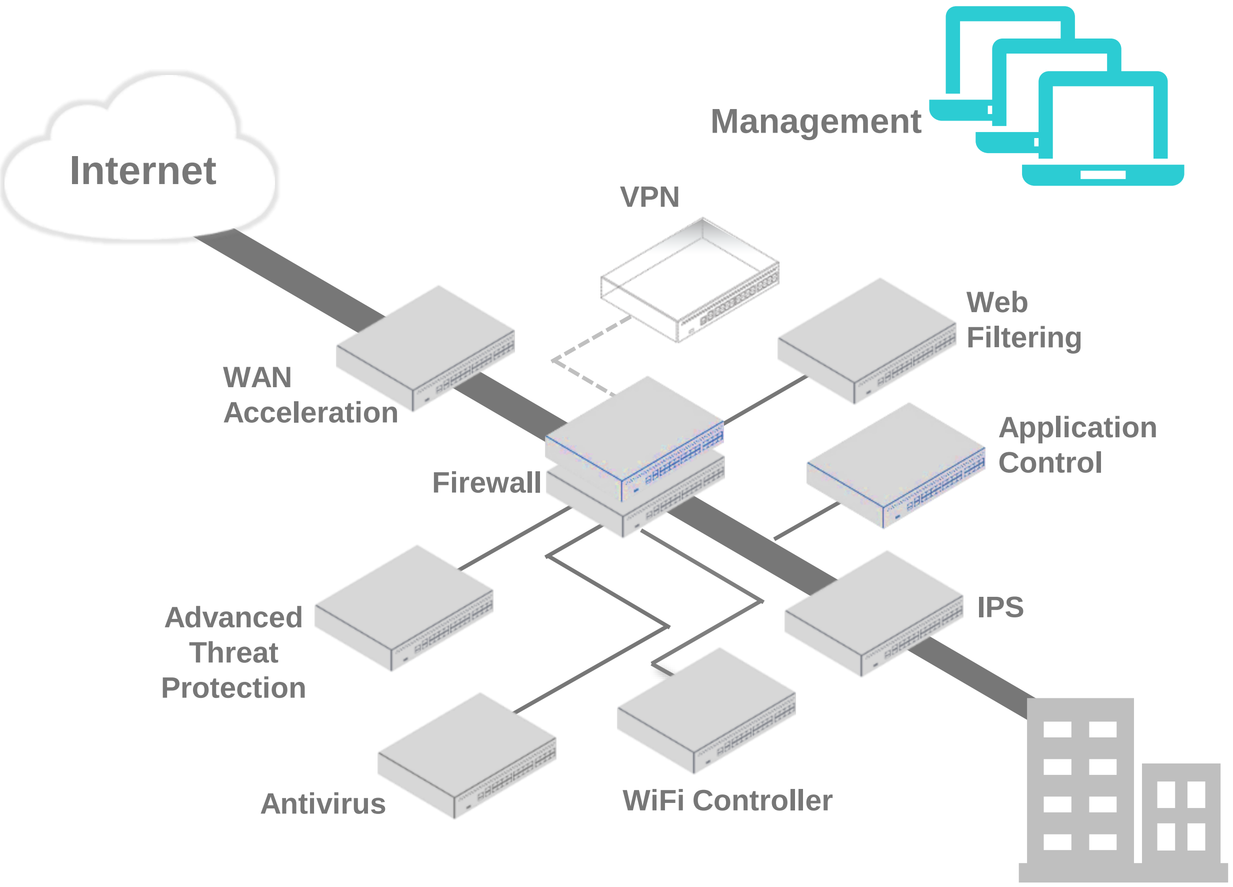
Product Range: Entry-Level · Mid-Range · High-End · Ultra High-End · Chassis-Based · Virtual Appliances

© Fortinet Inc. All Rights Reserved.

Security Driven Networking

FortiGate NGFW - Powerful Multi-Layered Protection

Point Solution Security



Internet

Management

VPN

Web Filtering

WAN Acceleration

Application Control

Firewall

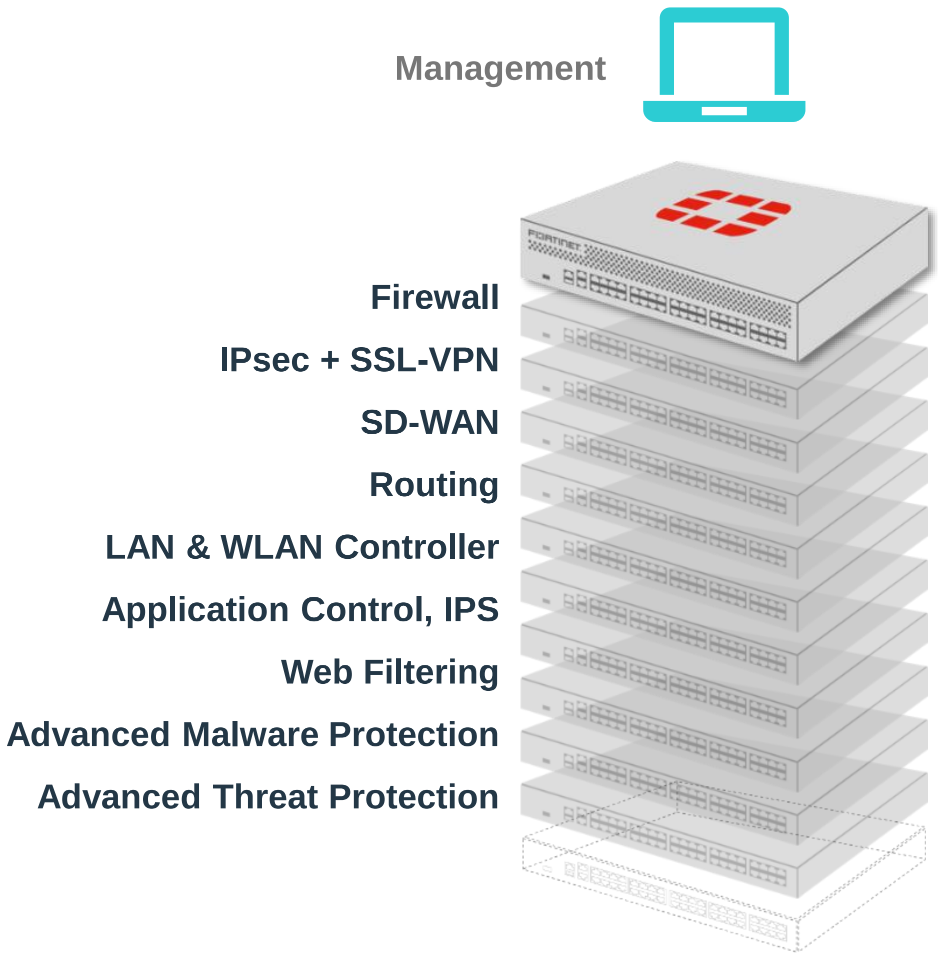
IPS

Advanced Threat Protection

Antivirus

WiFi Controller

Integrated Security



Management

Firewall

IPsec + SSL-VPN

SD-WAN

Routing

LAN & WLAN Controller

Application Control, IPS

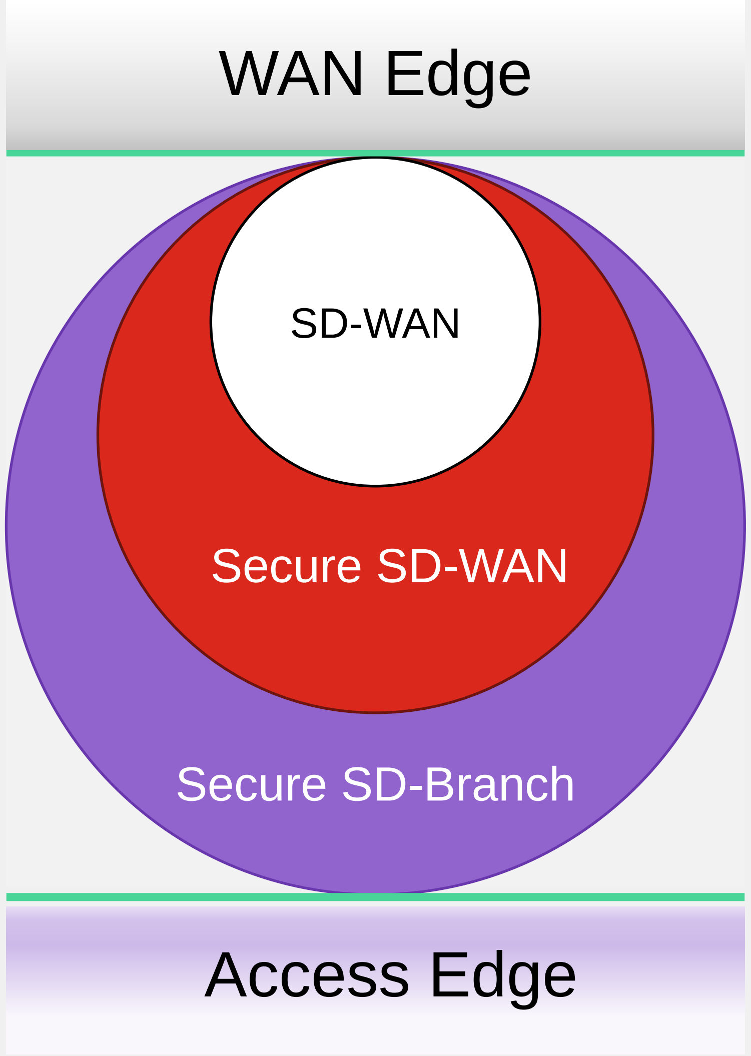
Web Filtering

Advanced Malware Protection

Advanced Threat Protection

© Fortinet Inc. All Rights Reserved.

