Security Fabric – integracja rozwiązań w świecie bezpieczeństwa

Michał Kędzierski

Channel Systems Engineer

mkedzierski@fortinet.com

Securing people, devices, and data everywhere.

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our security solutions are among the most deployed, most patented, and most validated in the industry.

Global Customer Base **680,000+** Customers	2022 Billings **$5.59B+** *(as of Dec 31, 2022)*	Market Capitalization **$59.38B** *(as of June 30, 2023)*
Broad, Integrated Portfolio of **50+** Enterprise Cybersecurity Products	Strong Analyst Validation **41** Enterprise Analyst Report Inclusions	Vertical Integration **$1B+** Investment in ASIC Design & Development

FORTINET

Founded: **October 2000**

Founded by: **Ken Xie and Michael Xie**

Headquarters: **Sunnyvale, CA**

Fortinet IPO (FTNT): **November 2009**

Listed in both: **NASDAQ 100 and S&P 500**

Member of: **2022 Dow Jones Sustainability World and North America Indices**

Security Investment Grade Rating: **BBB+ Baa1**

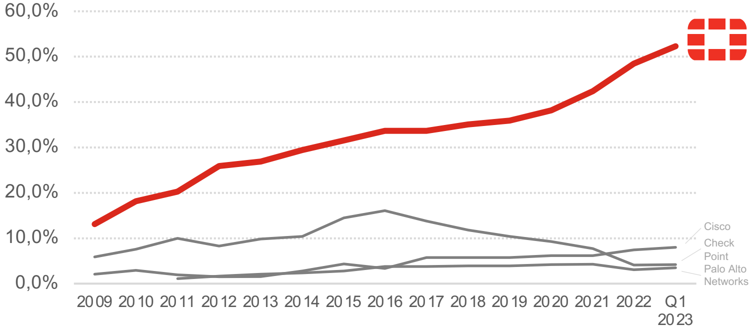
Investing in Innovation for Our Customers

Strong investment in our supply chain

~50%

of All Next-Gen Firewall Shipments & #1 in revenue market share

Global Firewall Shipments



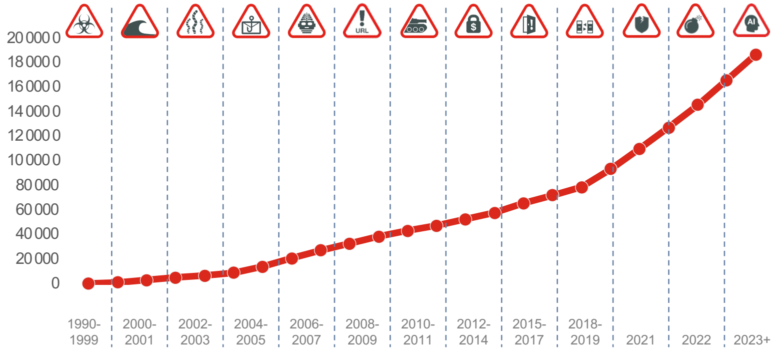
Source: IDC Quarterly Security Appliance Tracker 2023Q1 (based on shipments of Firewall + UTM appliances)

Investment in scale of threat intelligence and AI/ML

100+B

global security events analyzed per day

Advanced Threats – Global CVE

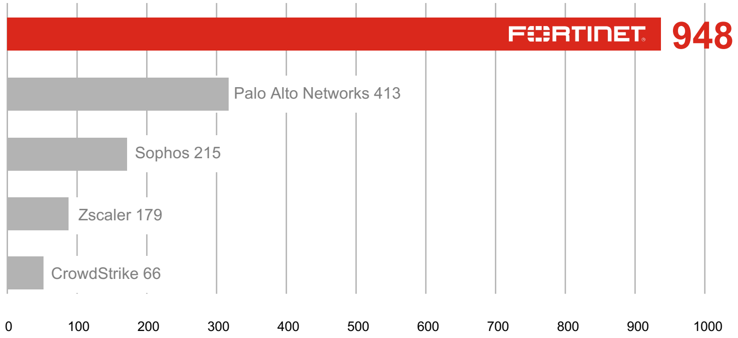


Organic R&D investment across our portfolio

1,285

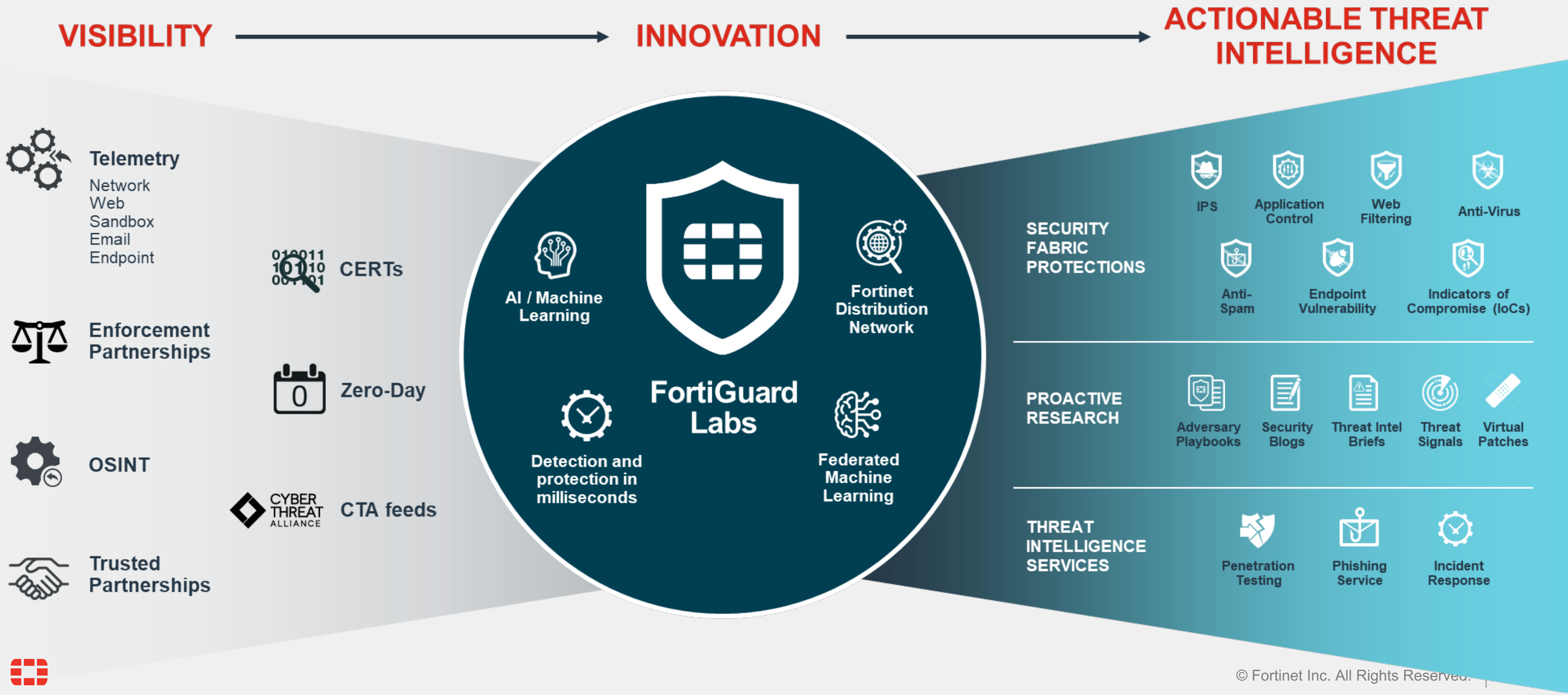
Global Industry Patents

U.S. Patents



Source: U.S. Patent Office, as of June 30, 2023

Actionable Threat Intel from FortiGuard Labs



VISIBILITY → INNOVATION → ACTIONABLE THREAT INTELLIGENCE

Telemetry
Network
Web
Sandbox
Email
Endpoint

CERTs

Enforcement Partnerships

Zero-Day

OSINT

CTA feeds

Trusted Partnerships

FortiGuard Labs

- AI / Machine Learning
- Fortinet Distribution Network
- 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)

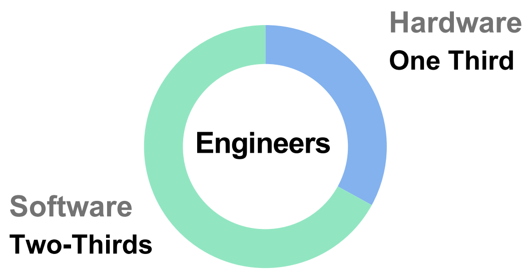
PROACTIVE RESEARCH
Adversary Playbooks, Security Blogs, Threat Intel Briefs, Threat Signals, Virtual Patches

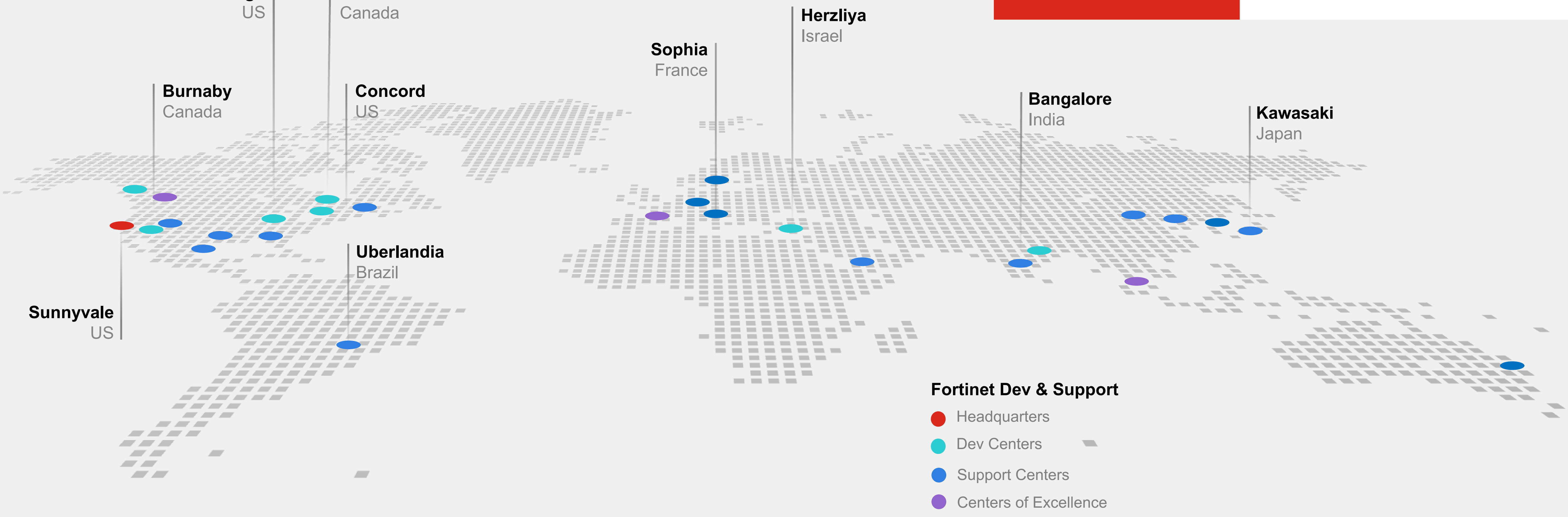
THREAT INTELLIGENCE SERVICES
Penetration Testing, Phishing Service, Incident Response

