



A secure Journey into the Cloud

Maximilian Schiffner

Systems Engineer, Austria



Company Overview



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.

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

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+

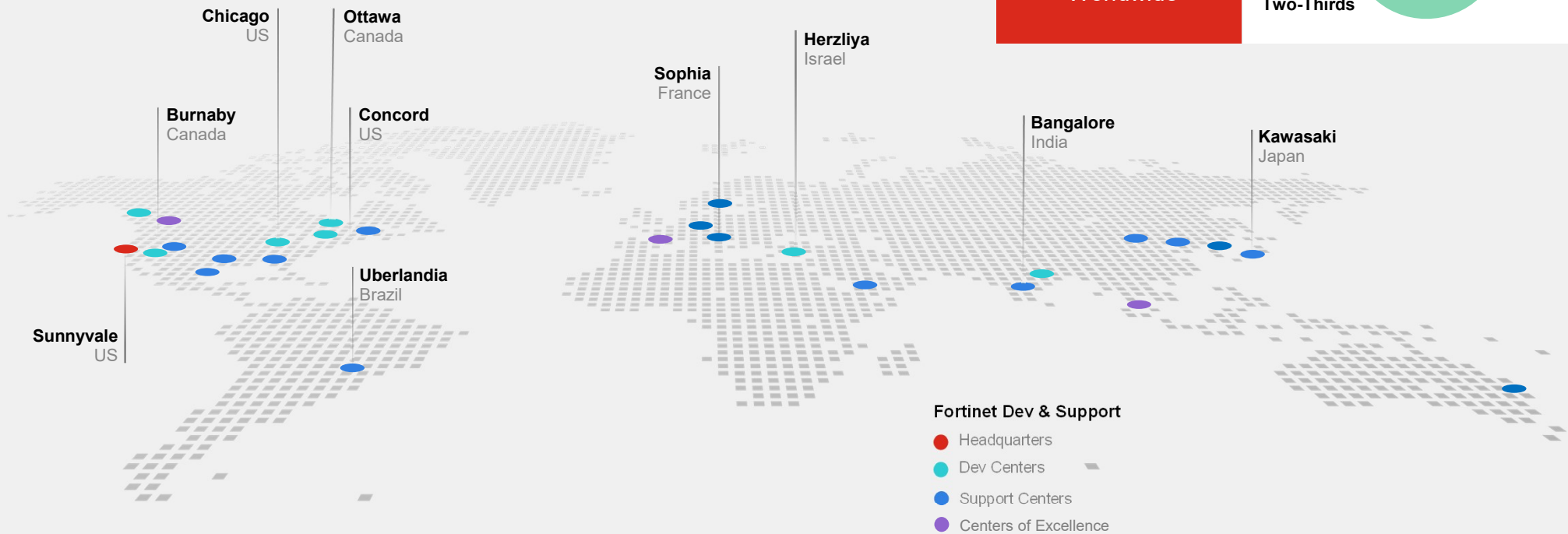
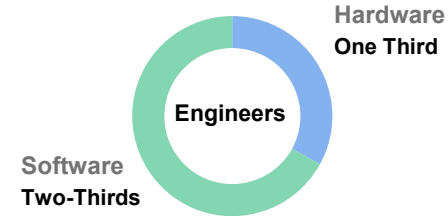
Investment in ASIC Design & Development



Global Reach & Support

Majority of our R&D is based in North America

13,600+
Employees
Worldwide



Enterprise “Best of Breed” & “Platform” Are Not Mutually Exclusive

Secure
Networking



Network Firewall

Dec 2022 Magic Quadrant for Network Firewalls

Fortinet Recognized as a Leader



SD-WAN

Sept 2022 Magic Quadrant for SD-WAN

Fortinet Recognized as a Leader



Wired and Wireless LAN

Nov 2022 Magic Quadrant for Wired and Wireless LAN

Fortinet Recognized as a Visionary



SASE

Aug 2023 Magic Quadrant for Single-Vendor SASE

Fortinet Recognized as a Challenger



FortiOS Operating System



Internal Use Only

© Fortinet Inc. All Rights Reserved.