Evolution of the WAN Edge at the Remote Branch



- **SD-WAN**

  Offers cost savings and improvements in application performance but lack security

- **Secure SD-WAN**

  Provides superior application experience, visibility, and security but still too many additional point products

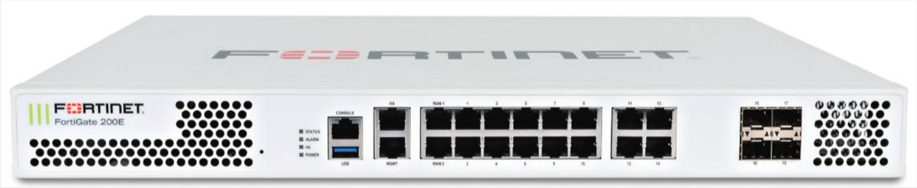
- **Secure SD-Branch**

  Provides integration of WAN and LAN platforms, reducing the number of devices, extending Secure SD-WAN features into the network

© Fortinet Inc. All Rights Reserved.

Secure SD-WAN

FortiGate



APPLICATION AWARE

- Visibility into 5000+ Applications
- High Application Identification Accuracy

MULTI-PATH INTELLIGENCE

- Application Steering Based on Expanded SLAs
- Automated Fail-Over Capabilities

WAN RESILIENCY

- WAN Path Remediation (FEC)
- Tunnel Bandwidth Aggregation (Per Packet Steering)

SIMPLIFIED MONITORING

- High-level Monitoring of SD-WAN Devices on a Map
- Expanded Historical SLA Analytics

SEGMENTATION

- Multi-Tenancy with Patented VDOM
- User Level Segmentation for Applications

© Fortinet Inc. All Rights Reserved.

(Secure) SD-Branch

Integrated Security

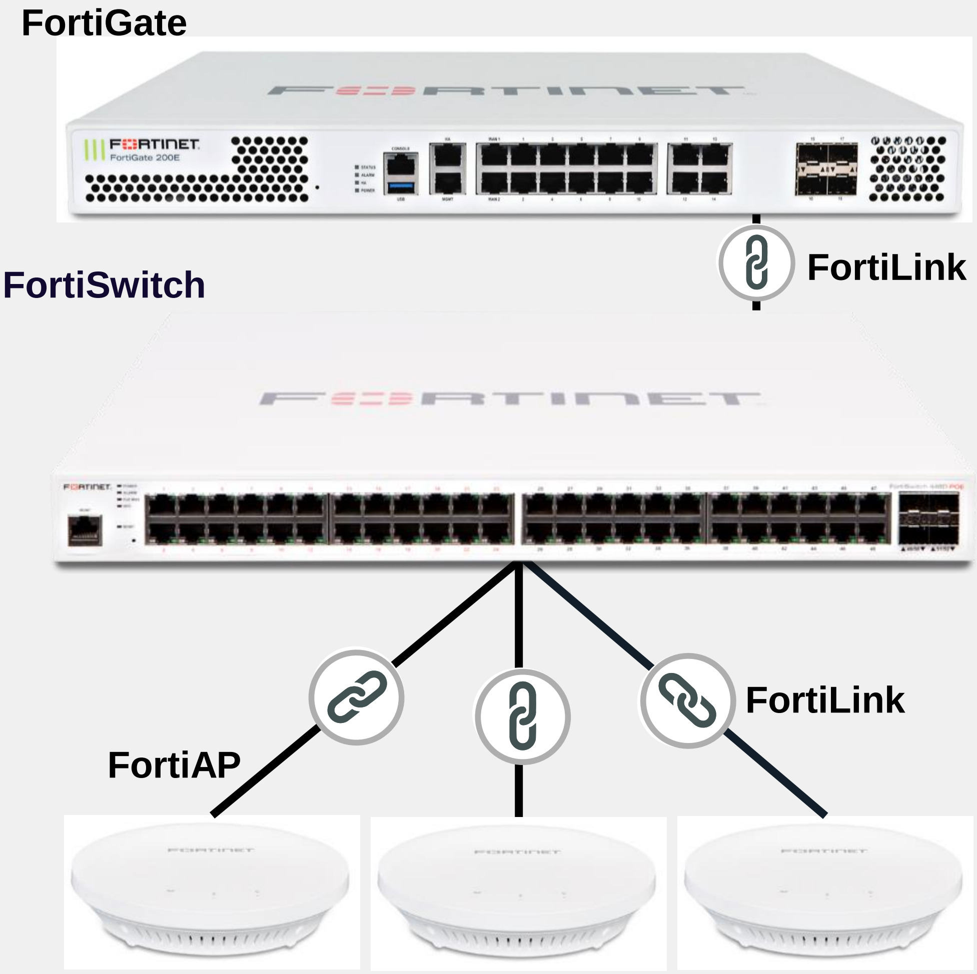
- FortiSwitch integrated into FortiGate as extensions of the NGFW
- Firewall and switch ports equally secure
- New NAC feature allows for secure IoT onboarding

Simplicity

- Ease of deployment and management through FortiGate interface
- Flexible architecture, scales as needs change
- Up to 300 switches per FortiGate

Lower Total Cost of Ownership

- FortiSwitch management included in FortiOS. No Licenses required.



© Fortinet Inc. All Rights Reserved.

Security Driven Networking

Security Driven Networking (**SASE Edge -** SASE)

- Expanding FOS on OPAQ Infrastructure
- Securing remote workforce with orchestration portal for SASE capabilities
- Securing thin branch with SASE to help customers moving from CAPEX to OPEX

Security Driven Networking (**WAN Edge:** SD-WAN)

- Increased Resiliency (Adaptive WAN Remediation)
- Efficient Operations (scalable ZTP, Analytics
- Better Cloud application experience with passive WAN monitoring
- Accelerated convergence for Thin & WAN edge
- New SD-WAN appliance with in-built WiFi6

Security Driven Networking (**DC Edge:** NGFW)

- Ultra-Scalability with pay as you grow model (FGT 7121F, 400G)
- Attack surface Reduction (Video filtering , DNS)
- Efficient Operations with network automation (Policy Learn mode, automated upgrades)

Security Driven Networking (**LAN Edge:** WiFi/Switch)

- Unified code base (L3 FortiLink, NAC Visibility and Zero trust response)
- Convergence (WLM and AIOps on FMG, FortiLAN cloud)
- Simplified Operation AI/ML driven wireless easy classification and remediation)

Security Driven Networking (**LTE Edge:** 5G)

- 5G backup (+SD-WAN for WWAN with new dual modem)
- LTE portfolio expansion (+WWAN application release, 101F/201F)
- SASE bundle for Thin edge and remote workers

Zero Trust Access (ZTNA)

- Single policy for on-net / off-net behavior
- Better & easier VPN with automated setup for HW/VM//SASE & cloud
- Granular access with role based application access
- Leverage existing products

Adaptive Cloud Security (VM, CWP, CASB)

- Centrally managed hybrid cloud (expended support & multi tenant policies)
- Effective usage of resources with autoscaling
- Extended application support for CASB
- Container guardian

Adaptive Cloud Security (WAF & Email)

- Email continuity switch to FortiMail cloud when service go down
- FortiWeb enhanced with ML-based API discovery, deep learning and more.
- FortiADC/FortiGSLB user experience visibility and Auto-Scaling capabilities

FortiGuard Threat *Intelligence* (Security Services)

- Increased Attack Surface Coverage – Video Filtering enhancement to our web filtering offering
- Security Rating expended to **Fabric Rating**
- **IoT real-time query service**

Fabric Management Center (SOC)

- MITRE attack analysis with expansion in cover and automated protection across the fabric and ecosystem
- SOAR enhanced AI/ML & out-of-the-box content packs. Integrations. FSR cloud. mobile app.
- IR unified console, FORTISOAR container, FortiCASB connector

Fabric Management Center (NOC)

- Insider threat analysis with EUBA support
- Enhanced visibility with extended product support across the Fabric & SD-Branch
- Efficient and scalable operation with SIEM
- SaaS management with Unified GUI, easy on boarding with ZTP templet and more & efficient full branch operations