Global Reach & Support

Majority of our R&D is based in North America

13,600+
Employees Worldwide

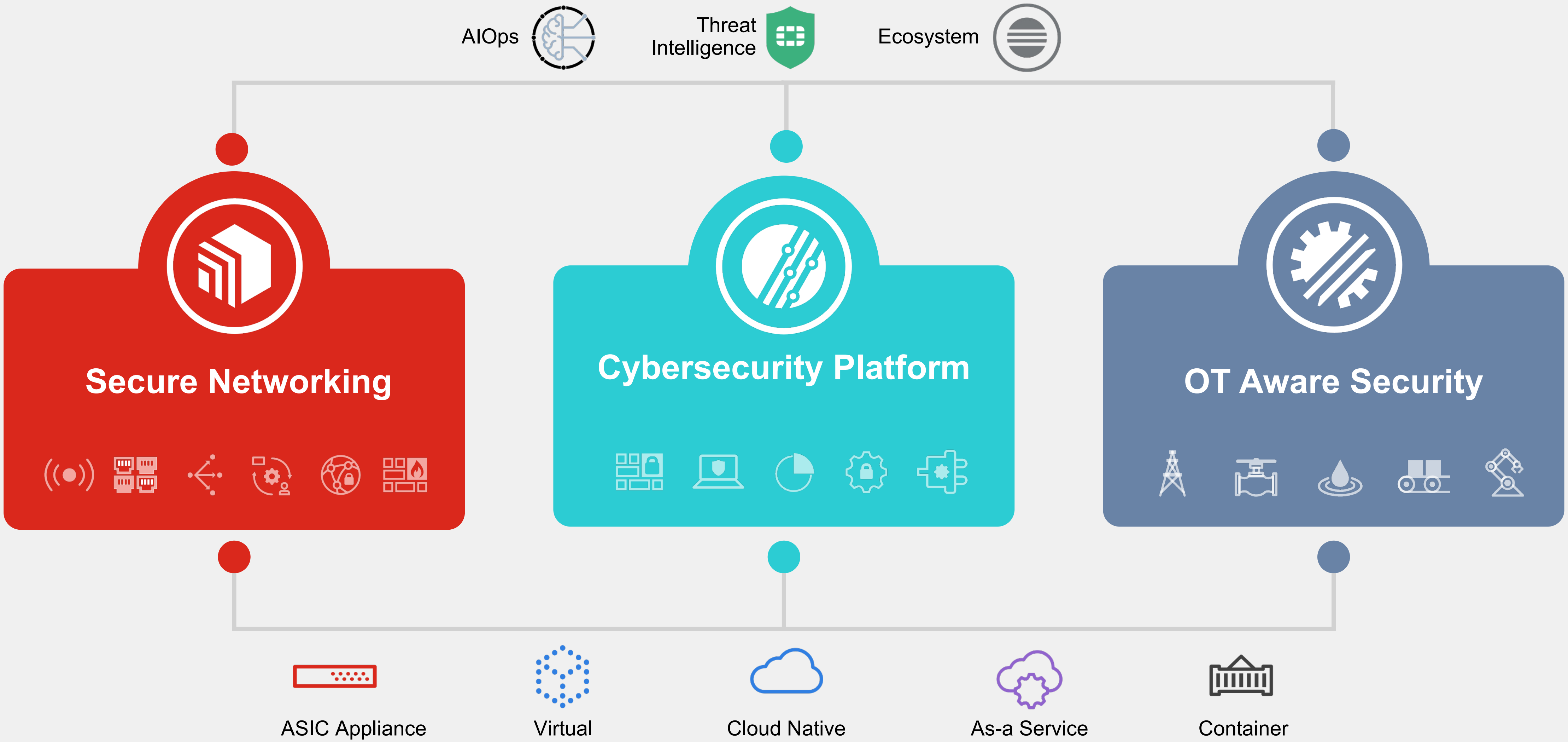




Fortinet Dev & Support

- 🟥 Headquarters
- ● Dev Centers
- ● Support Centers
- ● Centers of Excellence

Consolidation Reduces Complexity & Accelerates Outcomes



AIOps

Threat Intelligence

Ecosystem

Secure Networking

Cybersecurity Platform

OT Aware Security

ASIC Appliance

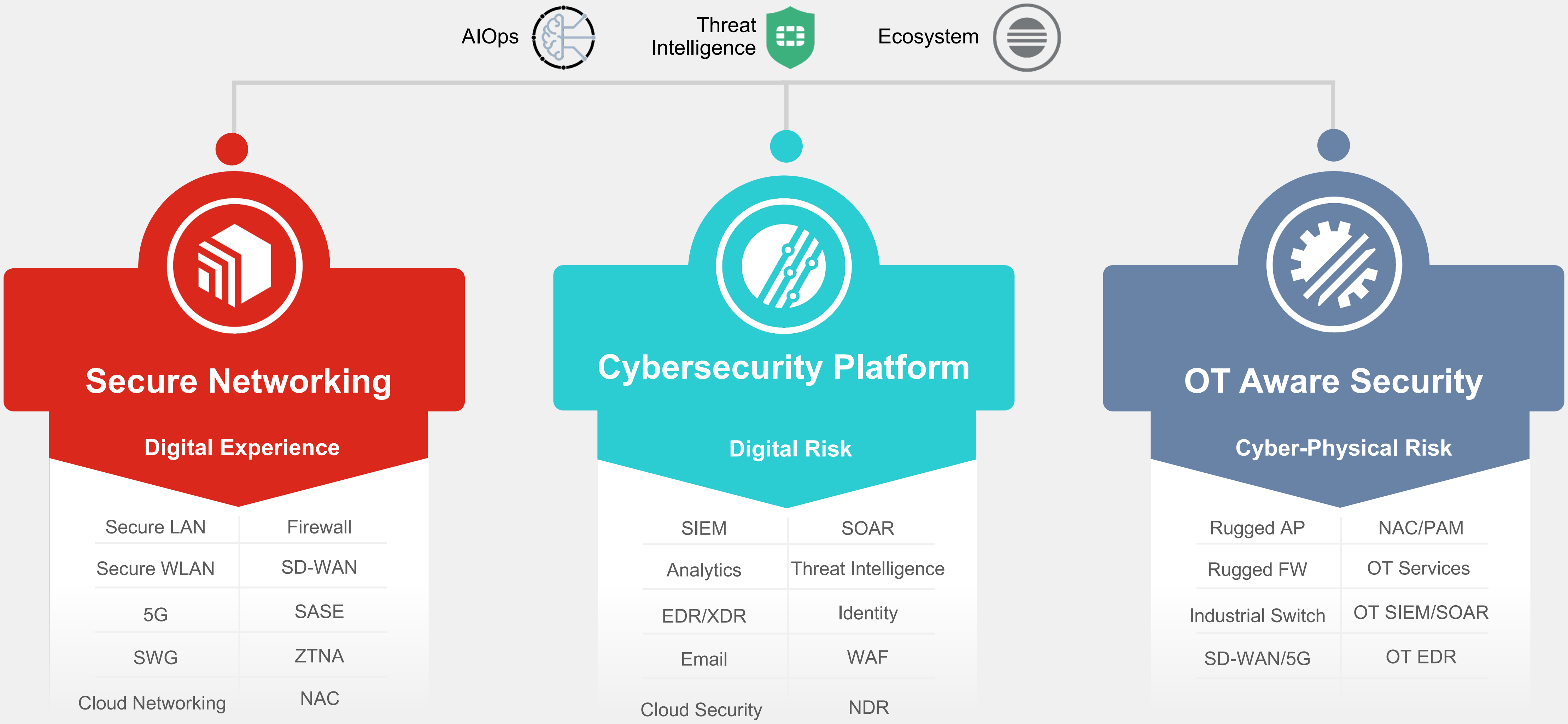
Virtual

Cloud Native

As-a Service

Container

Consolidation Reduces Complexity & Accelerates Outcomes



AIOps

Threat Intelligence

Ecosystem

Secure Networking

Digital Experience

Secure LAN	Firewall
Secure WLAN	SD-WAN
5G	SASE
SWG	ZTNA
Cloud Networking	NAC

Cybersecurity Platform

Digital Risk

SIEM	SOAR
Analytics	Threat Intelligence
EDR/XDR	Identity
Email	WAF
Cloud Security	NDR

OT Aware Security

Cyber-Physical Risk

Rugged AP	NAC/PAM
Rugged FW	OT Services
Industrial Switch	OT SIEM/SOAR
SD-WAN/5G	OT EDR

Fortinet Security Fabric

Broad

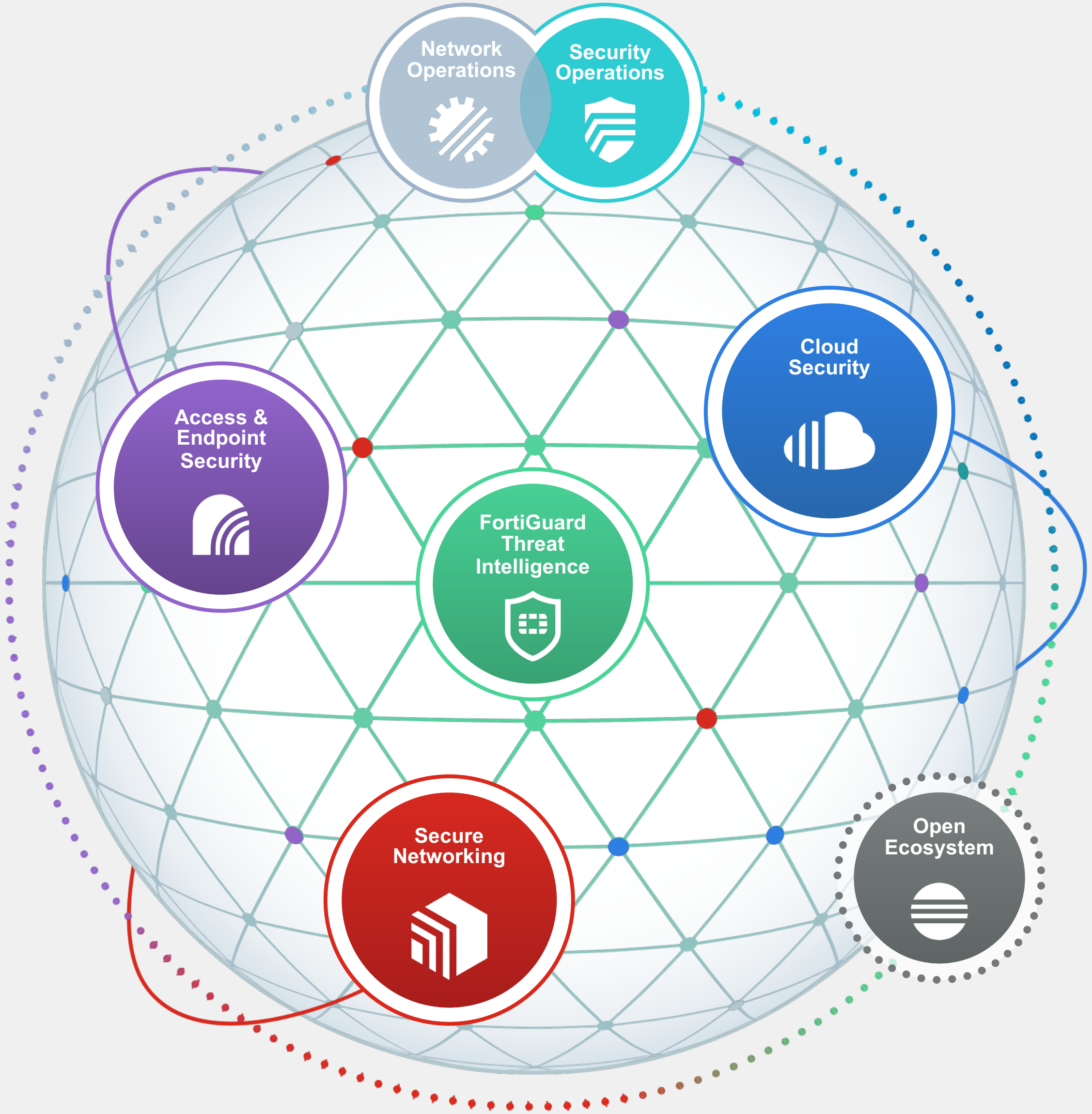
visibility and protection of the entire digital attack surface to better manage risk

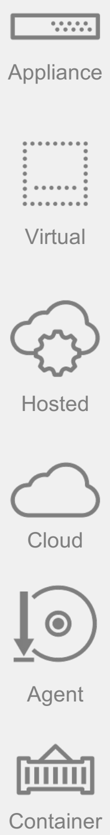
Integrated

solution that reduces management complexity and shares threat intelligence

Automated

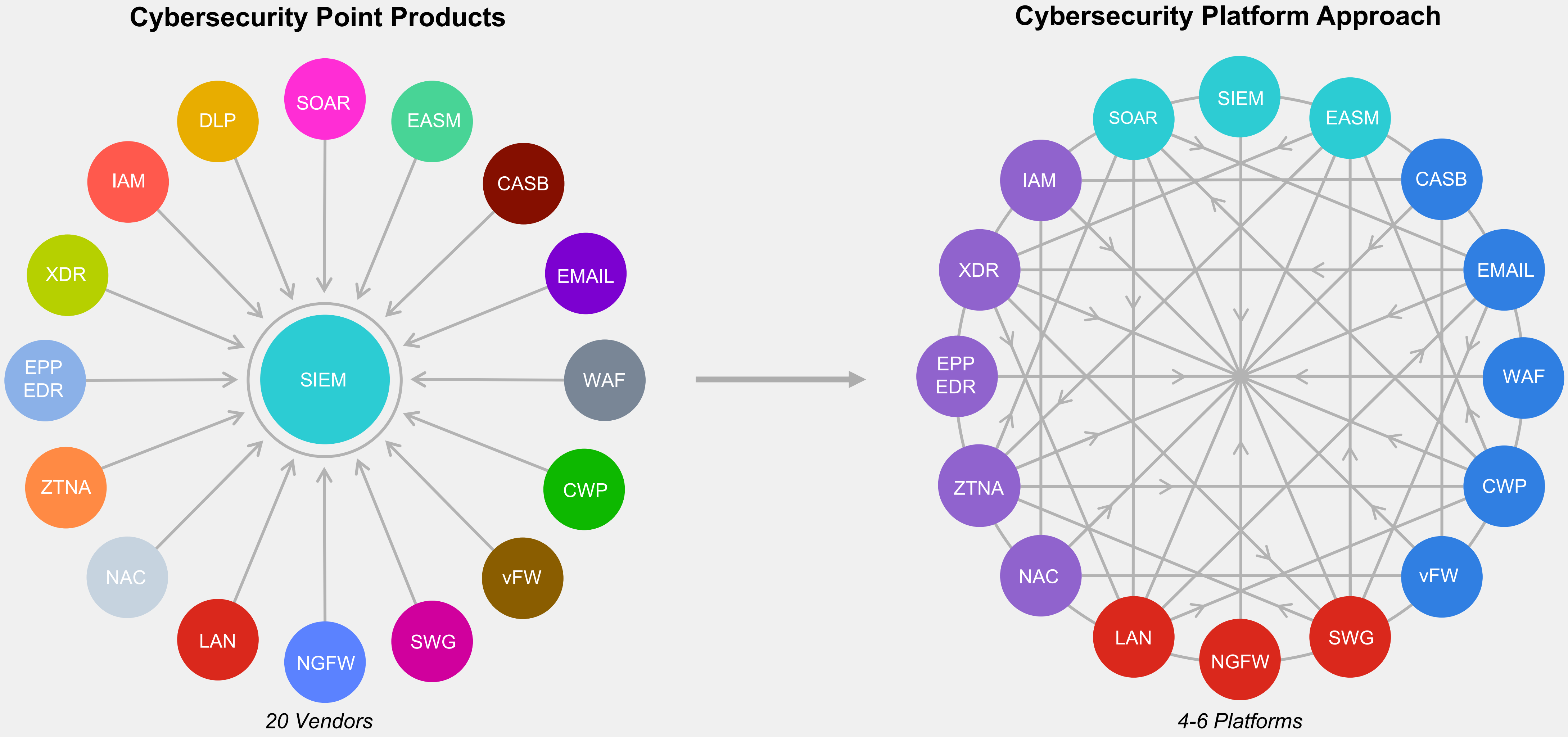
self-healing networks with AI-driven security for fast and efficient operations