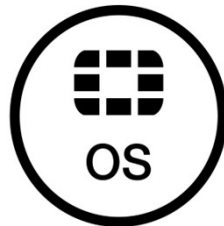
5

The Fortinet Advantage



Security Processors

Superior NGFW and
SD-WAN performance
and efficiency



FortiOS

Ties all the Security Fabric's
security and networking
components together



Security Fabric

Organically developed, highly
integrated and automated
cybersecurity platform



Ecosystem

300+ partners
500+ integrations



Fortinet Security Fabric

Broad

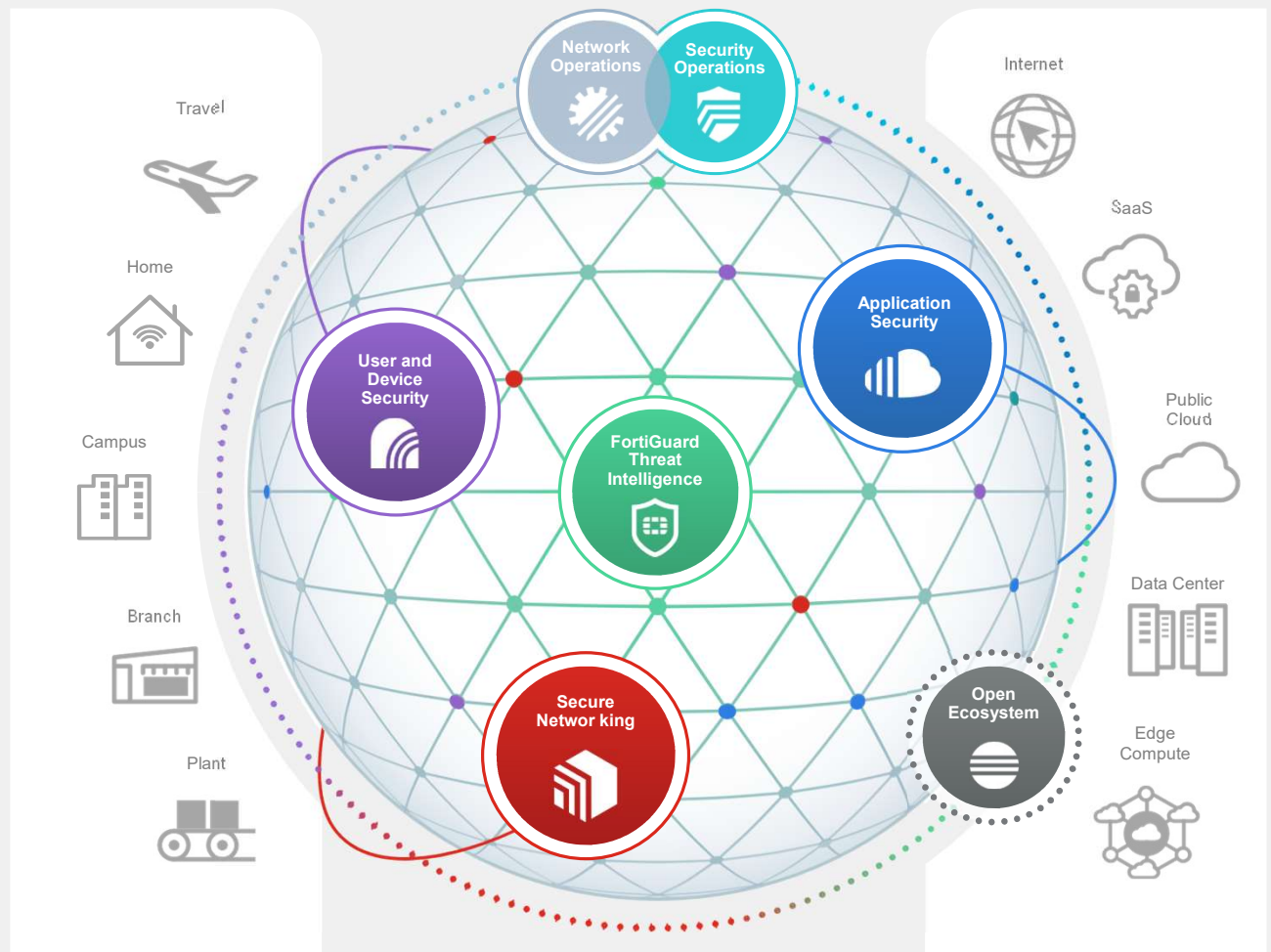
visibility and protection of the entire digital attack surface to better manage risk

Integrated

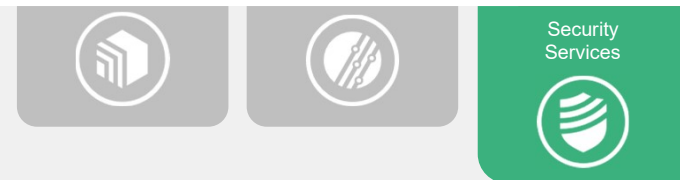
solution that reduces management complexity and shares threat intelligence