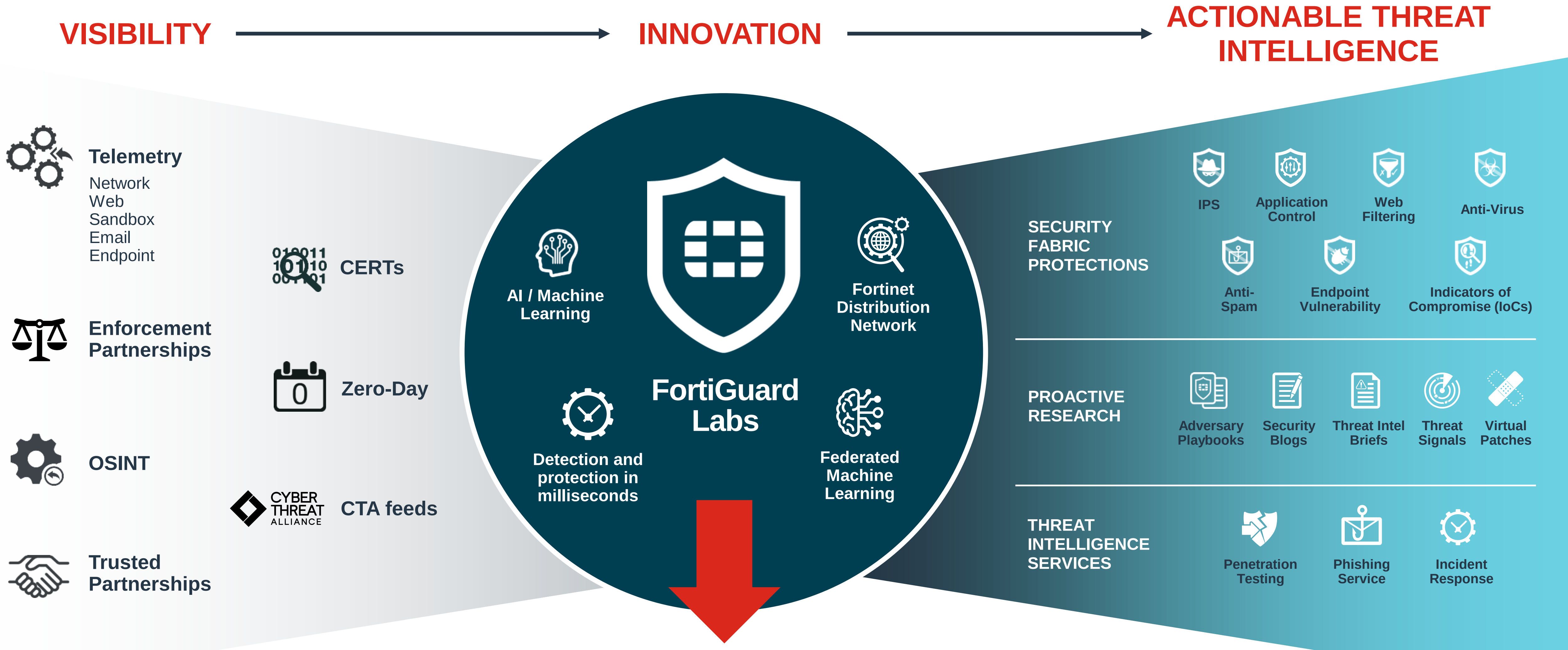
Advance Services

- SOC as a Service to augment organization and MSSP's SOC
- Best Practice Evaluation
- FortiGuard Consultant

© Fortinet Inc. All Rights Reserved.

FortiGuard Labs

FortiGuard Labs



VISIBILITY → INNOVATION → ACTIONABLE THREAT INTELLIGENCE

Telemetry
Network
Web
Sandbox
Email
Endpoint

CERTs

Enforcement Partnerships

Zero-Day

OSINT

CTA feeds

Trusted Partnerships

AI / Machine Learning

Fortinet Distribution Network

FortiGuard Labs

Detection and protection in milliseconds

Federated Machine Learning

SECURITY FABRIC PROTECTIONS
IPS
Application Control
Web Filtering
Anti-Virus
Anti-Spam
Endpoint Vulnerability
Indicators of Compromise (IoCs)

PROACTIVE RESEARCH
Adversary Playbooks
Security Blogs
Threat Intel Briefs
Threat Signals
Virtual Patches

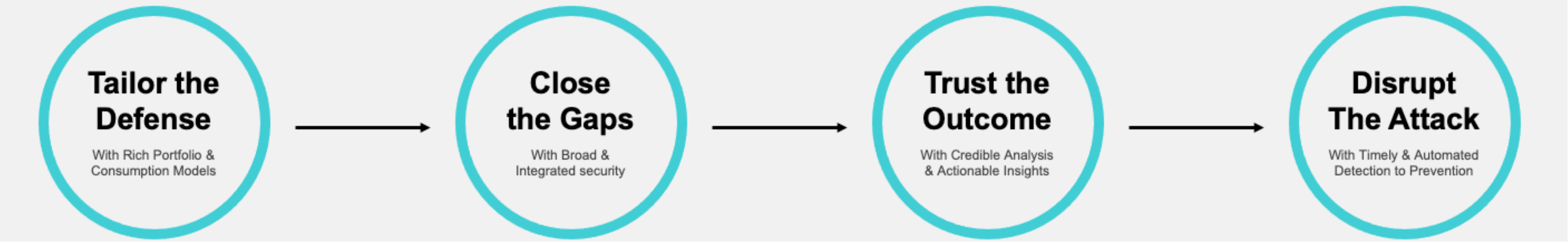
THREAT INTELLIGENCE SERVICES
Penetration Testing
Phishing Service
Incident Response

Our platform ingests and analyzes more than 100 billion events every day, on average.

© Fortinet Inc. All Rights Reserved.

FGD Security Services

Market leading security integrated across the attack lifecycle & surface



Tailor the Defense
With Rich Portfolio & Consumption Models

Close the Gaps
With Broad & Integrated security

Trust the Outcome
With Credible Analysis & Actionable Insights

Disrupt The Attack
With Timely & Automated Detection to Prevention

Content Security

Optimized to monitor and protect against file-based attack tactics

SBX AV DLP

MM CRED

Content Disarm Reconstruction

Virus Outbreak Service

Web Security

Optimized to monitor and protect against web-based attack tactics

VF Video Filtering

WF Web Filtering

WAF Web Application

C2

BOT Botnet DB

DNS

Geo IP & IP Rep

Device Security

Optimized to protect against device & vulnerability-based attack

OT IPS IoT

Vulnerability Scanning

MAC Address Vendor Mapping

Device / OS Detection

SOC/NOC Tools

Continuously evaluate and advance your security posture

PHISH Anti phishing

SoC as a Service

Fabric Rating

IoC

Outbreak Alert

Incident Response

FortiGuard Consulting

Pen Testing

And more ….

Bundles & EA

Freedom to choose the best Security and purchasing models

Enterprise License Agreement

ENT

ATP UTP

© Fortinet Inc. All Rights Reserved.

Service Offering	**A-la-carte**	**ATP**	**UTP**	**SMB** (FG 80 and lower)	**ENT**
24*7 Support SD-WAN, ZTNA, Application control, botnet control and database services	V	V	V	V	V
Content Security Av, AI-powered cloud sandbox, IPS	V	V	V	V	V
Web Security AI-powered Web, Video and DNS Filtering	V		V	V	V
Central Management & Analytics FortiGate Cloud management	V			V	
Device Security IoT and OT Advanced Security & compliance tools	V				V
Recommended add-ons SOC-as-a-Service Management SD-WAN Monitoring & Overlay Controller VPN Cloud Fortinet Client	V				

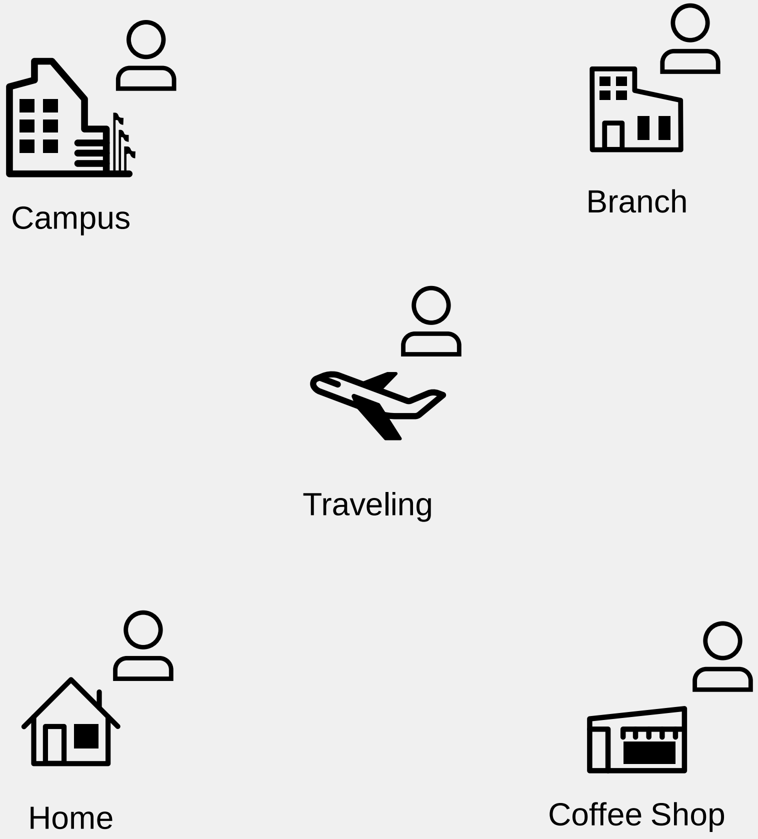
© Fortinet Inc. All Rights Reserved.