Konsolidacja dostawców produktów bezpieczeństwa

Więcej nie znaczy lepiej



Extensive Cybersecurity Ecosystem

480+ Open Ecosystem Integrations

Fabric Connectors (13)

Fortinet-developed deep integrations that automate security operations and policies

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

Fabric APIs (248)

Partner-developed integrations using Fabric APIs that provide broad visibility with end-to-end solutions

DELL · DRAGOS · EQUINIX · intel · Megaport · rubrik · Security Bridge · SIEMENS Ingenuity for life · splunk> · tufin

Fabric DevOps (10)

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

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

Extended Security Fabric Ecosystem (200+)

Collaboration with threat sharing organizations and integrations with other vendor products

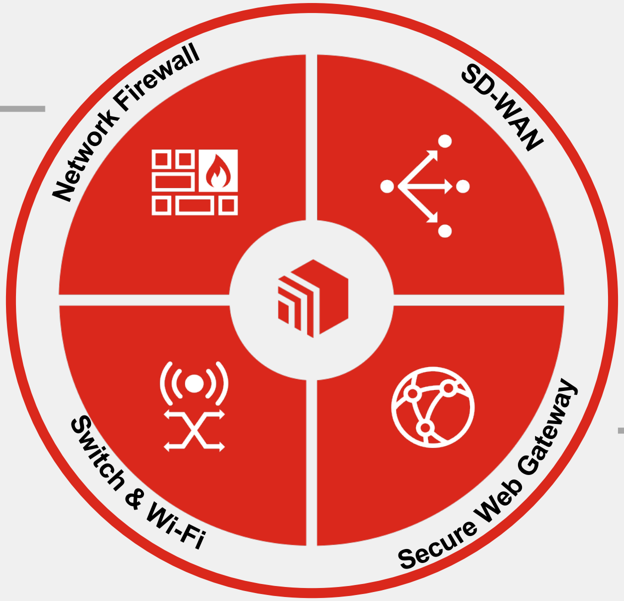
CYBER THREAT ALLIANCE · MITRE · STIX · INTERPOL · OT CSA · Firewalls · Switching · Wireless · Endpoint Security

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

Figures as of June 30, 2021

Network Security Portfolio

FortiGate Firewall
- Next-Generation Firewall
- Internal Segmentation
- Hyperscale Firewall



FortiProxy
- Secure Web Gateway
- On Premises

FortiSASE SWG
- Secure Web Gateway
- Cloud-Delivered

FortiGuard AI-Powered Security

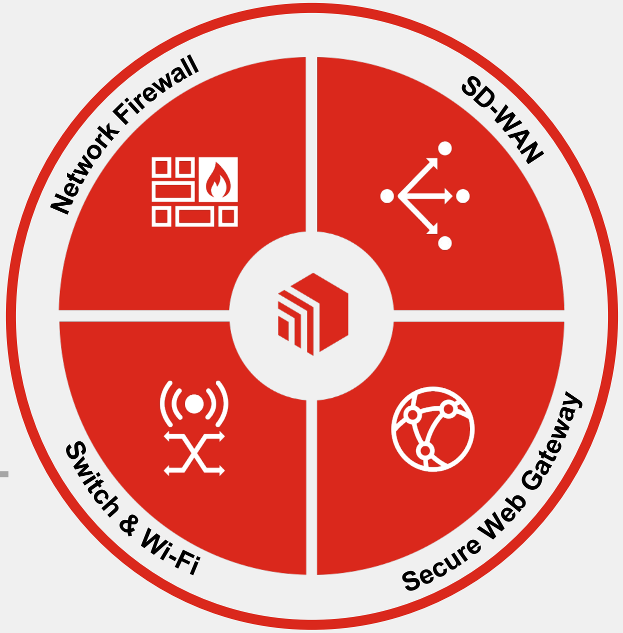
Enterprise Networking Portfolio

FortiAP
- Indoor
- Outdoor

FortiSwitch
- Campus/Branch
- Data Center

FortiNAC
- Zero Trust for Devices
- User Access Control
- Guest Access Control

Linksys HomeWRK
- Home Network



FortiGate SD-WAN
- WAN Edge device
- Application Steering
- Advanced Routing
- Cloud On-Ramp

FortiExtender
- LTE/5G WWAN Gateway
- SD-Branch

FortiGuard AI-Powered Security

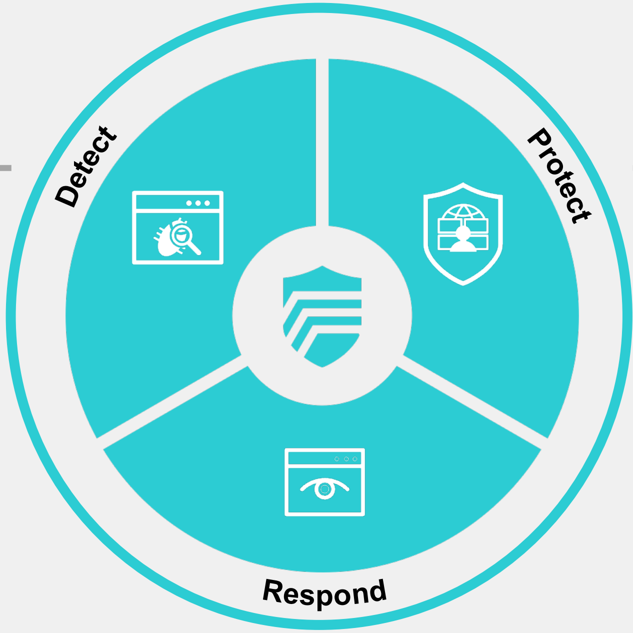
Security Operations

FortiGuard AI-Powered Detection
- Vulnerability, IOC, Decoys, IoT/OT Detection

FortiDeceptor
- Detect reconnaissance
- Engage ransomware
- Identify lateral movement

FortiNDR
- Detect anomalies
- Analyze malware
- Automate response

FortiRecon
- Map the attack surface
- Detect threat infrastructure



FortiGuard AI-Powered Protection
- AV, IPS, Botnet, Web Filtering, Anti-spam, App Control, WAF, IoT/OT virtual patching

FortiClient EPP
- NGAV
- Application Inventory
- Cloud Sandbox

FortiEDR
- Attack Surface Hardening / NGAV
- EDR / XDR
- Ransomware protection

FortiSandbox
- Zero-day detection in real time
- Appliance, VM, Hosted, and SaaS

FortiGuard AI-Powered Response
- Outbreak Detection, XDR, Playbooks.

FortiAnalyzer
- Fabric Visibility
- Fabric Analytics
- Fabric Automation

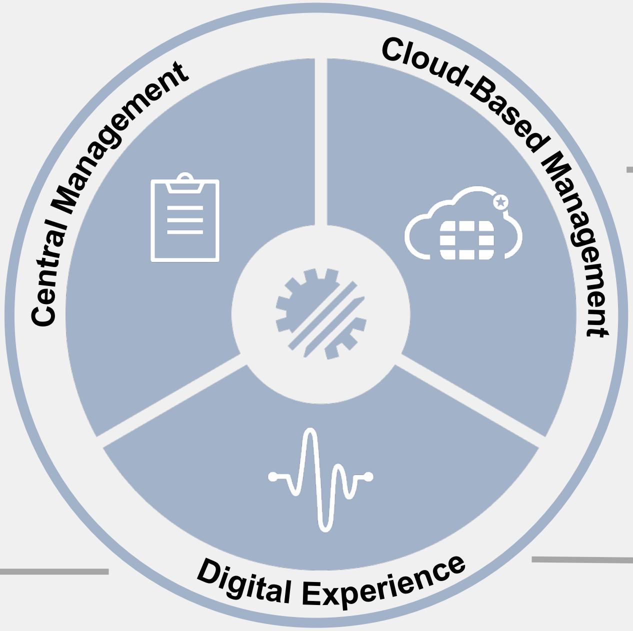
FortiSIEM
- Multi-vendor Visibility
- AI-powered Analytics
- Risk-based Response

FortiSOAR
- Multi-vendor Automation
- Process Orchestration
- Threat Intelligence Management

SOC as a Service
- Managed Firewall and Endpoint
- Alert Triage

Incident Response Service
- Identify & contain incidents
- Scope and remediate

Network Operations Portfolio



FortiManager
- Enterprise Management
- Fabric device management
- Automated workflows
- Compliance and reporting
- Fabric Partners Orchestration

FortiCloud
- SaaS-delivered Single Pane
- SMB use cases
- Multitenancy for MSSPs

Device management
FortiGate
FortiSwitch
FortiAP
FortiExtender

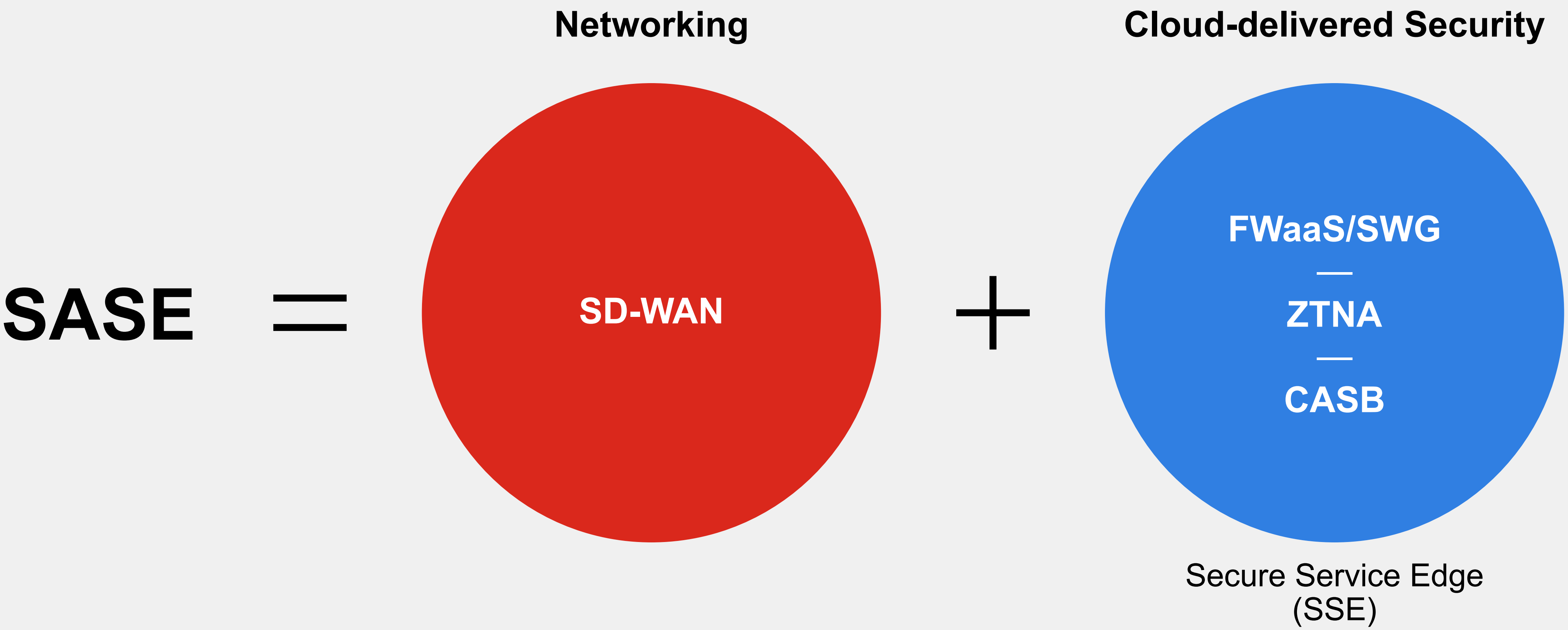
FortiMonitor
- Digital experience monitoring
- Network performance monitoring

FortiAIOps
- Anomaly detection
- Automated network troubleshooting

FortiGuard AI-Powered Security

What is SASE (Secure Access Service Edge)?