Automated

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



FortiGuard Labs Overview



VISIBILITY

Telemetry
Network
Web
Sandbox
Email
Endpoint

CERTs

Enforcement Partnerships

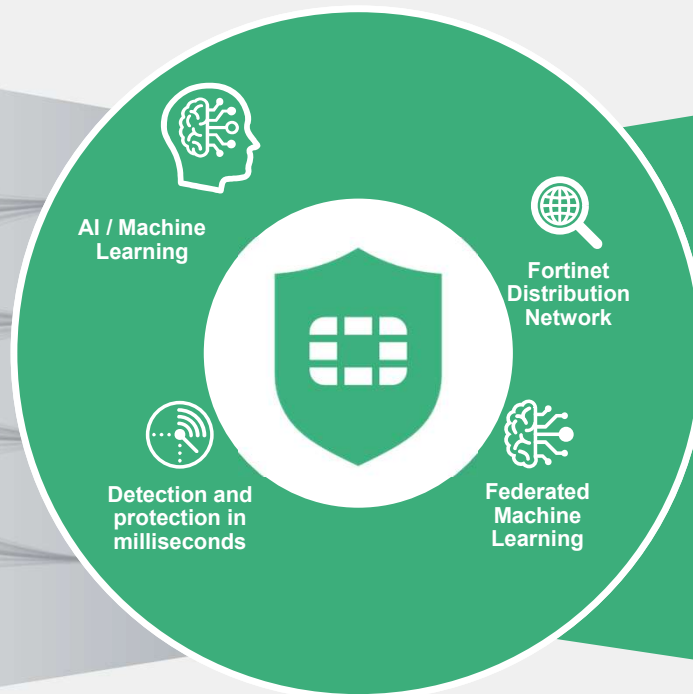
Zero-Day

OSINT

CTA feeds

Trusted Partnerships

INNOVATION



FortiGuard Labs

ACTIONABLE THREAT INTELLIGENCE

FORTIGUARD AI-POWERED SECURITY

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**
Detailed Threat Analysis **Architecture Evaluation** **Cybersecurity Workshops**





Secure Networking

NGFW, SD-WAN, SASE

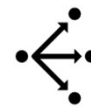


Fabric Solution: Secure Networking



Network Firewall

Comprehensive, integrated, and automated cybersecurity solution



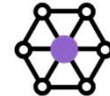
Secure SD-WAN & 5G

Transform and secure WAN, enhancing user experience and mitigating risk.



Secure Wireless & Wired LAN

Wi-Fi and Ethernet network equipment secured by a cybersecurity mesh



Secure Access Services Edge (SASE)

Cloud-delivered security and superior user experience for remote users



AI-powered Security Services

Counter threats in real-time with AI-powered protection natively integrated into the Fabric



[Go Back](#)

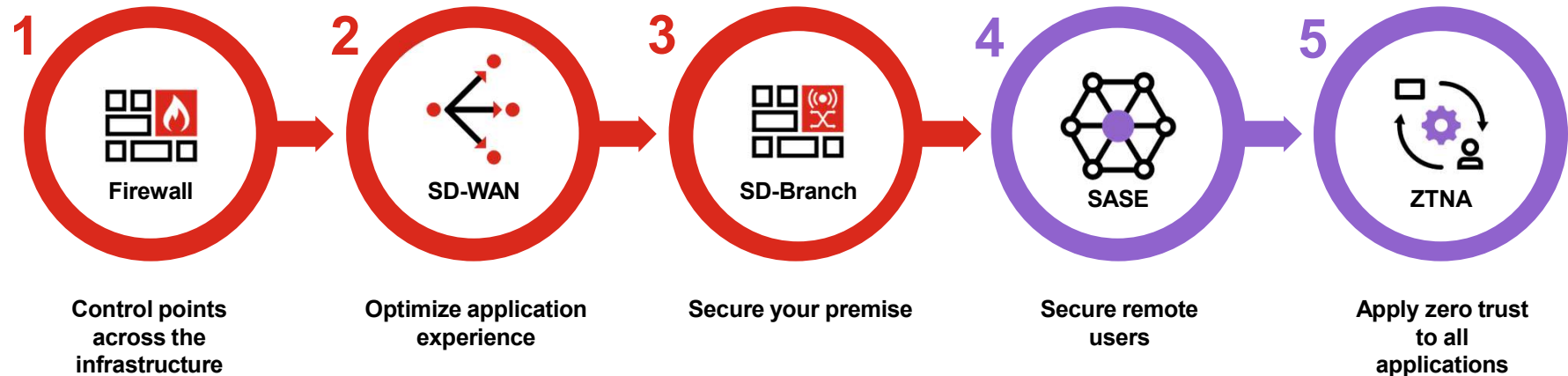
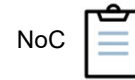
[End](#)

© Fortinet Inc. All Rights Reserved.