FortiClient ZTNA

Supporting Work From Anywhere (WFA)

A better user experience

- Access from in or out of Office
- Automatic secure tunnels to applications
- SSO Supported



Campus

Branch

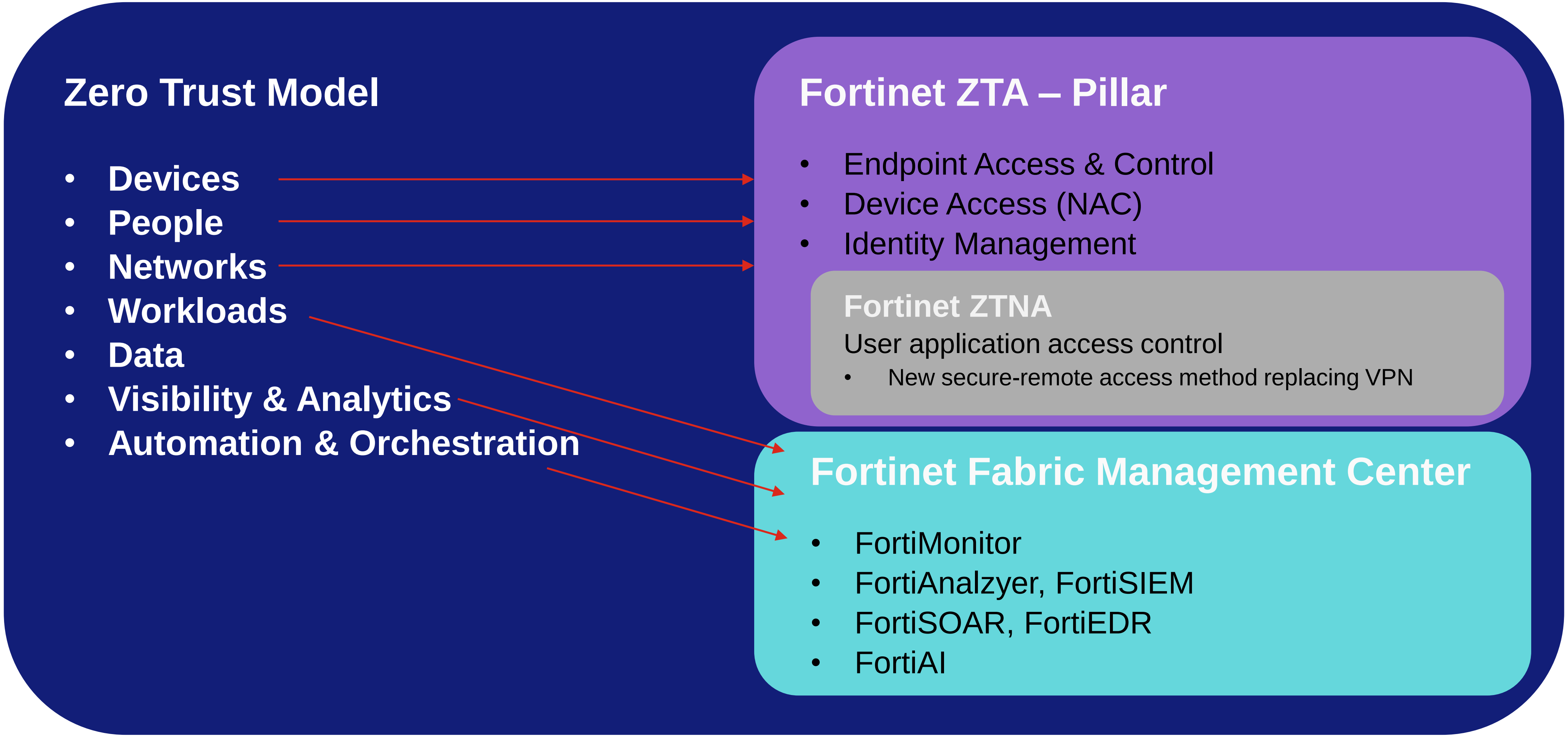
Traveling

Home

Coffee Shop

© Fortinet Inc. All Rights Reserved.

Fortinet ZTA, FMC and ZTNA in Context



Zero Trust Model

- Devices
- People
- Networks
- Workloads
- Data
- Visibility & Analytics
- Automation & Orchestration

Fortinet ZTA – Pillar

- Endpoint Access & Control
- Device Access (NAC)
- Identity Management

Fortinet ZTNA

User application access control

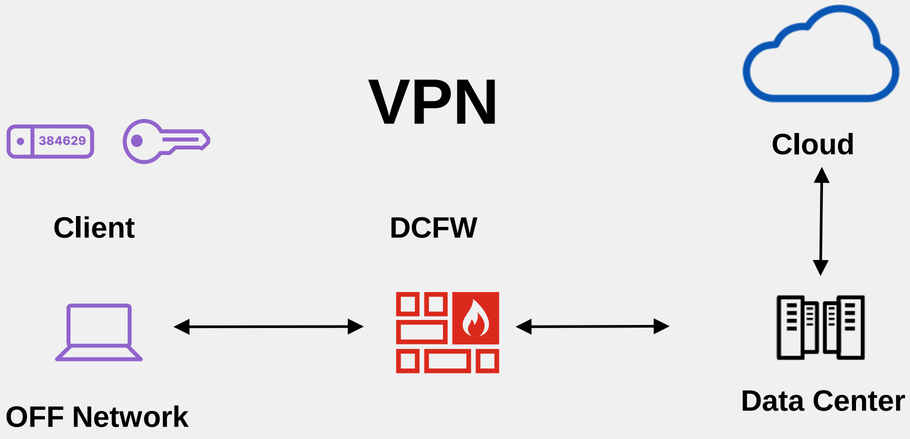
- New secure-remote access method replacing VPN

Fortinet Fabric Management Center

- FortiMonitor
- FortiAnalzyer, FortiSIEM
- FortiSOAR, FortiEDR
- FortiAI

From Traditional VPN to ZTNA

VPN

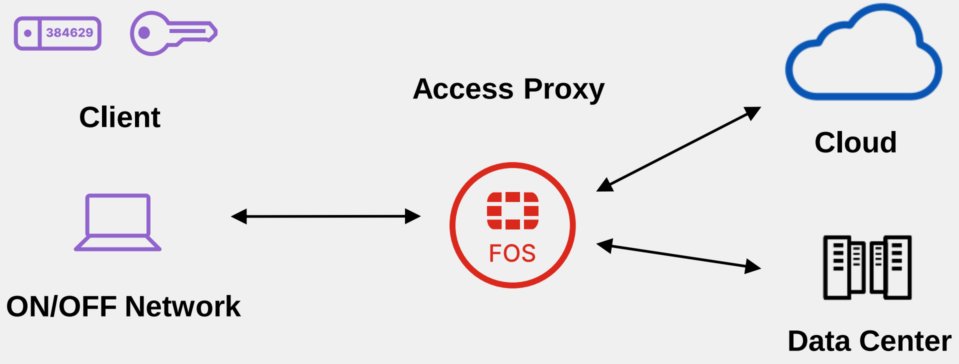


One Time Trust Check

Access Entire Network

Generic Rule Set

ZTNA



Continuous Trust Check

Access Specific Applications

User Contextual Rule Set

© Fortinet Inc. All Rights Reserved.

Fortinet’s ZTNA

What’s it made of? Existing Fortinet Security Fabric Products

Core Elements

FortiGate

- FortiGate builds the secure tunnel, maintains user group/application access table (FOS 7.0)

FortiClient / Central Management

- FortiClient Central Management configures the ZTNA agent in FortiClient for the secure connection back to the FortiGate (FortiClient 7.0)
  - FortiClient Central Management: Either FortiClient EMS or FortiClient Cloud

- Authentication Solution
  - FortiAuthenticator, FortiToken or any 3rd party supported by the Security Fabric

© Fortinet Inc. All Rights Reserved.

Fortinet ZTNA advantages

Complete coverage vs. other ZTNA solutions

- Leveraging existing investments in on-prem Firewalls
  - Most ZTNA solutions are SASE-only options with expensive charges for company-wide coverage
  - Leverage SD-WAN, SD-Branch capabilities

- Improved Security (“Secure ZTNA”)
  - Extend FortiGate protection to wherever you are
  - Traffic traversing Industry-leading FortiGate technology
- No Licenses Required
  - Simply a feature in FOS & Supported FortiClient version to turn on!

© Fortinet Inc. All Rights Reserved.