Cloud-delivered network and security convergence solution for work-from-anywhere



Networking

Cloud-delivered Security

SASE =

SD-WAN

+

FWaaS/SWG

—

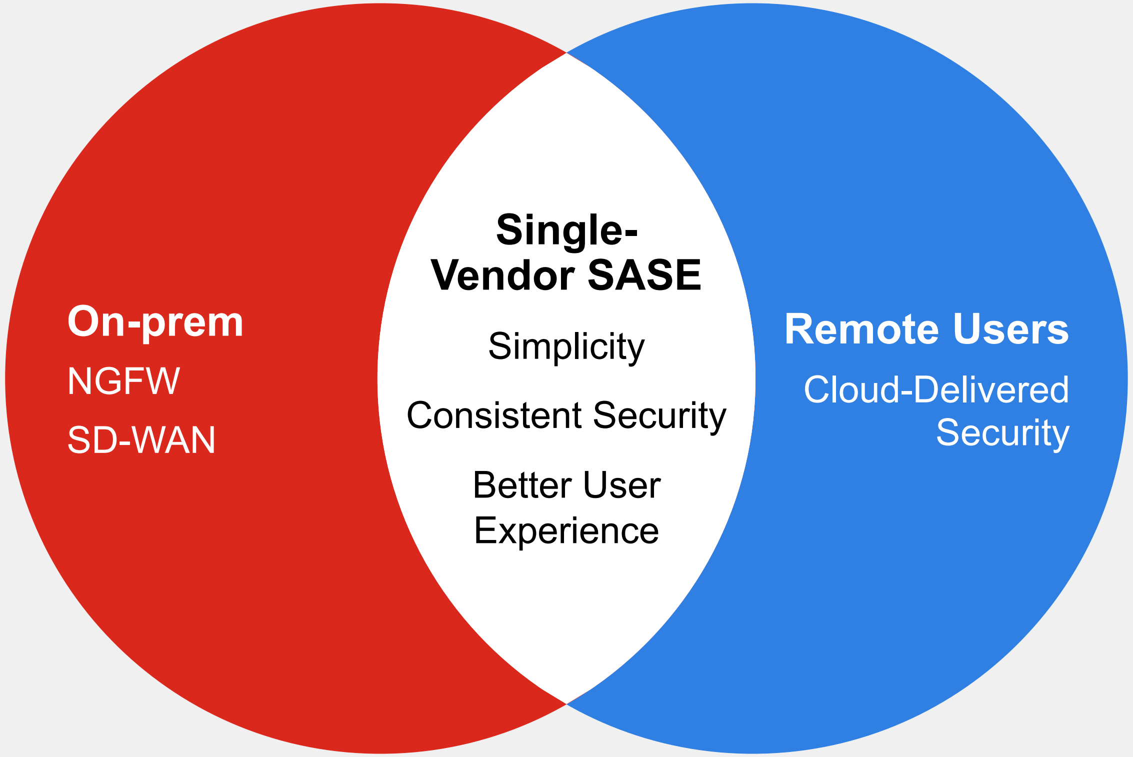
ZTNA

—

CASB

Secure Service Edge
(SSE)

Convergence of On-Prem and Remote Users Network

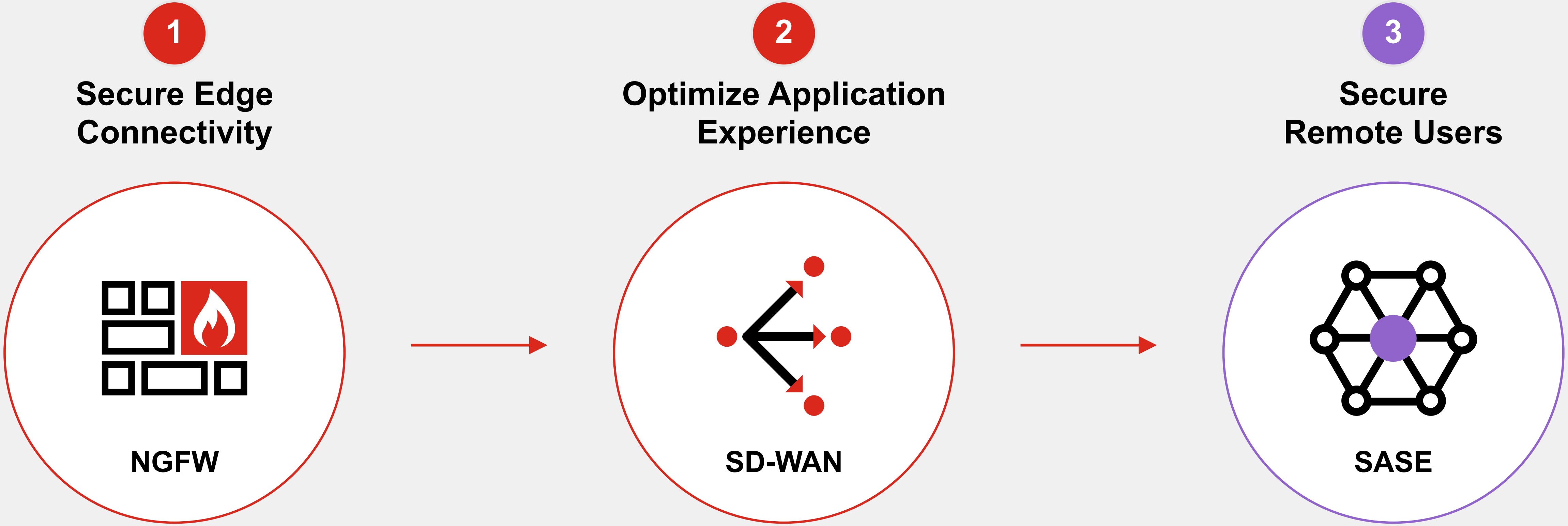


Single-vendor SASE Benefits

- Improved risk posture and reduced security gaps
- Provide simplicity eliminating multiple products
- Efficient operations with single agent
- Cost savings from product and vendor reduction