10

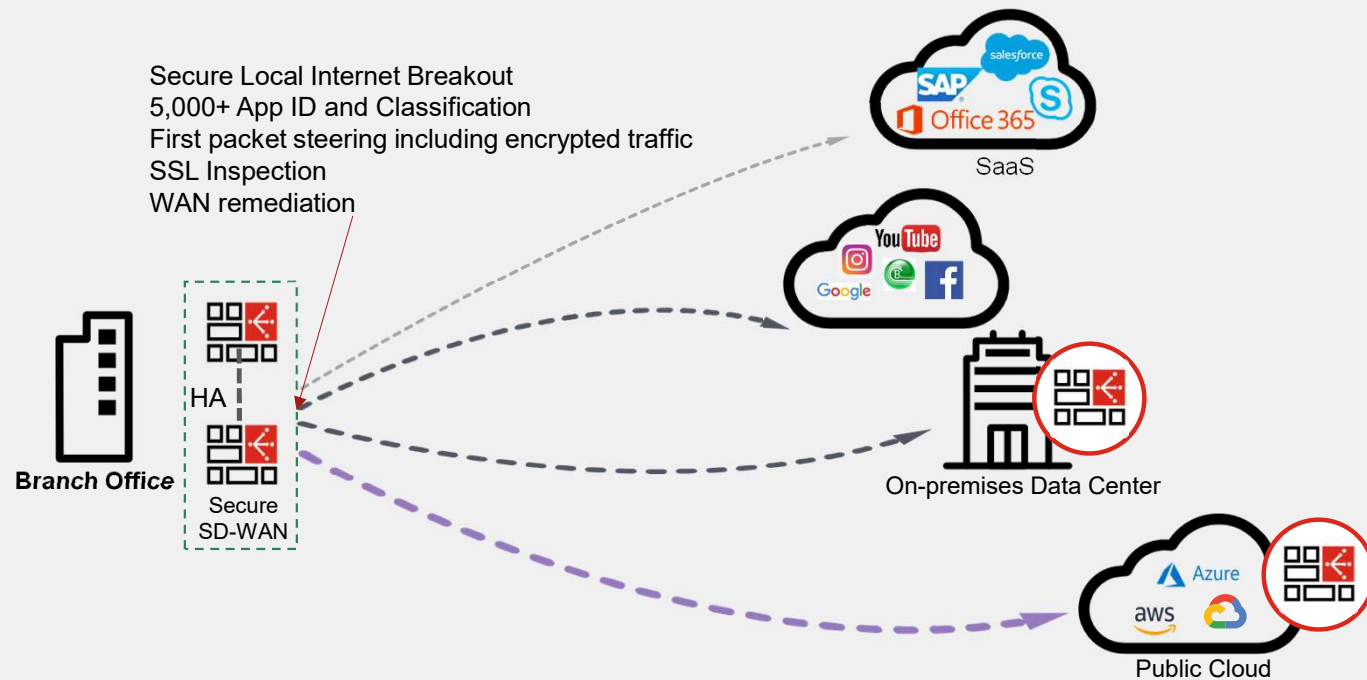
Secure Networking Journey

The convergence of networking and security across WLAN, LAN, SD-WAN, ZTNA, SASE, and network firewall enables networking that is location, user, device, content, and application aware.



Enabling Application Resilient Networks

Secure Local Internet Breakout



Intelligent Steering
Traffic Agnostic

Reliable Accuracy
Including encrypted traffic

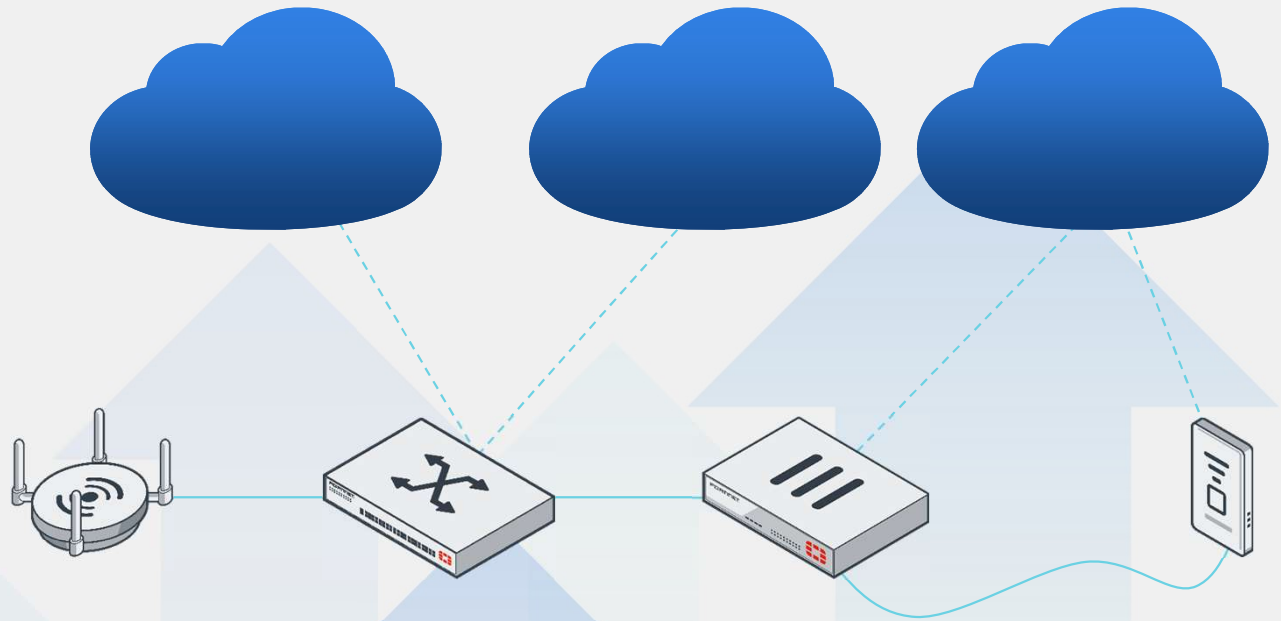
Continuous Learning
Broadest support 5k+ apps