Evolution of VPN tunnels

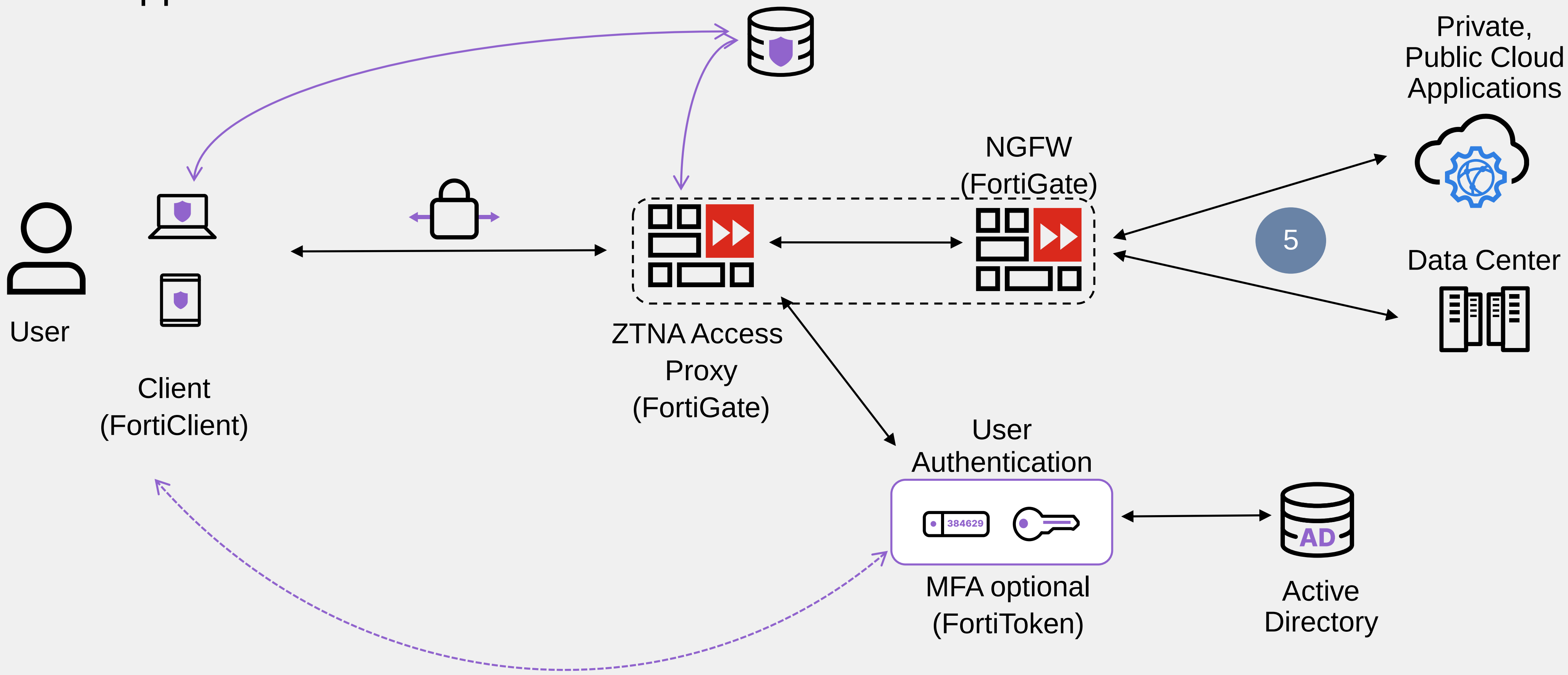
Bringing Zero Trust principles to remote access

- Ongoing verification
  - Per session user identity checks
  - Per session device posture checks (OS version, A/V status, vulnerability assessment)
- More granular control
  - Access granted only to specific application
  - No more broad VPN access to the network
- Easier user experience
  - Auto-initiates secure tunnel when user accesses applications
  - Same experience on and off-net

© Fortinet Inc. All Rights Reserved.

Zero Trust Network Access (ZTNA) Technology

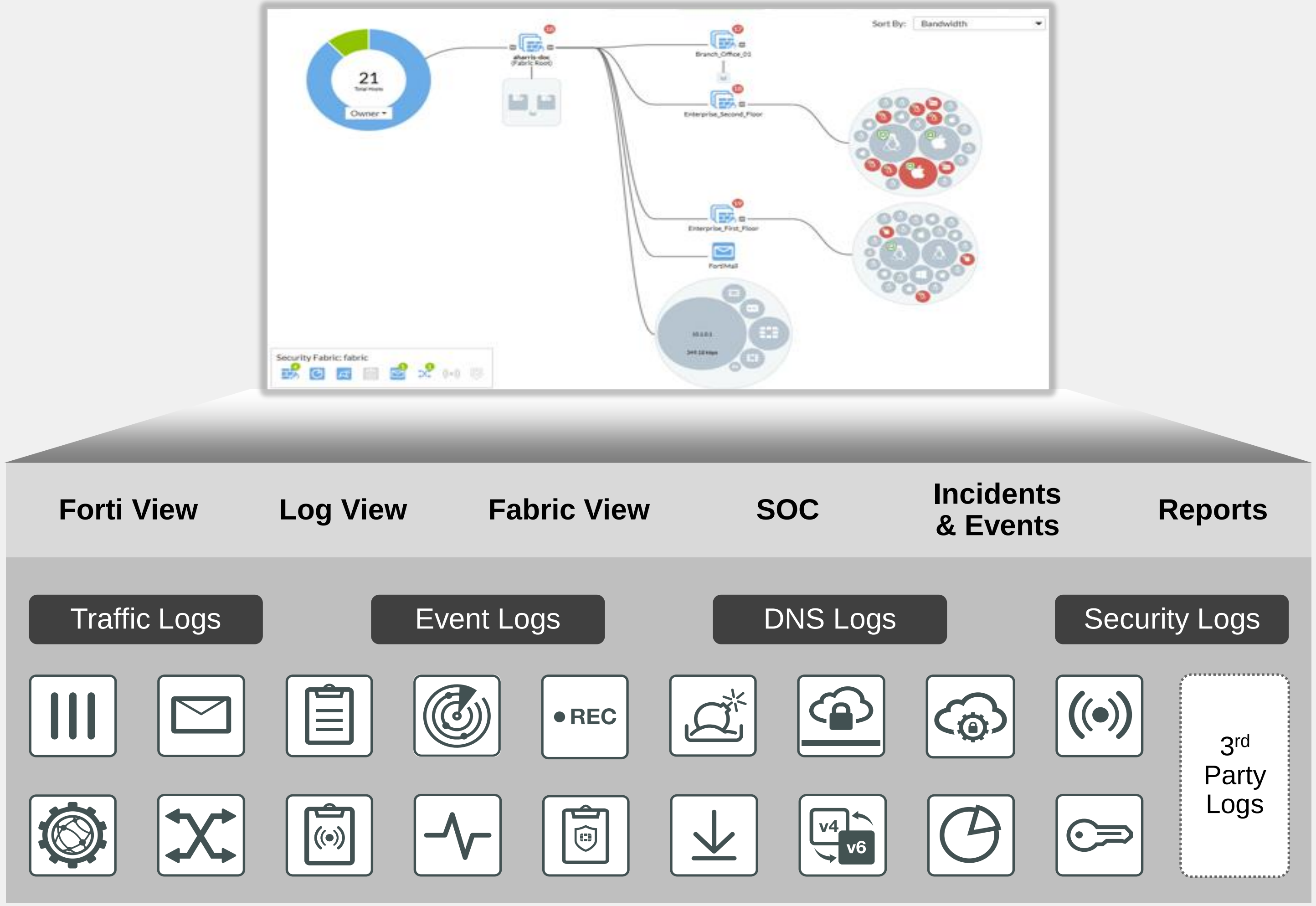
Granular Application Access



- Automatic, transparent encrypted tunnels
- Split tunneling
- Per Session verification & identification
- Additional layers of security with MFA
- Single-Sign-on agent supports FortiAuthenticator