Pragmatic Journey to SASE

With Fortinet’s convergence of security and networking everywhere



1

Secure Edge Connectivity

NGFW

2

Optimize Application Experience

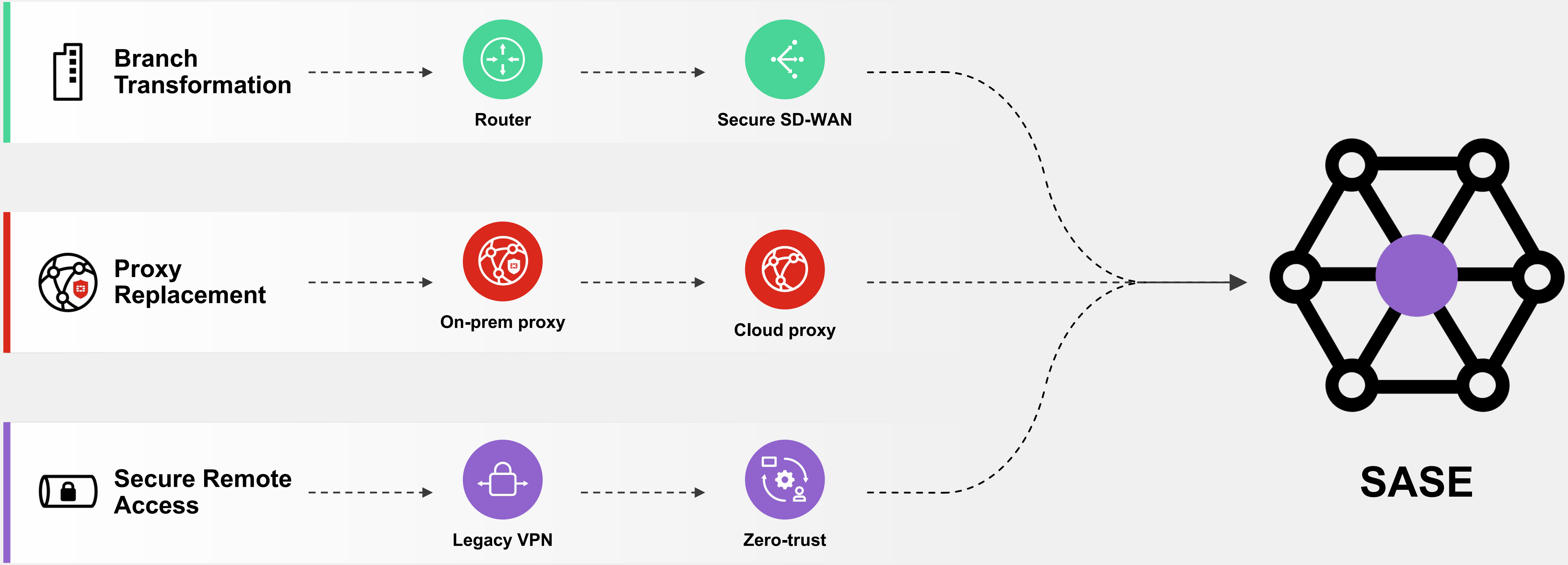
SD-WAN

3

Secure Remote Users

SASE

Key Customer Initiatives for SASE



FortiSASE

Single Vendor SASE with AI-powered Security Services

Securing Remote Users

FortiClient Unified Agent

Secure Edge

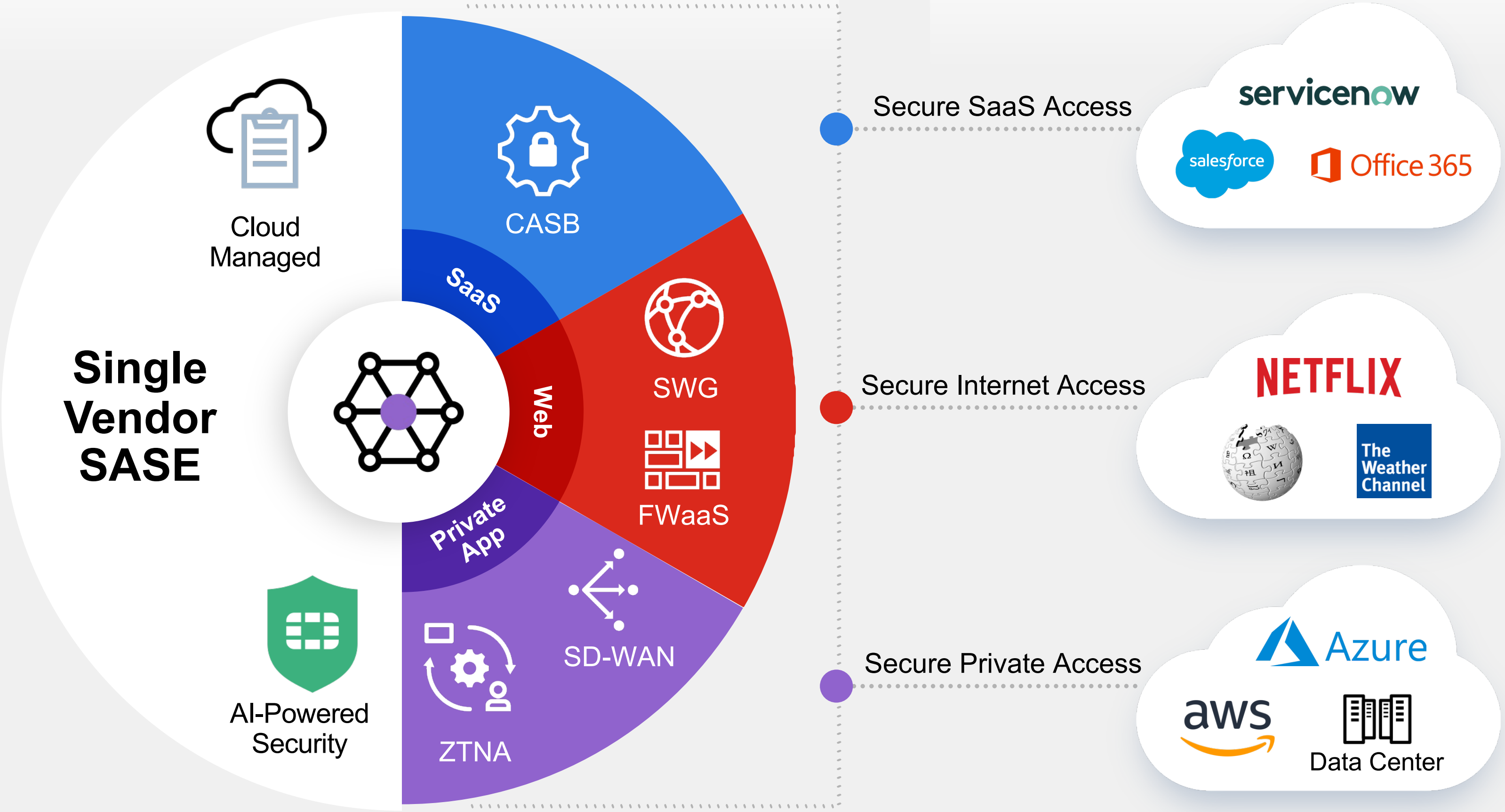
FortiGate Secure SD-WAN

MicroBranch

FortiAP FortiSwitch FortiExtender

Cloud-delivered Security & Networking

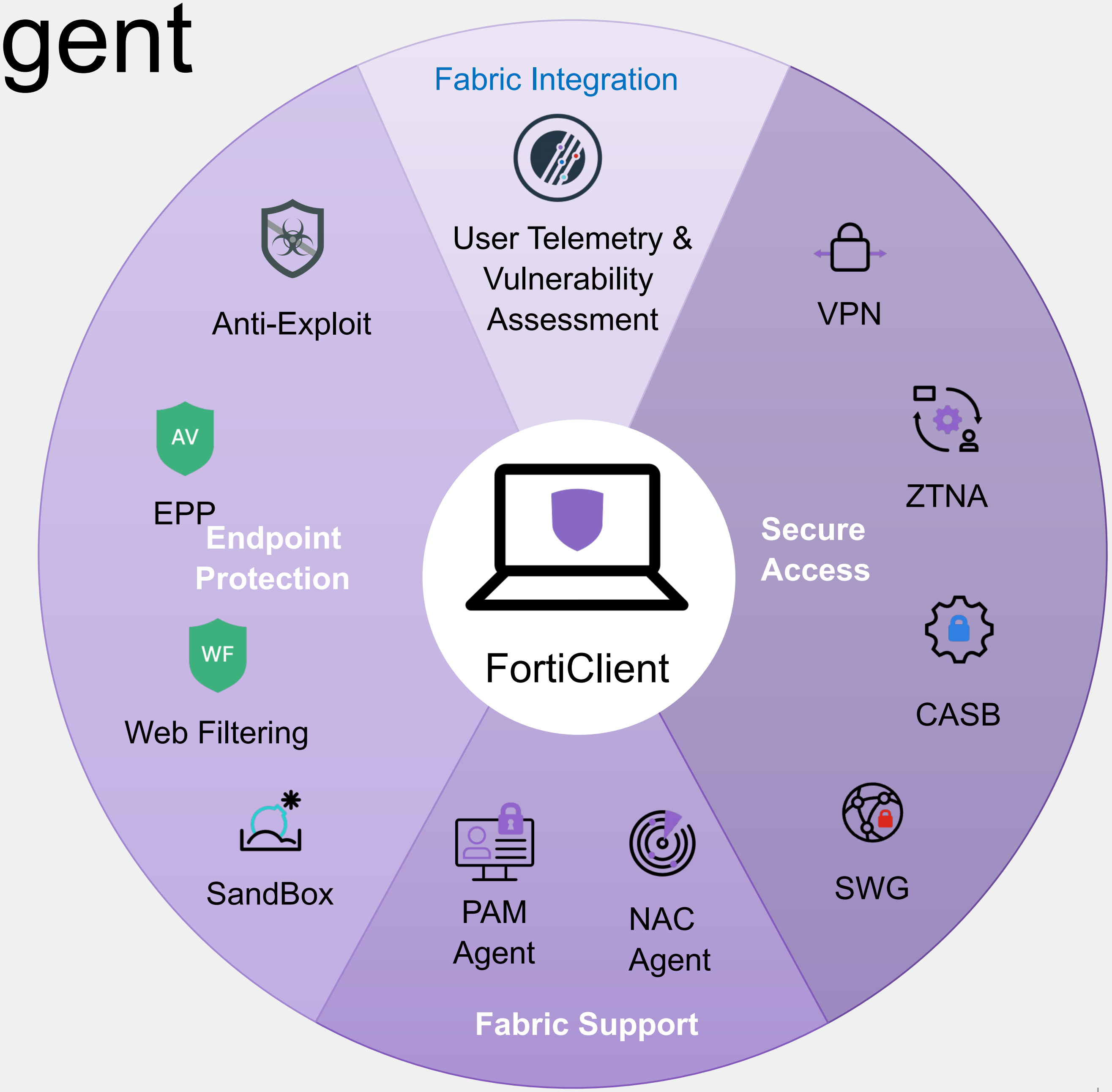
Improved User Experience



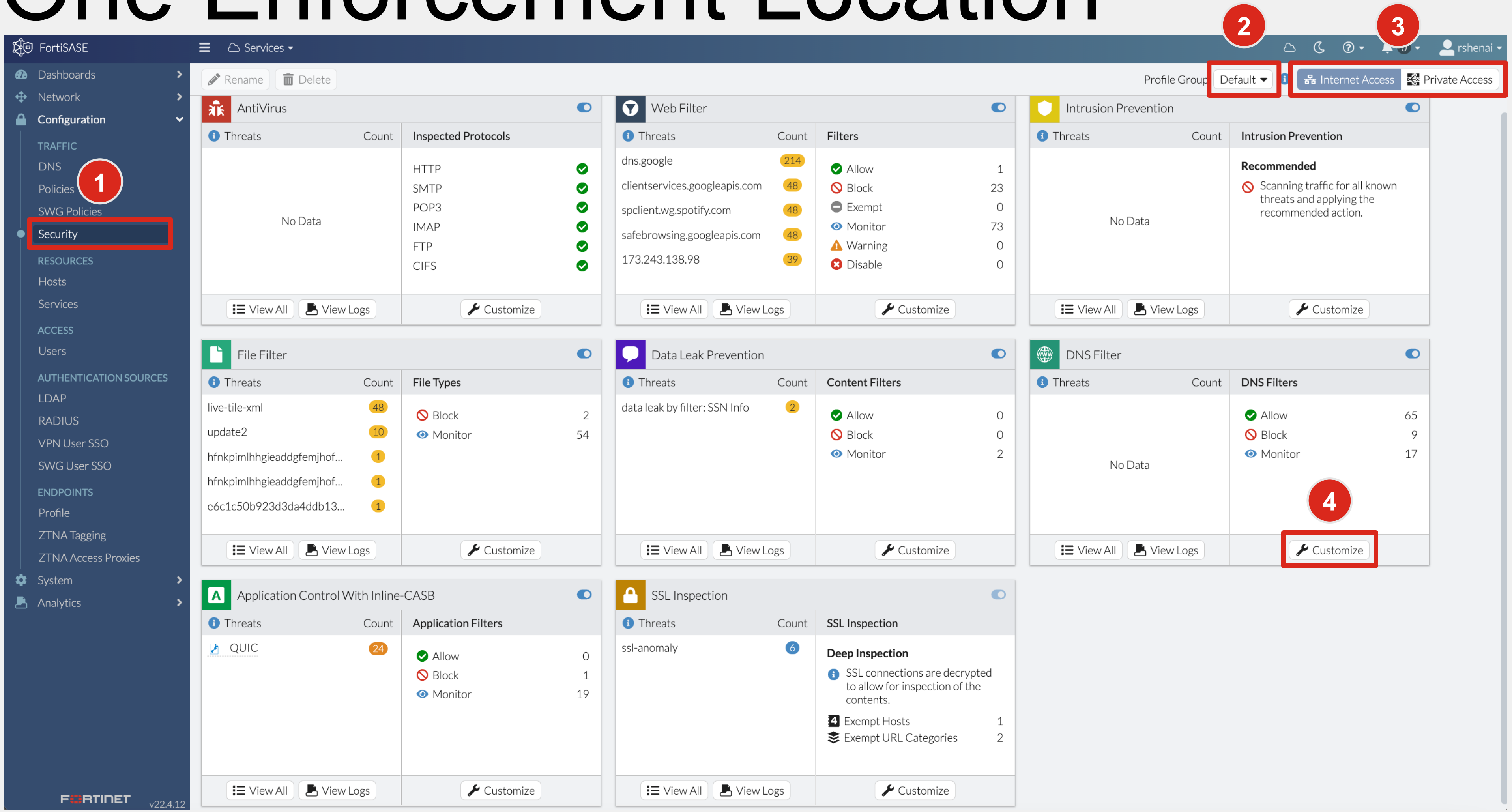
FortiClient Unified Agent

One agent to rule them all

- One agent for endpoint protection, Telemetry, PAM, NAC and Secure Access
- Client is included with SASE
- Consistent security and user experience



Security Configuration— One Enforcement Location



AntiVirus

Threats	Count
No Data	

Inspected Protocols	
HTTP	✓
SMTP	✓
POP3	✓
IMAP	✓
FTP	✓
CIFS	✓

Web Filter

Threats	Count
dns.google	214
clientservices.googleapis.com	48
spclient.wg.spotify.com	48
safebrowsing.googleapis.com	48
173.243.138.98	39

Filters	
Allow	1
Block	23
Exempt	0
Monitor	73
Warning	0
Disable	0

Intrusion Prevention

Threats	Count
No Data	

Intrusion Prevention

Recommended

Scanning traffic for all known threats and applying the recommended action.

File Filter

Threats	Count
live-tile-xml	48
update2	10
hfnkpimlhhgieaddgfemjhof...	1
hfnkpimlhhgieaddgfemjhof...	1
e6c1c50b923d3da4ddb13...	1

File Types	
Block	2
Monitor	54

Data Leak Prevention

Threats	Count
data leak by filter: SSN Info	2

Content Filters	
Allow	0
Block	0
Monitor	2

DNS Filter

Threats	Count
No Data	

DNS Filters	
Allow	65
Block	9
Monitor	17

Application Control With Inline-CASB

Threats	Count
QUIC	24

Application Filters	
Allow	0
Block	1
Monitor	19

SSL Inspection

Threats	Count
ssl-anomaly	6

SSL Inspection

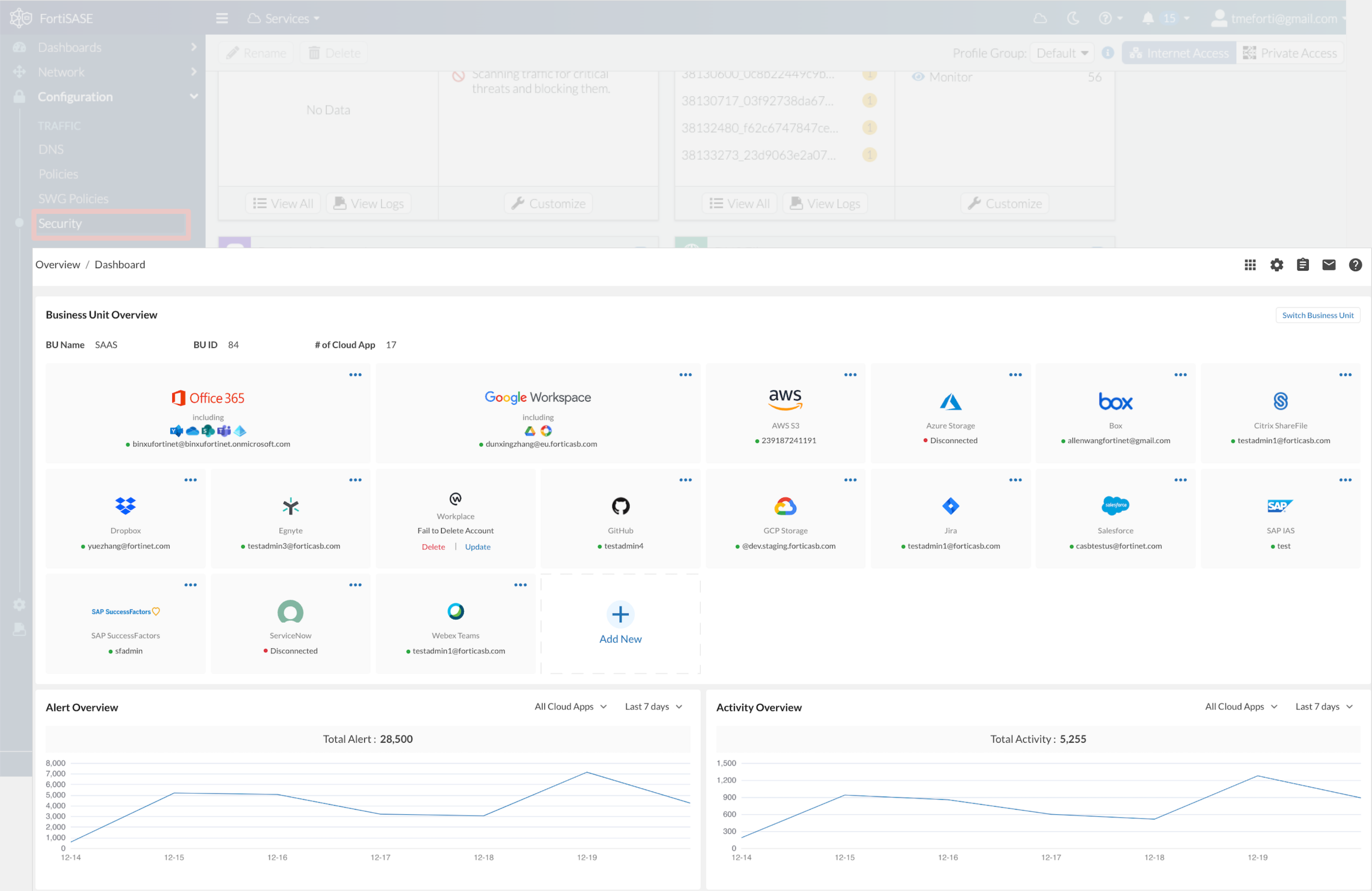
Deep Inspection

SSL connections are decrypted to allow for inspection of the contents.