Self-healing
Realtime Optimization



SD-BRANCH

- ✓ Automated Provisioning
- ✓ Central Orchestration
- ✓ Integrated Wireless, Switch, 4G/5G Backup



Managed SD-Branch



Simple, Zero-Touch SD-WAN



FortiExtender 5G Backup



ASIC Walkthrough



GENERATIONAL LEAPS IN:

CONTENT
INSPECTION

&

NETWORK
PROCESSING

Mid Range and
High End



2019

2020

2023

Entry Level



5th Gen System on a Chip

7 nm Technology

Secure Boot

Industry-Leading

Performance Per Watt

88%

Less Power Consumption
Compared to Leading
Industry-Standard CPUs

2.5Gbps

SSL Deep Inspection

Dual Cluster

CPU

Octa Core

32x Encryption

Hardware-Accelerated Encryption

FORTINET®

FortiSP5

T6WYOSBG-0001

● ● A

Interfaces

1G / 2.5G / 5G /
10G / 40G

NP7 lite + CP 10

Security Processing Unit

VXLAN / GRE / QoS

Hardware-Accelerated Encapsulation
and Traffic Shaping

Volumetric

DDoS

Protection

17x

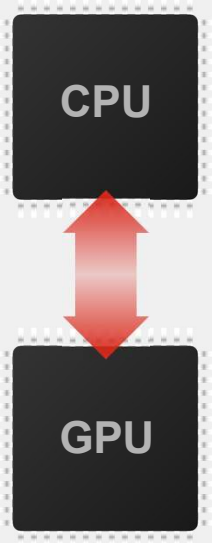
Security Compute Rating for
Firewall Performance vs. Leading
Industry-Standard CPUs



Fortinet Designed Security Processing Unit (SPU)

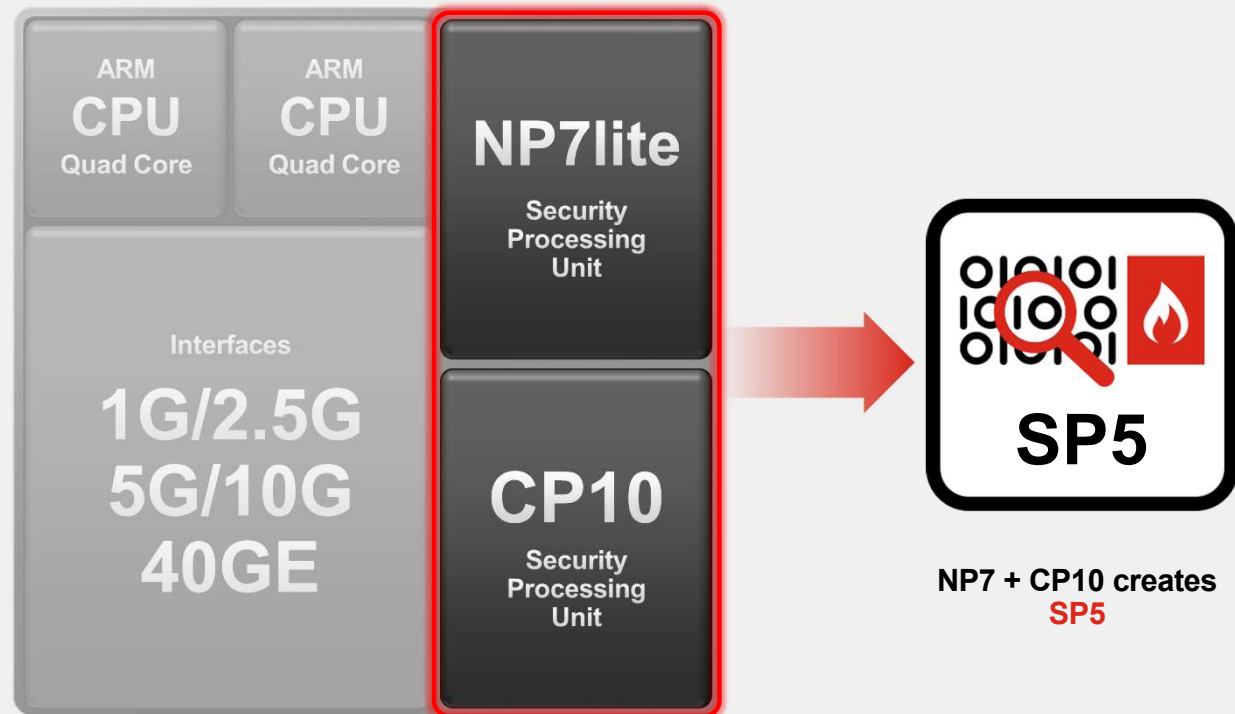
Off Loading the Networking and Security Functions