FortiAnalyzer as a SOC

Logging & Reporting



Forti View | Log View | Fabric View | SOC | Incidents & Events | Reports

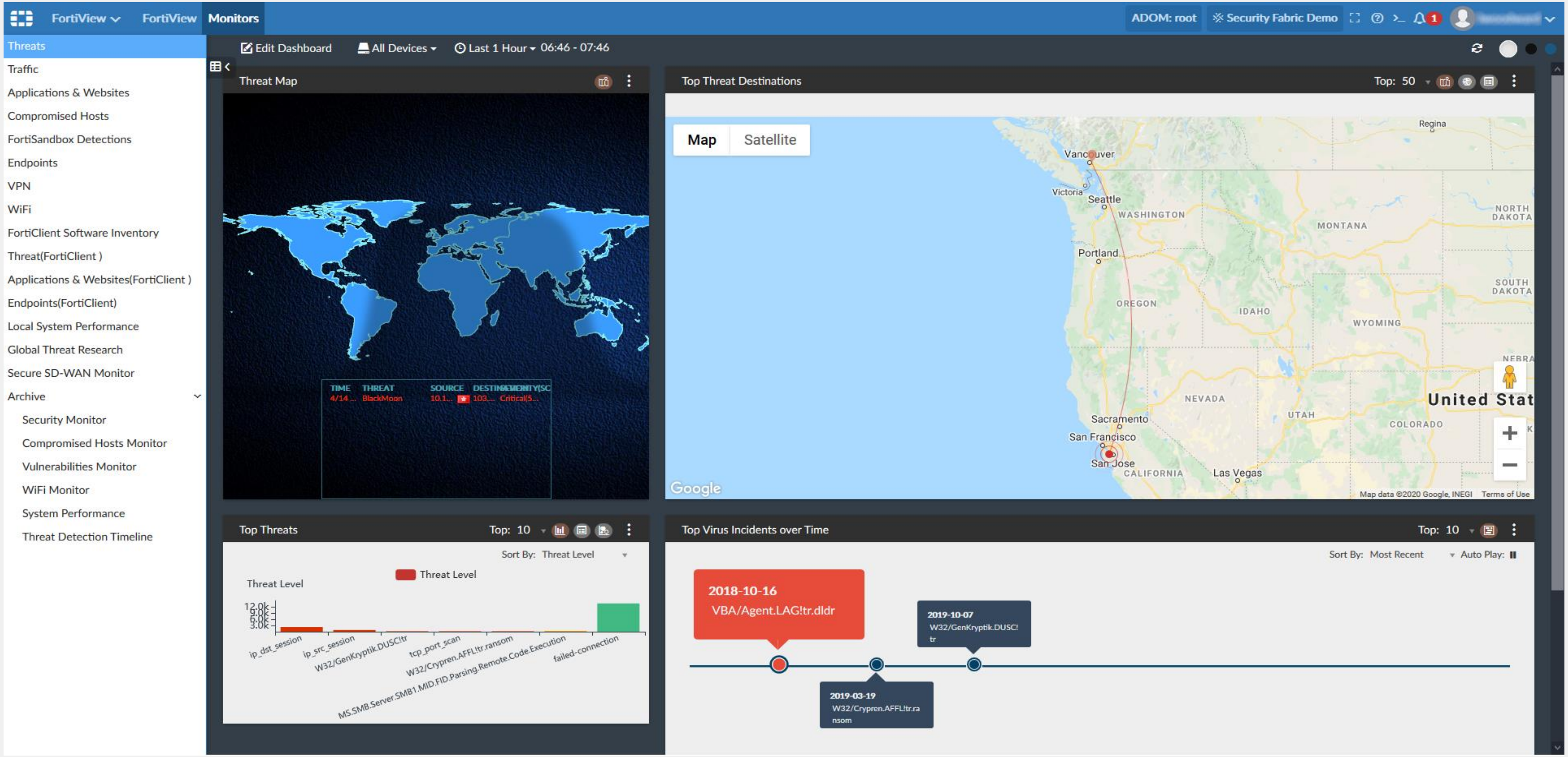
Traffic Logs | Event Logs | DNS Logs | Security Logs

3rd Party Logs

1. FortiGate
2. FortiClient
3. FortiNAC
4. FortiMail
5. FortiAuthenticator
6. FortiManager
7. FortiWeb
8. FortiSandbox
9. FortiCarrier
10. FortiCache
11. FortiDDos
12. FortiDeceptor
13. FortiProxy
14. Security Fabric
15. FortiRecorder
16. Generic Syslog

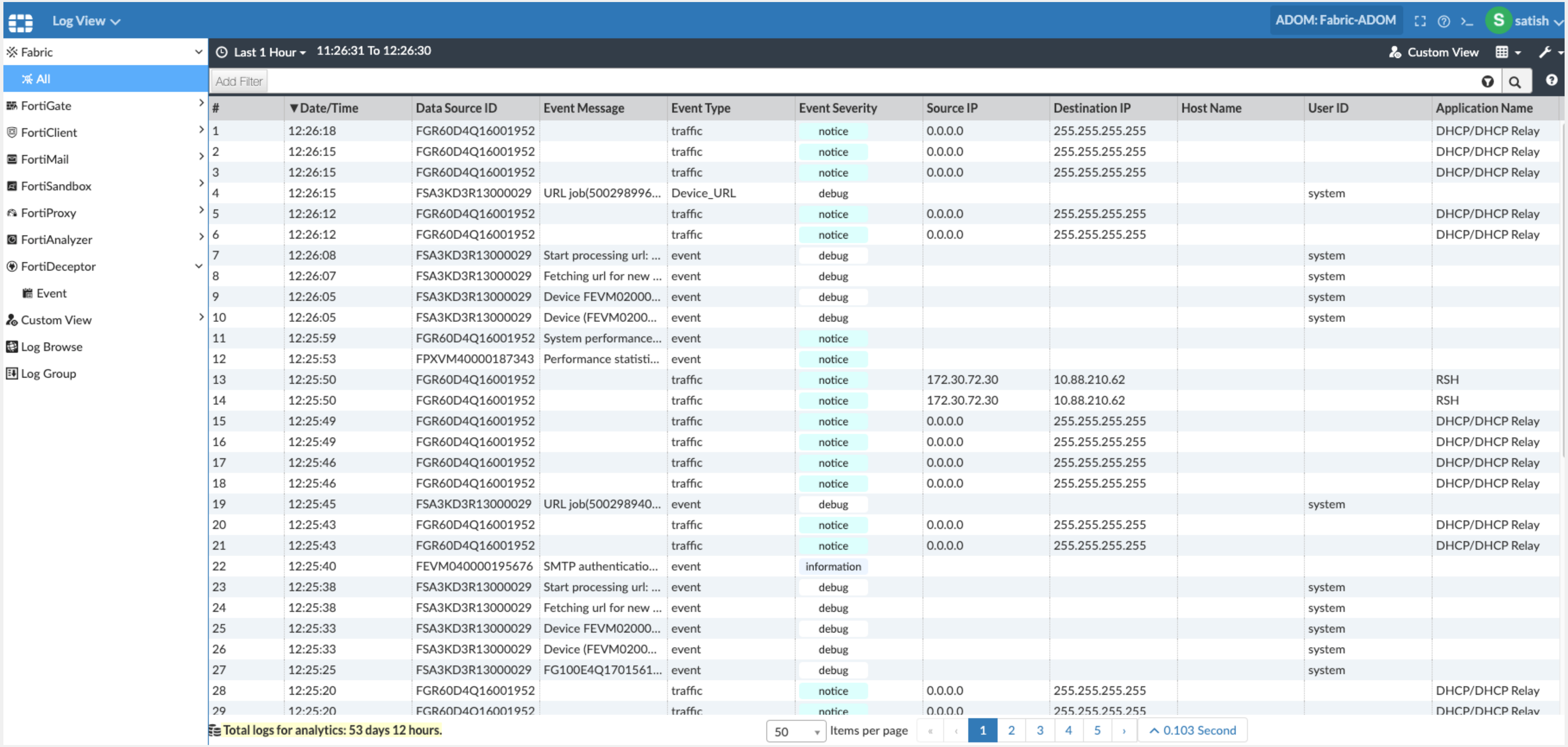
© Fortinet Inc. All Rights Reserved.

FortiView Monitors



© Fortinet Inc. All Rights Reserved.

Indicator of Compromise



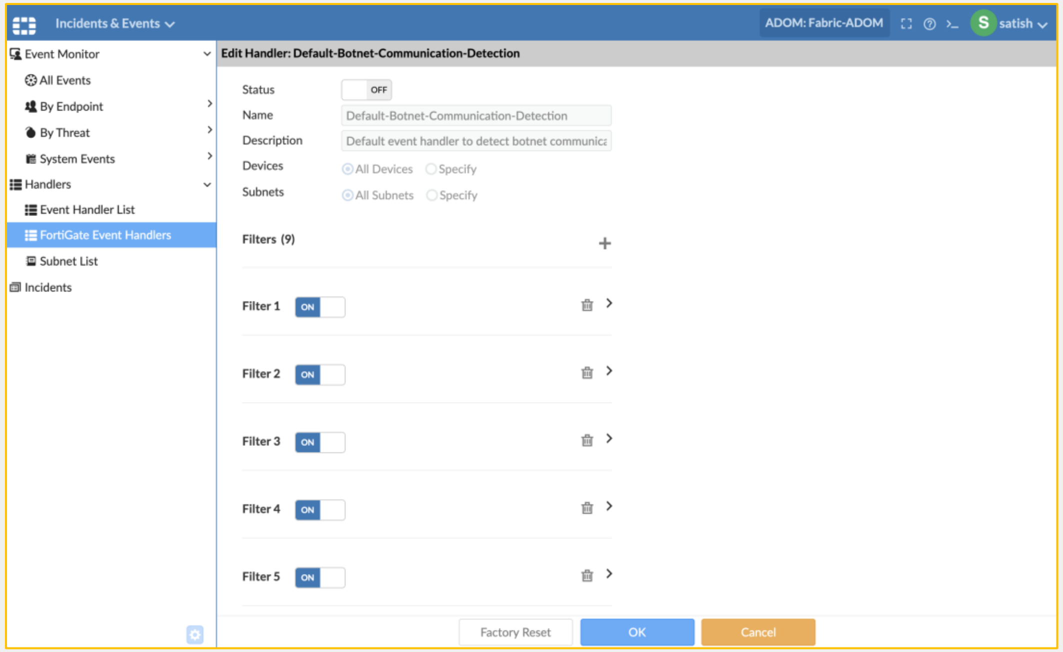
#	▼Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID	Application Name
1	12:26:18	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
2	12:26:15	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
3	12:26:15	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
4	12:26:15	FSA3KD3R13000029	URL job(500298996...	Device_URL	debug				system	
5	12:26:12	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
6	12:26:12	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
7	12:26:08	FSA3KD3R13000029	Start processing url: ...	event	debug				system	
8	12:26:07	FSA3KD3R13000029	Fetching url for new ...	event	debug				system	
9	12:26:05	FSA3KD3R13000029	Device FEVM02000...	event	debug				system	
10	12:26:05	FSA3KD3R13000029	Device (FEVM0200...	event	debug				system	
11	12:25:59	FGR60D4Q16001952	System performance...	event	notice					
12	12:25:53	FPXVM40000187343	Performance statisti...	event	notice					
13	12:25:50	FGR60D4Q16001952		traffic	notice	172.30.72.30	10.88.210.62			RSH
14	12:25:50	FGR60D4Q16001952		traffic	notice	172.30.72.30	10.88.210.62			RSH
15	12:25:49	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
16	12:25:49	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
17	12:25:46	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
18	12:25:46	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
19	12:25:45	FSA3KD3R13000029	URL job(500298940...	event	debug				system	
20	12:25:43	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
21	12:25:43	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
22	12:25:40	FEVM040000195676	SMTP authenticatio...	event	information					
23	12:25:38	FSA3KD3R13000029	Start processing url: ...	event	debug				system	
24	12:25:38	FSA3KD3R13000029	Fetching url for new ...	event	debug				system	
25	12:25:33	FSA3KD3R13000029	Device FEVM02000...	event	debug				system	
26	12:25:33	FSA3KD3R13000029	Device (FEVM0200...	event	debug				system	
27	12:25:25	FSA3KD3R13000029	FG100E4Q1701561...	event	debug				system	
28	12:25:20	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay
29	12:25:20	FGR60D4Q16001952		traffic	notice	0.0.0.0	255.255.255.255			DHCP/DHCP Relay