Exempt Hosts	1
Exempt URL Categories	2

1. Simplified FOS Security from single pane
2. Default profiles available for fast consumption
3. Web and Private App visibility
4. Security profiles can be customized

CASB: Provides Protection for Your SaaS applications



Overview / Dashboard

Business Unit Overview

Switch Business Unit

BU Name SAAS BU ID 84 # of Cloud App 17

Application	Account / Status
Office 365 including	● binxufortinet@binxufortinet.onmicrosoft.com
Google Workspace including	● dunxingzhang@eu.forticasb.com
AWS S3	● 239187241191
Azure Storage	● Disconnected
Box	● allenwangfortinet@gmail.com
Citrix ShareFile	● testadmin1@forticasb.com
Dropbox	● yuezhang@fortinet.com
Egnyte	● testadmin3@forticasb.com
Workplace	Fail to Delete Account Delete | Update
GitHub	● testadmin4
GCP Storage	● @dev.staging.forticasb.com
Jira	● testadmin1@forticasb.com
Salesforce	● casbtestus@fortinet.com
SAP IAS	● test
SAP SuccessFactors	● sfadmin
ServiceNow	● Disconnected
Webex Teams	● testadmin1@forticasb.com

Add New

Alert Overview All Cloud Apps Last 7 days

Total Alert : 28,500

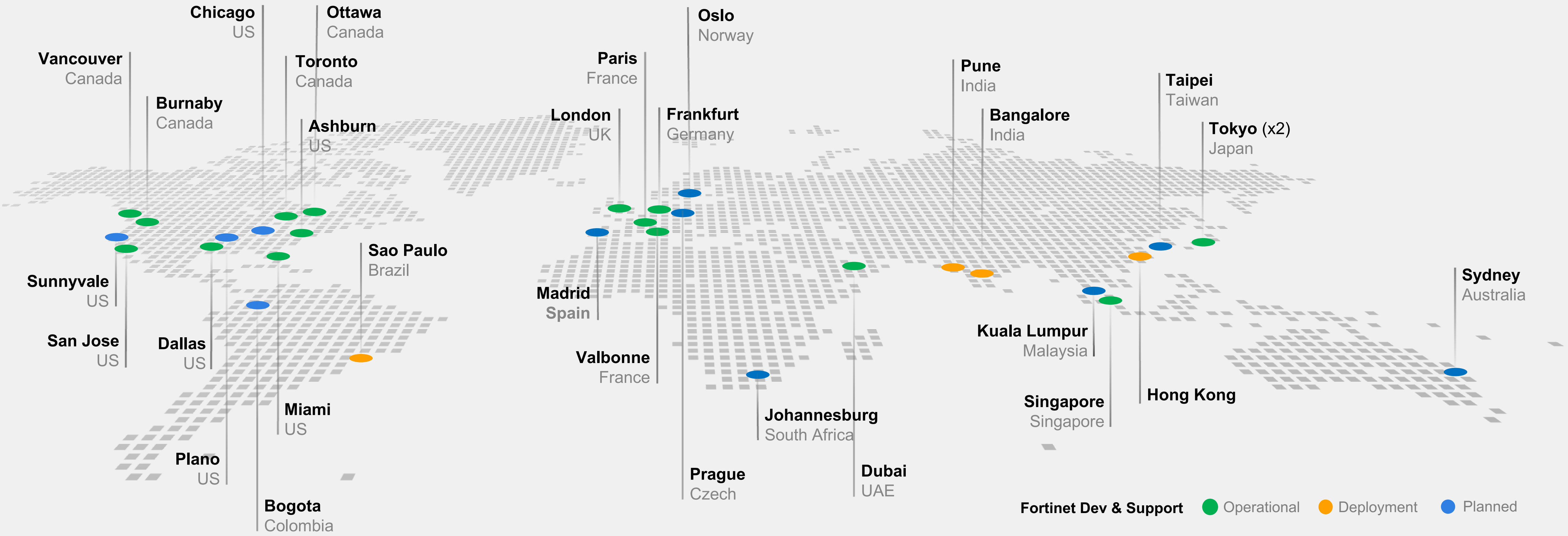
Activity Overview All Cloud Apps Last 7 days

Total Activity : 5,255

- Application status
- Activity history
- Risk statistics
- Highest risk users, files, triggered policies & countries
- Risk/usage trends

FortiSASE PoP Coverage Expanding Rapidly

85% of US and EMEA regions already have acceptable latency based on our current PoP coverage



Global coverage

Global theatres

23 active datacenters

Rapid roll out

4 imminent launches

Tactical locations

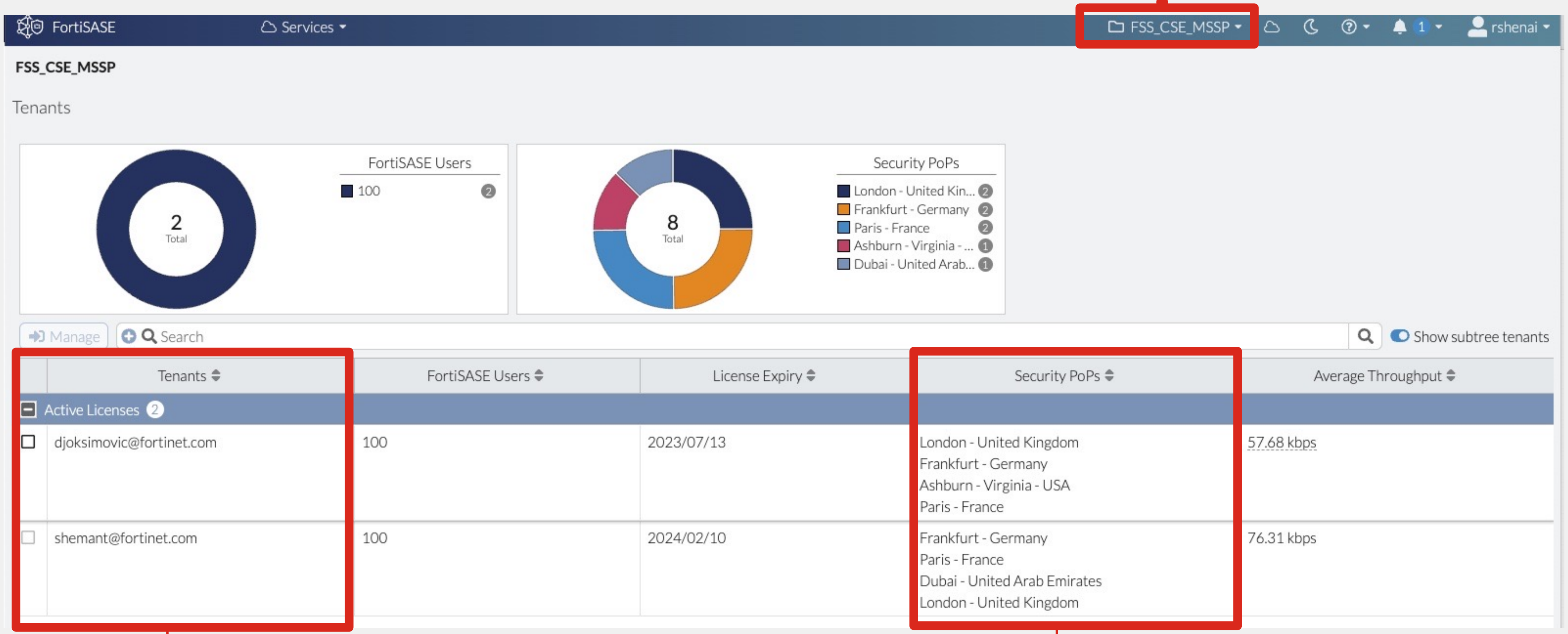
40 datacenters in 2024

Regional coverage

FortiSASE Multi-Tenancy Support

MSSP Portal

Parent Tenant / SP/ MSSP



FSS_CSE_MSSP

Tenants

FortiSASE Users	
🟦 100	2

2 Total

Security PoPs	
London - United Kin...	2
Frankfurt - Germany	2
Paris - France	2
Ashburn - Virginia - ...	1
Dubai - United Arab...	1

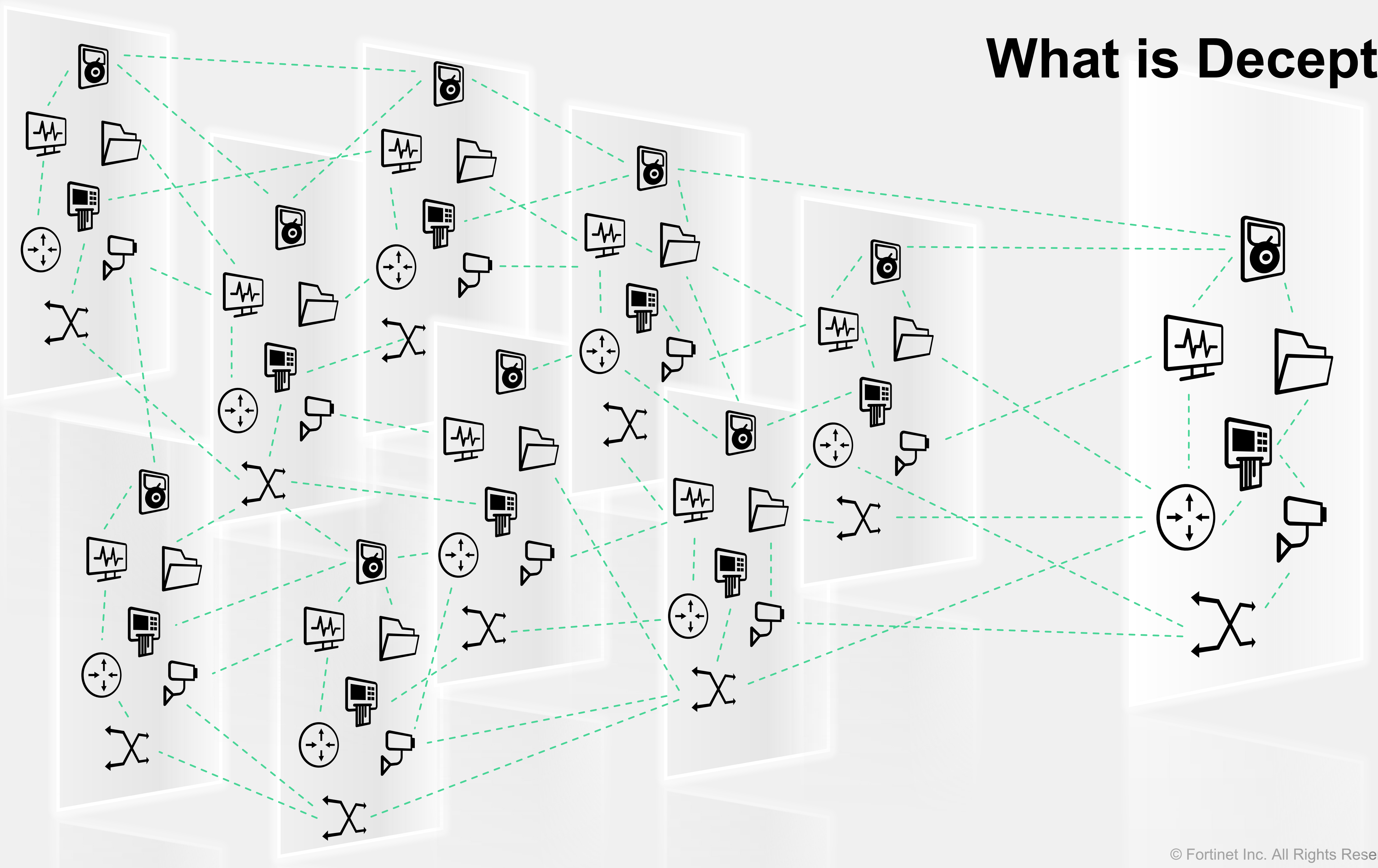
8 Total

	Tenants ⇕	FortiSASE Users ⇕	License Expiry ⇕	Security PoPs ⇕	Average Throughput ⇕
⊟	Active Licenses 2				
□	djoksimovic@fortinet.com	100	2023/07/13	London - United Kingdom Frankfurt - Germany Ashburn - Virginia - USA Paris - France	57.68 kbps
□	shemant@fortinet.com	100	2024/02/10	Frankfurt - Germany Paris - France Dubai - United Arab Emirates London - United Kingdom	76.31 kbps

Child Tenants

SASE PoPs per Customer/ Tenant

What is Deception?



What is Deception?

Diverting attackers to fake assets to protect enterprises' real assets

Decoys
Fake assets, fake network devices, fake applications and fake services

Lures
Fake services of the honeypots/decoys

Network traffic
Fake network traffic beaconing (SMB,CDP, UPnP, and more)

Breadcrumbs (tokens)
Fake resources placed on real IT assets and point to the fake systems

Prioritize alerts from the deception

High-fidelity alerts that require your immediate attention

Honeypots vs Deception

Deception — Much More Than a Honeypot

	Traditional Honeypots	Deception Technology
Authenticity	◔	●
Ease of deployment and operation	◔	●
Scalability	○	●
Interaction	◔	●
Capture Lateral Movement	○	●
Automated Threat Response	○	●

FortiDeceptor Technology

Technology Overview

An advanced threat deception designed to DECEIVE, EXPOSE, and ELIMINATE external and internal threats early in the attack kill chain and proactively block these threats before any significant damage occurs.