Gaming and AI Systems



Graphical Processing Unit (GPU)

Off-Loads graphic's rendering compute from the CPU

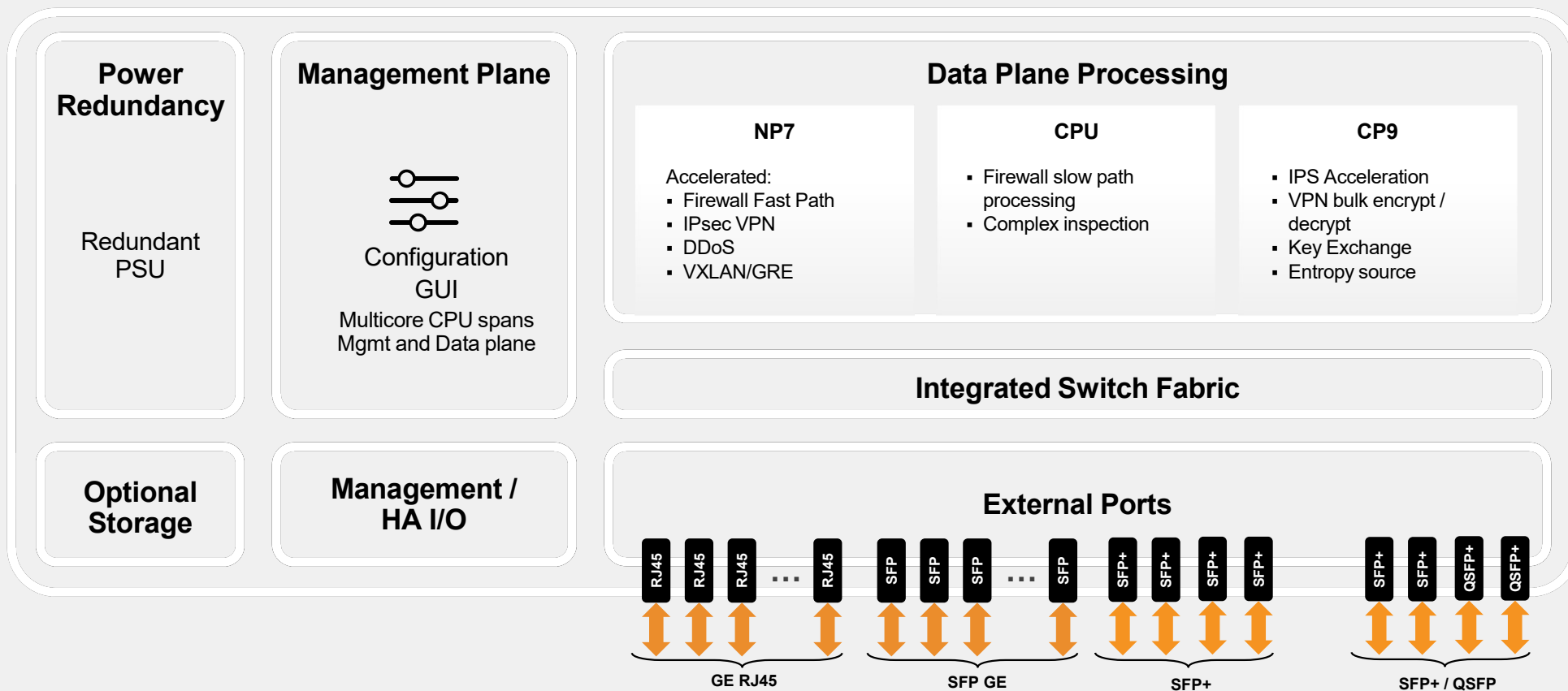


NP7 + CP10 creates
SP5



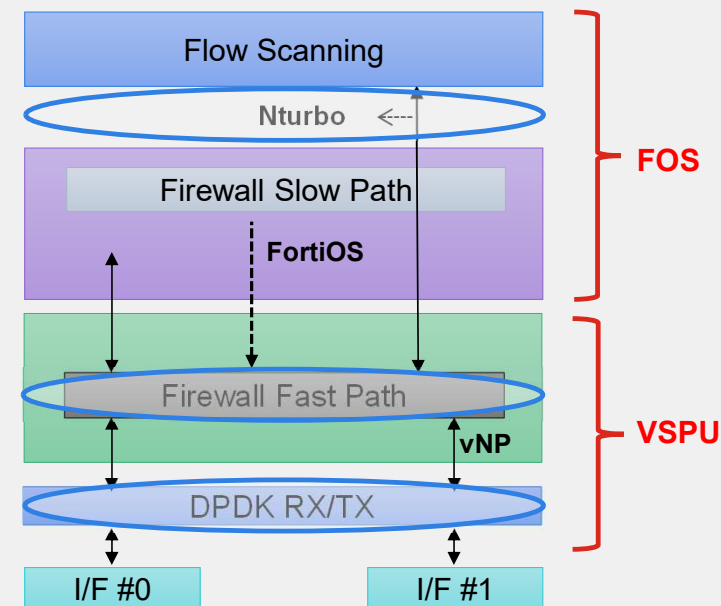


FortiGate Hardware Architecture



SPU— virtual SPU

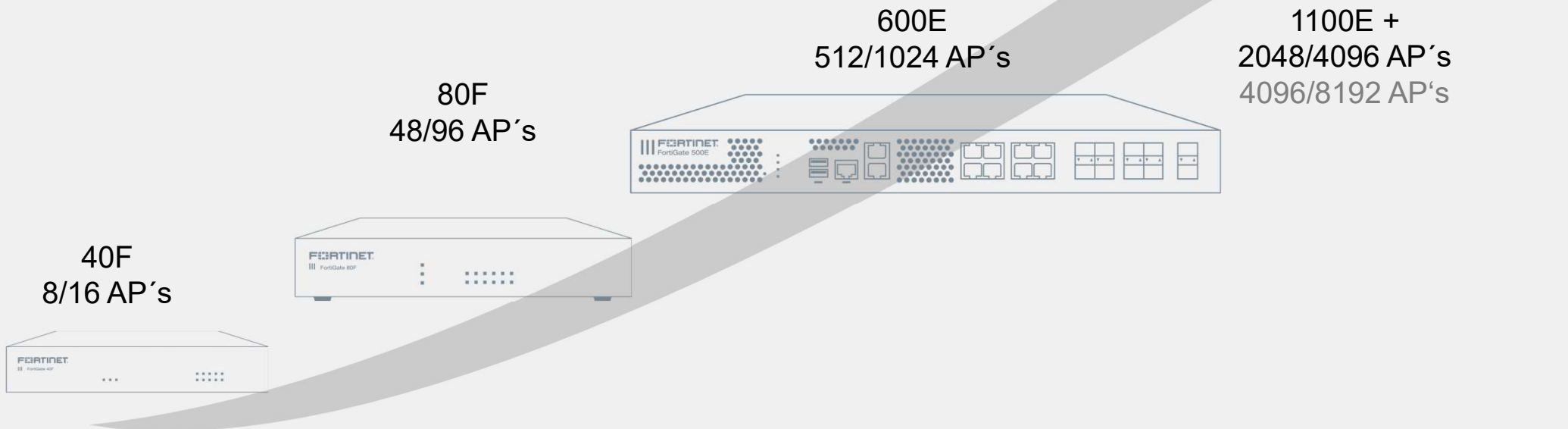
- The VSPU is a combination of the VNP and the DPDK library
 - VNP = NP functionality that allows us to software accelerate the traffic and the flow-based processing traffic (Nturbo)
 - DPDK library allows a pooling mode driver which drastically increase the performance.
 - It is independent of the Hypervisor
- Everyone is using DPDK in their VM
 - What makes Fortinet different is the addition of the virtual NP
 - The VNP allows the same scanning software acceleration as our desktop or appliance.



FortiGate **is** a Wireless / Switch Controller



- **Every** FortiGate has a built-in wireless controller
- Models with integrated wireless and PoE available