Total logs for analytics: 53 days 12 hours.

© Fortinet Inc. All Rights Reserved.

Security Fabric Integration

FortiAnalyzer



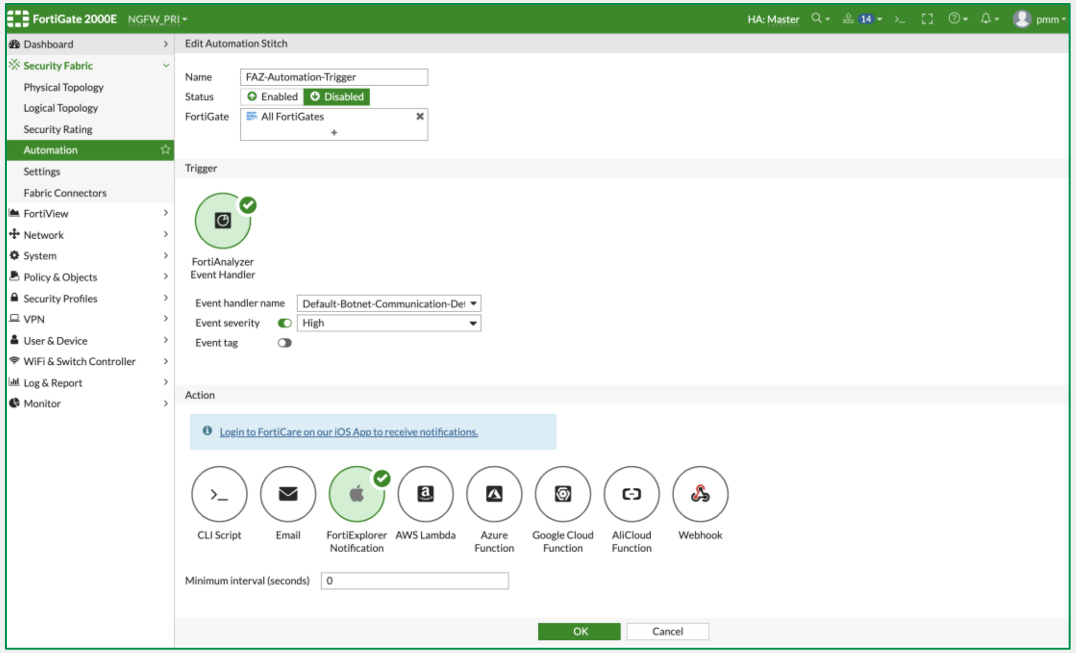
Edit Handler: Default-Botnet-Communication-Detection

Status: OFF
Name: Default-Botnet-Communication-Detection
Description: Default event handler to detect botnet communica
Devices: ● All Devices ○ Specify
Subnets: ● All Subnets ○ Specify

Filters (9)

Filter 1: ON
Filter 2: ON
Filter 3: ON
Filter 4: ON
Filter 5: ON

FortiGate



Edit Automation Stitch

Name: FAZ-Automation-Trigger
Status: Enabled [✓ Disabled]
FortiGate: All FortiGates

Trigger

FortiAnalyzer Event Handler ✓

Event handler name: Default-Botnet-Communication-De‹
Event severity: High
Event tag

Action

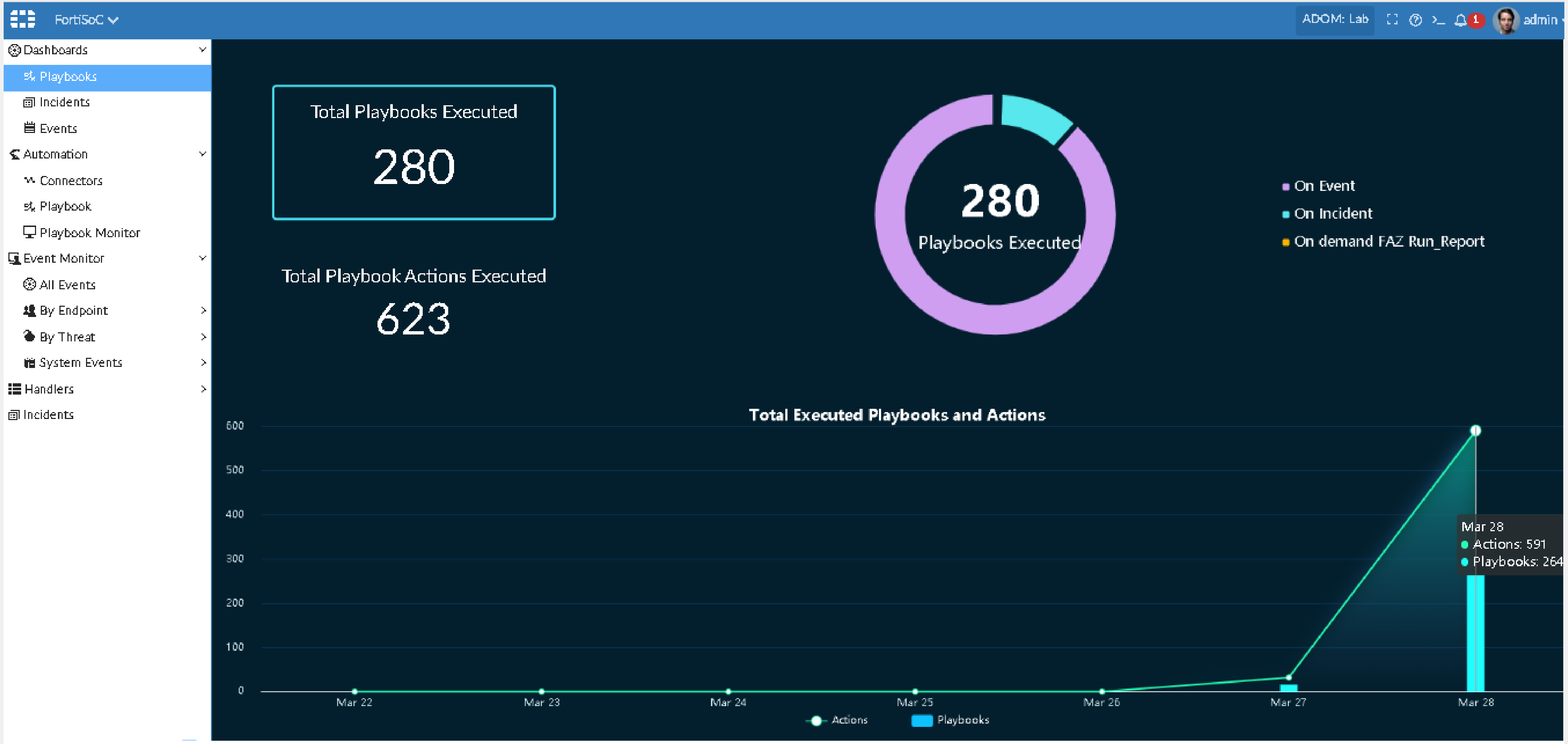
Login to FortiCare on our iOS App to receive notifications.

Minimum interval (seconds): 0

- **Security Fabric's** Analytics Engine is part of FortiAnalyzer and is necessary for the Fabric
- **Automation Stitch** is like If-this-then-that of the Security Fabric. FortiAnalyzer is the Analytics backend of the Security Fabric and can be leveraged natively in a FortiGate thought a secure channel between FortiGate & FortiAnalyzer

© Fortinet Inc. All Rights Reserved.