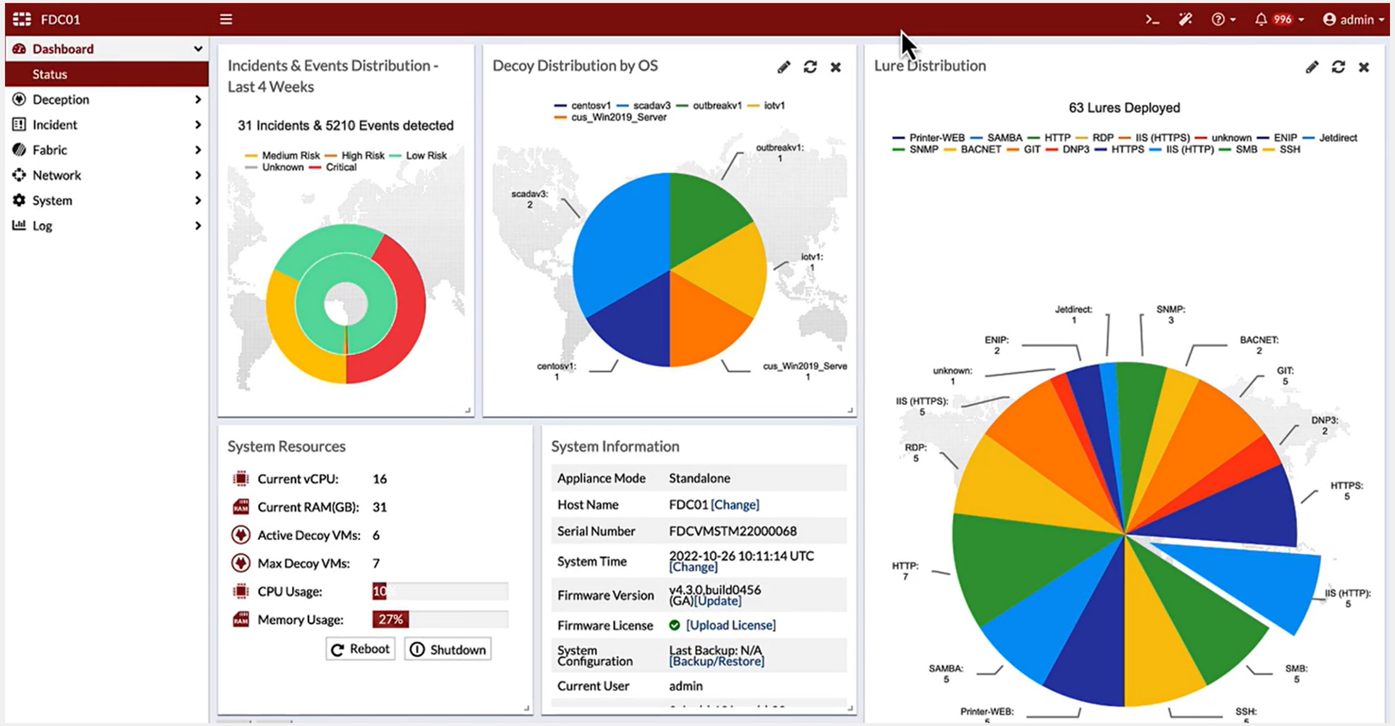
FortiDeceptor
Advanced Threat Deception

HW Appliance

Virtual Appliance

Fabric Integration:

- FortiGate
- FortiSIEM
- FortiNAC
- FortiAnalyzer
- FortiSandbox
- FortiSOAR
- FortiEDR
- Third-Party



Incidents & Events Distribution - Last 4 Weeks

31 Incidents & 5210 Events detected

Decoy Distribution by OS

Lure Distribution

63 Lures Deployed

System Resources

Current vCPU: 16
Current RAM(GB): 31
Active Decoy VMs: 6
Max Decoy VMs: 7
CPU Usage: 10%
Memory Usage: 27%

System Information

Appliance Mode	Standalone
Host Name	FDC01 [Change]
Serial Number	FDCVMSTM22000068
System Time	2022-10-26 10:11:14 UTC [Change]
Firmware Version	v4.3.0.build0456 (GA)[Update]
Firmware License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin

Overview – FortiDeceptor Decoys, Lures, and Tokens

Local Windows Decoys

- Windows 7
- Windows 10

Custom Windows Decoys

- Windows 7
- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- RedHat Enterprise Linux 7.9

Windows Lures/Tokens

- SMB
- RDP
- SMTP
- ICMP
- FTP
- TCP Port Listener
- NBNSSpoofSpotter
- SWIFT Lite 2
- SQL (MS-Server)
- Cache Credentials
- SQL ODBC
- SAP Connector
- HoneyDocs (Office / PDF / Excel)

VPN Decoys

- FortiOS

VPN Lures

- SSLVPN

Linux Decoys

- Ubuntu 16.0.4
- Ubuntu 18.0.4
- CentOS
- MacOS
- Outbreak Alerts

Linux Lures/Tokens

- SSH
- SAMBA
- TCP Port Listener
- ICMP
- Radius
- FTP
- ESXi
- ELK
- GIT
- MariaDB (MySQL)
- Tomcat (Webserver)
- SCADABR (MGMT)

IoT Decoys

- Cisco Router
- TP-Link Router
- IP Camera
- Printers (HP, LX, BR)
- UPS
- SWIFT VPN Gateway

VoIP Decoys

- SIP
- XMPP
- MQTT
- 4G/5G-3GPP

Application Decoys

- SAP
- ERP
- POS

Cloud Decoys

Azure

aws

Google Cloud

Medical Decoys

- PACS / Infusion Pump
- DICOM
- SPACECOM
- INFUSOMAT (Braun)

OT Decoys

- Schneider Electric
  - Modicon M241
  - PowerMeter PM-5560
  - EcoStrucure BMS Server
  - SCADAPack 333E
- Siemens
  - S7-200 PLC
  - S7-300 PLC
  - S7-1500 PLC
- Rockwell Automation
  - Rockwell PLC
  - 1769-L16ER/B LOGIX5316ER
  - 1769-L35E Ethernet Port
- Niagara
  - Niagara4 Station
  - NiagaraAX Station
- Phoenix Contact AXC 1050
- MOXA NPORT 5110
- GUARDIAN-AST
- GE PLC 90 (SRTP)
- Liebert Spruce UPS
- VAV-DD BACnet controller
- Kamstrup 382
- Ascent Compass MNG
- IPMI Device
- Modicon M580
- PowerLogic ION7650
- Emerson iPro by Dixell
- C-More HMI

OT Lures

- HTTP/HTTPS
- FTP
- TFTP
- SNMP
- TELNET
- MODBUS
- S7COMM
- BACNET
- IPMI
- MOXA
- TRICONEX
- ENIP (EtherNet/IP)
- DNP3
- IEC 60870-5-104
- PROFINET
- KAMSTRUP
- Guardon-AST

Schneider Electric

SIEMENS

Rockwell Automation

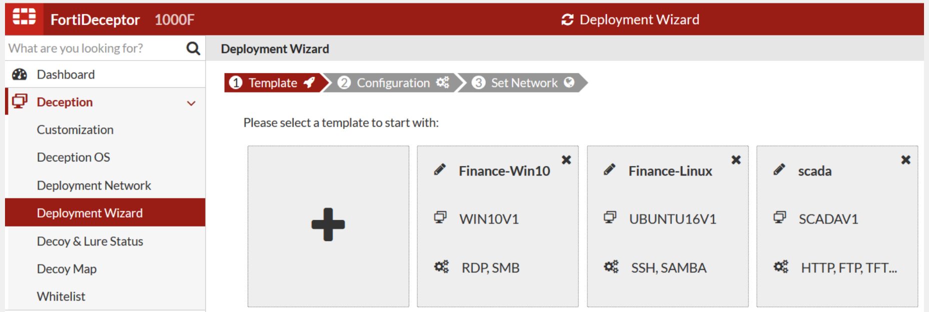
TRIDIUM

VERTIV

General Electric

FortiDeceptor: LifeCycle

Deceive



FortiDeceptor 1000F | Deployment Wizard

What are you looking for?

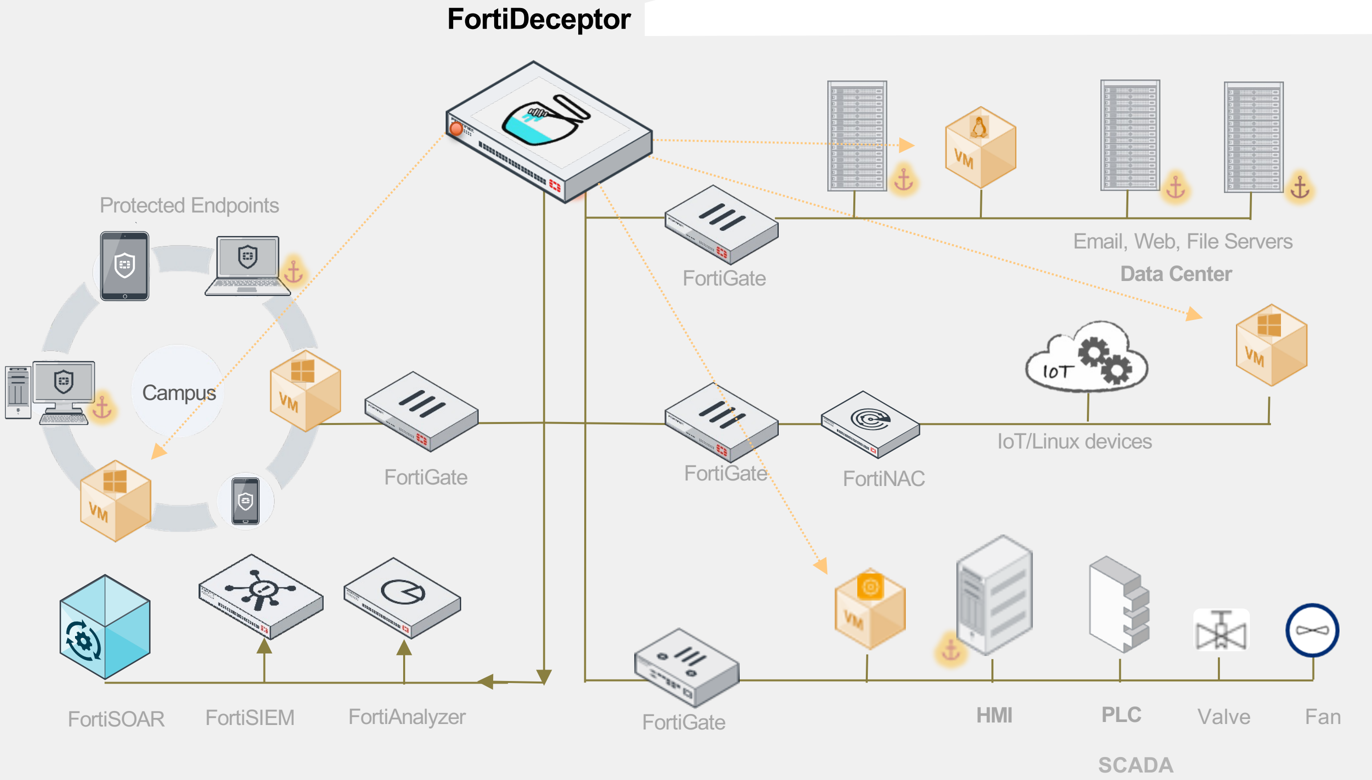
- Dashboard
- Deception
  - Customization
  - Deception OS
  - Deployment Network
  - Deployment Wizard
  - Decoy & Lure Status
  - Decoy Map
  - Whitelist

Deployment Wizard

1 Template › 2 Configuration › 3 Set Network

Please select a template to start with:

Template	OS	Services
Finance-Win10	WIN10V1	RDP, SMB
Finance-Linux	UBUNTU16V1	SSH, SAMBA
scada	SCADAV1	HTTP, FTP, TFT...