FortiSOC: Playbooks



Total Playbooks Executed

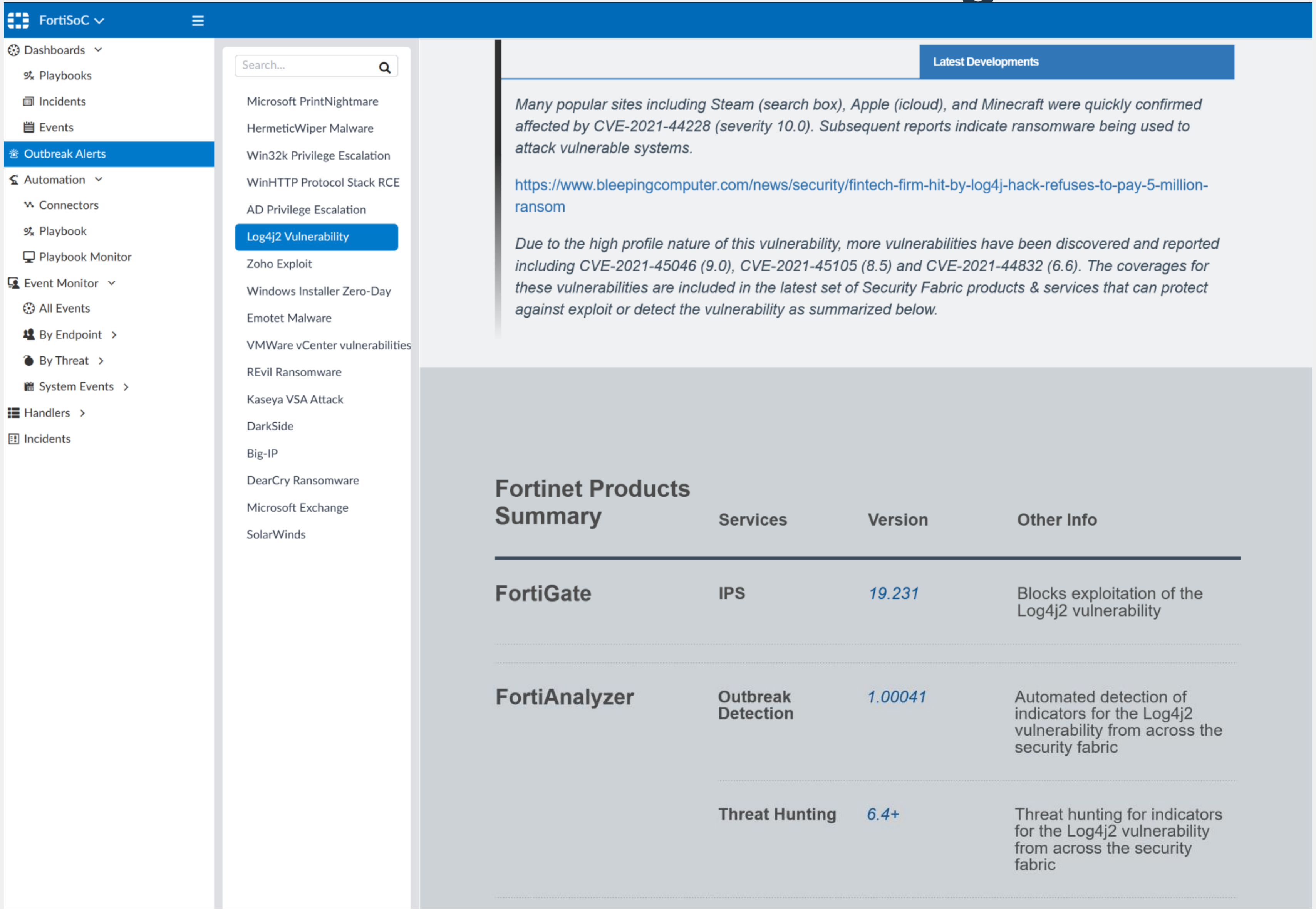
280

Total Playbook Actions Executed

623

© Fortinet Inc. All Rights Reserved.

FortiSOC: OutBreak and Alerting service



Many popular sites including Steam (search box), Apple (icloud), and Minecraft were quickly confirmed affected by CVE-2021-44228 (severity 10.0). Subsequent reports indicate ransomware being used to attack vulnerable systems.

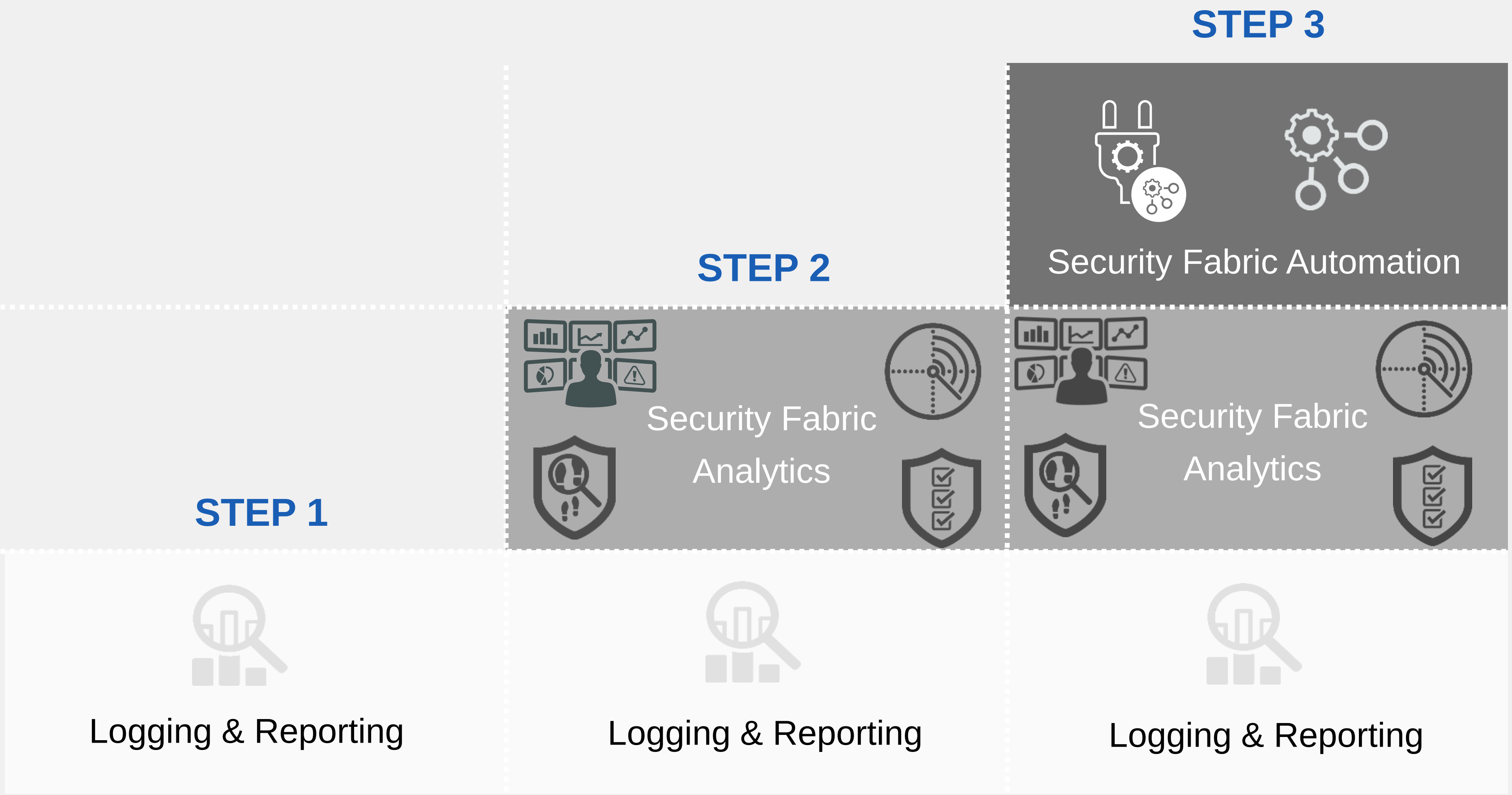
https://www.bleepingcomputer.com/news/security/fintech-firm-hit-by-log4j-hack-refuses-to-pay-5-million-ransom

Due to the high profile nature of this vulnerability, more vulnerabilities have been discovered and reported including CVE-2021-45046 (9.0), CVE-2021-45105 (8.5) and CVE-2021-44832 (6.6). The coverages for these vulnerabilities are included in the latest set of Security Fabric products & services that can protect against exploit or detect the vulnerability as summarized below.

Fortinet Products Summary	Services	Version	Other Info
FortiGate	IPS	*19.231*	Blocks exploitation of the Log4j2 vulnerability
FortiAnalyzer	Outbreak Detection	*1.00041*	Automated detection of indicators for the Log4j2 vulnerability from across the security fabric
	Threat Hunting	*6.4+*	Threat hunting for indicators for the Log4j2 vulnerability from across the security fabric

© Fortinet Inc. All Rights Reserved.

FortiAnalyzer: Three Stages of Deployment



STEP 3

Security Fabric Automation

STEP 2

Security Fabric Analytics

Security Fabric Analytics

STEP 1

Logging & Reporting

Logging & Reporting

Logging & Reporting

Ref: 2020 CISO Benchmark Study

© Fortinet Inc. All Rights Reserved.

FORTINET®