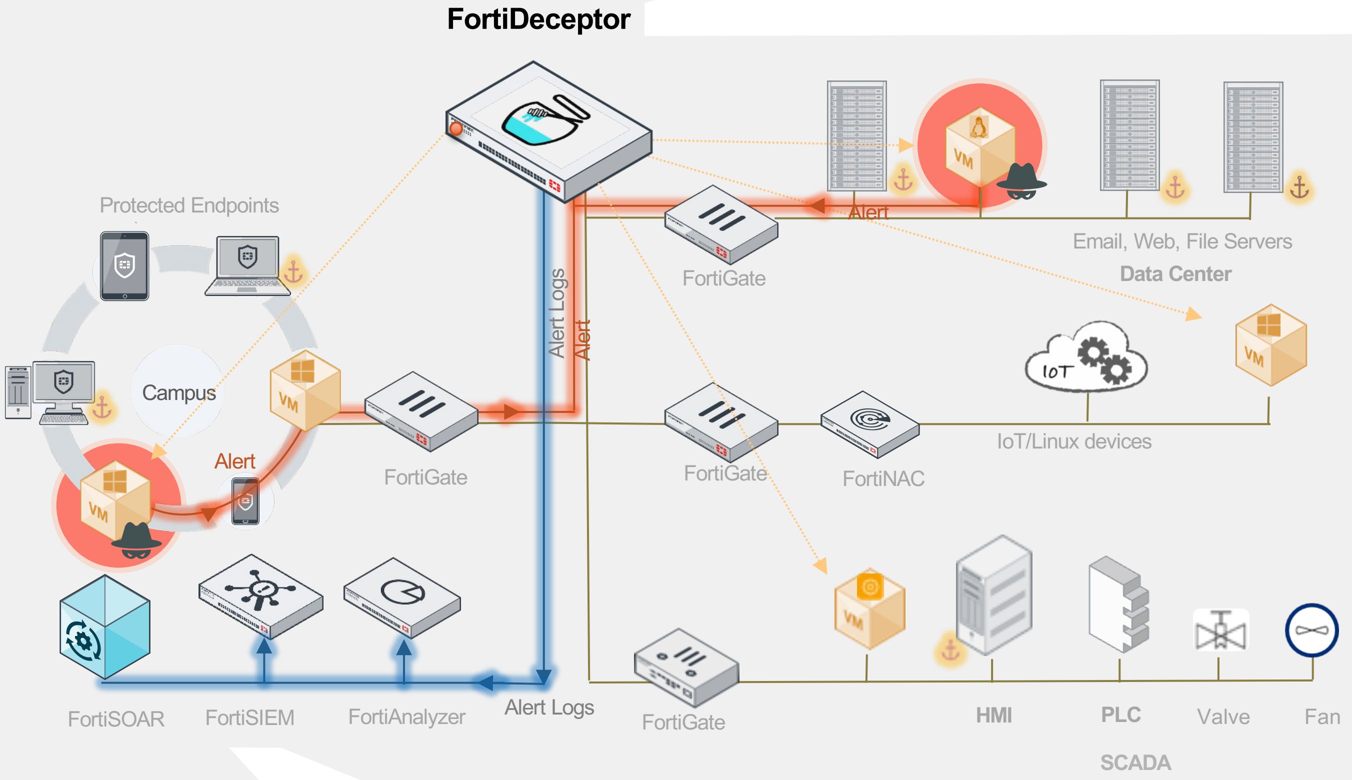


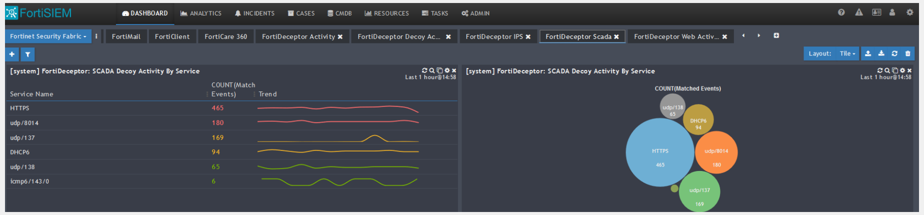
- Lure attackers to decoys that appear indistinguishable from real IT and OT assets and are highly interactive
- Centrally manage and automate the deployment of decoy VMs (Windows, Linux, ICS/SCADA) and generation of lures (data, application /services*)

OT Lures: MODBUS, S7-200, IPMI, Bacnet, Triconex, Guardian-AST, IEC104, ENIP
IoT Lures: Medical PACS, DICOM, infusion pump, ERP, POS, GIT
IT Lures: SSL VPN, RDP, SMB, SQL, SSH, SAMBA, etc

FortiDeceptor: LifeCycle

Deceive > Expose





[system] FortiDeceptor: SCADA Decoy Activity By Service

Last 1 hour@14:58

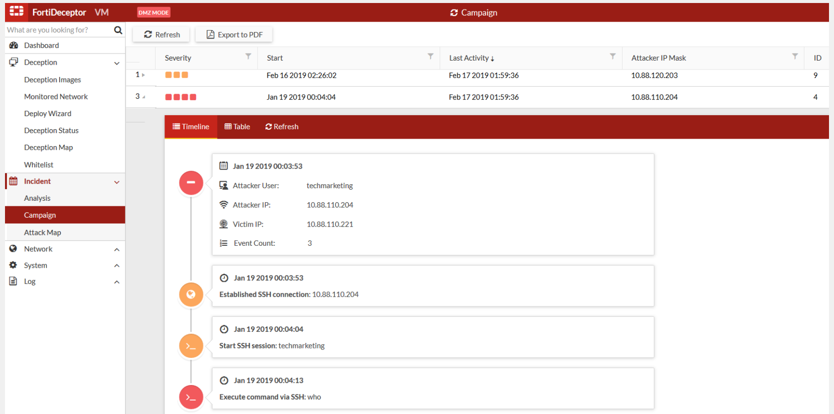
Service Name	COUNT(Match Events)	Trend
HTTPS	465	
udp/8014	180	
udp/137	169	
DHCP6	94	
udp/138	65	
icmp6/143/0	6	

[system] FortiDeceptor: SCADA Decoy Activity By Service

Last 1 hour@14:58

COUNT(Matched Events)

udp/138	65
DHCP6	94
HTTPS	465
udp/8014	180
udp/137	169



	Severity	Start	Last Activity ↓	Attacker IP Mask	ID
1 ▸	🟧🟧🟧	Feb 16 2019 02:26:02	Feb 17 2019 01:59:36	10.88.120.203	9
3 ◢	🟥🟥🟥🟥	Jan 19 2019 00:04:04	Feb 17 2019 01:59:36	10.88.110.204	4

Jan 19 2019 00:03:53
Attacker User: techmarketing
Attacker IP: 10.88.110.204
Victim IP: 10.88.110.221
Event Count: 3

Jan 19 2019 00:03:53
Established SSH connection: 10.88.110.204

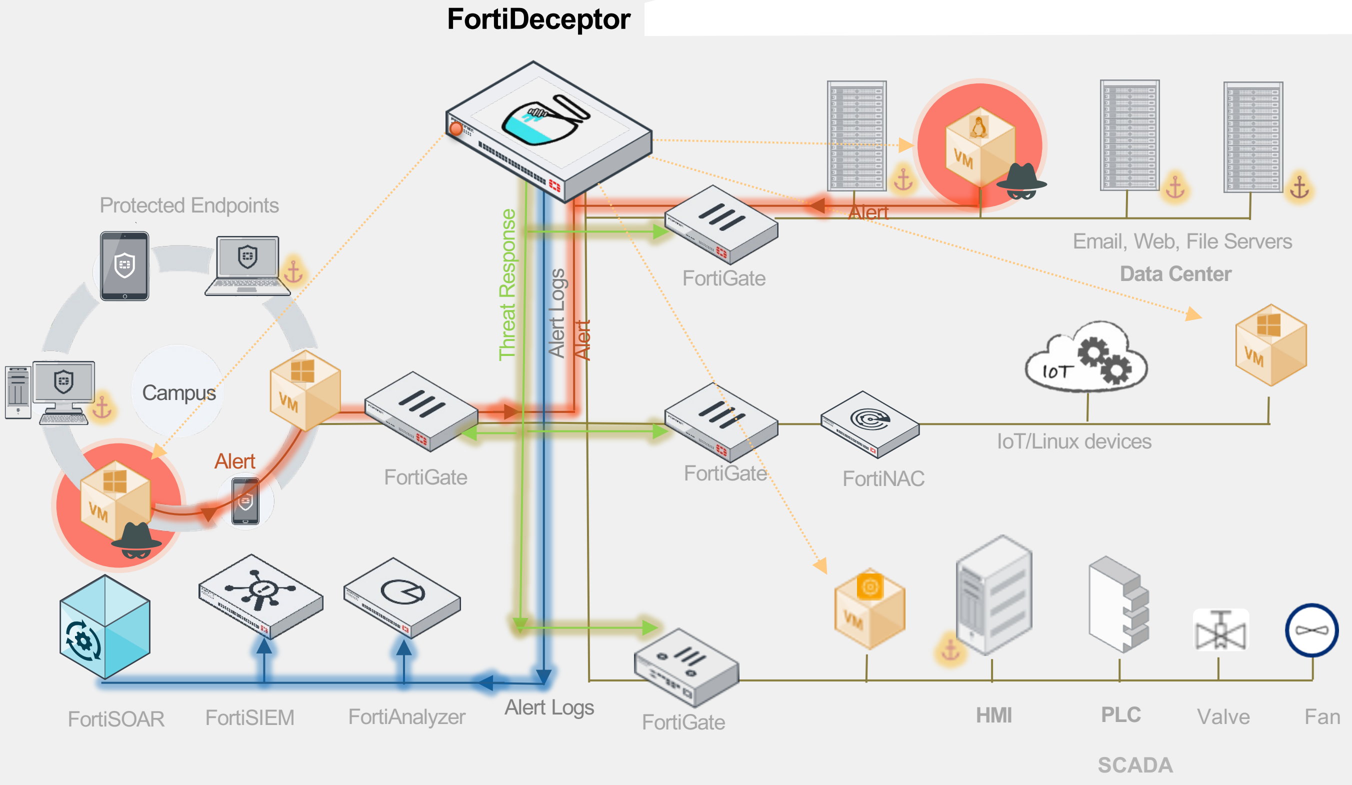
Jan 19 2019 00:04:04
Start SSH session: techmarketing

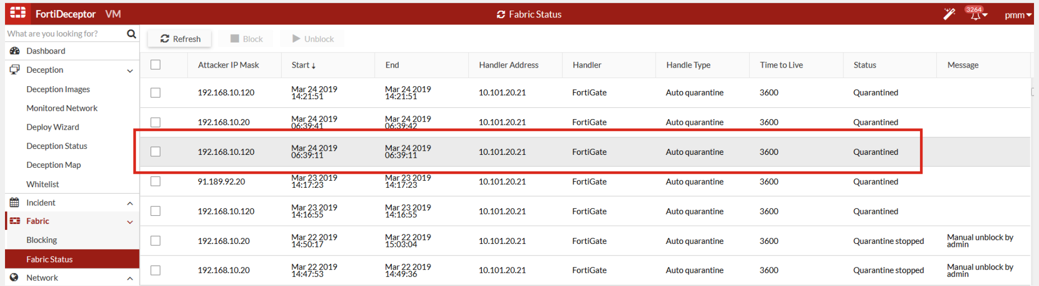
Jan 19 2019 00:04:13
Execute command via SSH: who

- Acts as an early warning system that generates alerts for review and validation
- Consolidate detection and correlation of external and internal actor activities into a single pane view of threat campaign

FortiDeceptor: LifeCycle

Deceive > Expose > Eliminate





□	Attacker IP Mask	Start ↓	End	Handler Address	Handler	Handle Type	Time to Live	Status	Message
□	192.168.10.120	Mar 24 2019 14:21:51	Mar 24 2019 14:21:51	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
□	192.168.10.20	Mar 24 2019 06:39:41	Mar 24 2019 06:39:42	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
□	192.168.10.120	Mar 24 2019 06:39:11	Mar 24 2019 06:39:11	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
□	91.189.92.20	Mar 23 2019 14:17:23	Mar 23 2019 14:17:23	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
□	192.168.10.120	Mar 23 2019 14:16:55	Mar 23 2019 14:16:55	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
□	192.168.10.20	Mar 22 2019 14:50:17	Mar 22 2019 15:03:04	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantine stopped	Manual unblock by admin
□	192.168.10.20	Mar 22 2019 14:47:53	Mar 22 2019 14:49:36	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantine stopped	Manual unblock by admin

- Manual/Automatic severity-based blocking of attackers before any real damage occurs
- Fabric integration
  - FortiGate: Quarantine IP address
  - FortiNAC: Isolate devices
  - FortiSOAR: Trigger playbooks
  - FortiSIEM: Visibility and threat hunting
  - 3rd Party: Fabric Connector

Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

Product Matrix

Click on icons in this document for additional information

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiOS
The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiProxy
Enforce internet, compliance and granular application control

FortiIsolator
Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDOS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiMail
Secure mail getaway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

FortiCNF
Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

FortiSASE
Enforce dynamic network access control and network segmentation

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiGuest
Simplified guest access, BYOD, and policy management

FortiPAM
Control & monitoring of elevated & privileged accounts, processes, and critical systems

FortiGuard Threat Intelligence

Powered by FortiGuard Labs

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud
Saas w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage and customize LTE internet access

FNDN
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOp Tools & Script
Fortinet & community-driven

Fabric API Integration
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiRecon
Digital Risk Protection (DRP) for early, actionable warning and fast response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
15% of hardware

FortiCare Premium*
20% of hardware

FortiCare Elite**
25% of hardware

FortiConverter
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for ForiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

FortiFone
Robust IP Phones w/ HD Audio with centralized management

FortiVoice
Integrated voice, chat, conferencing management, and fax with centralized

FortiCamera
HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
High-performance NVR with AI-powered video management software

FORTINET®