Fortinet secure Ethernet Edge through FortiLink

Direct control, configuration and management of LAN through FortiGate FortiOS

Integrated Security

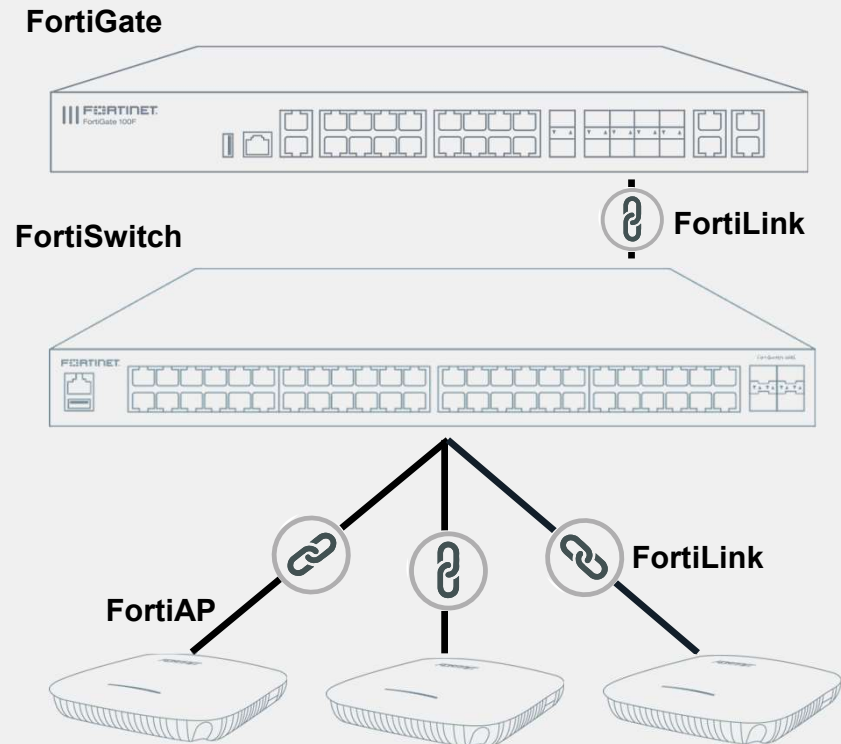
- Extends NGFW features to the Ethernet switch
- Base NAC features included
- Giant step beyond centralized management

Simplicity

- Agile deployment and management
- Flexible architecture, scales as needs change
- Rich data set for AI/ML

Lower Cost of Ownership

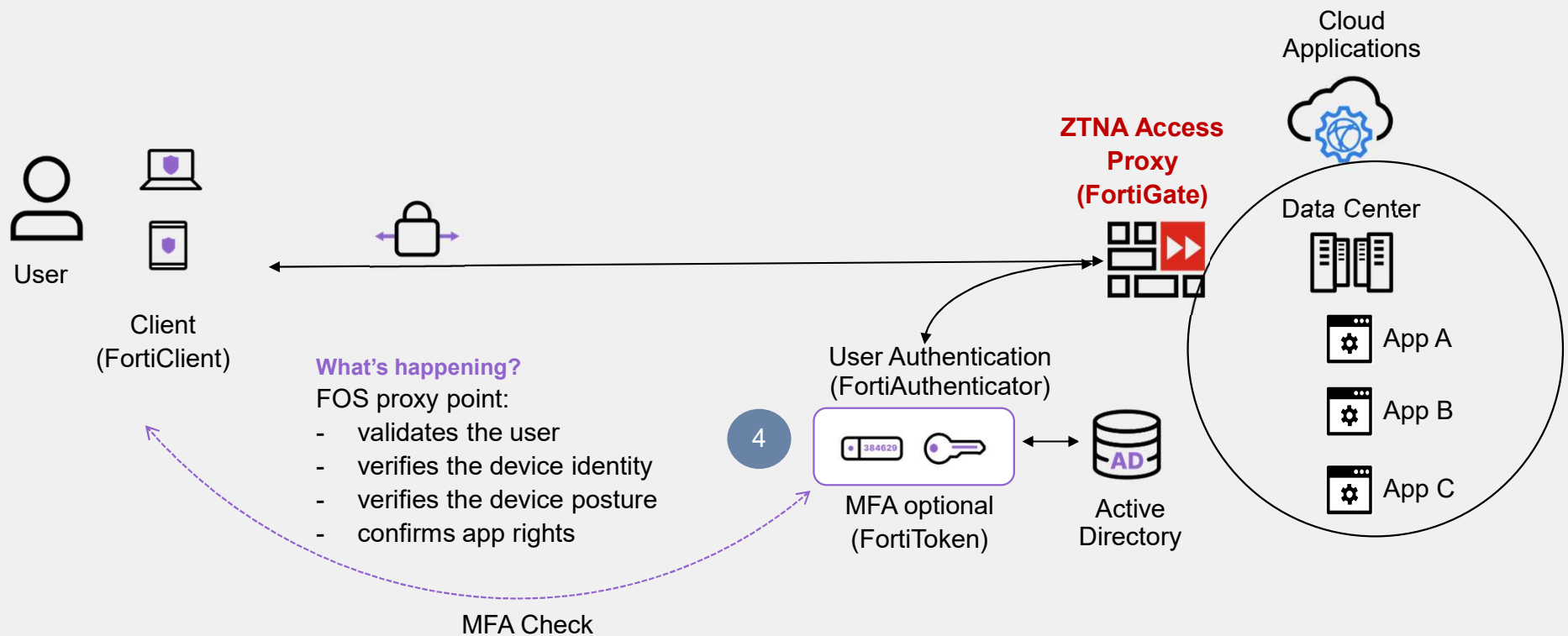
- Included with FortiOS
- No licenses required



Zero Trust Network Access (ZTNA) Technology



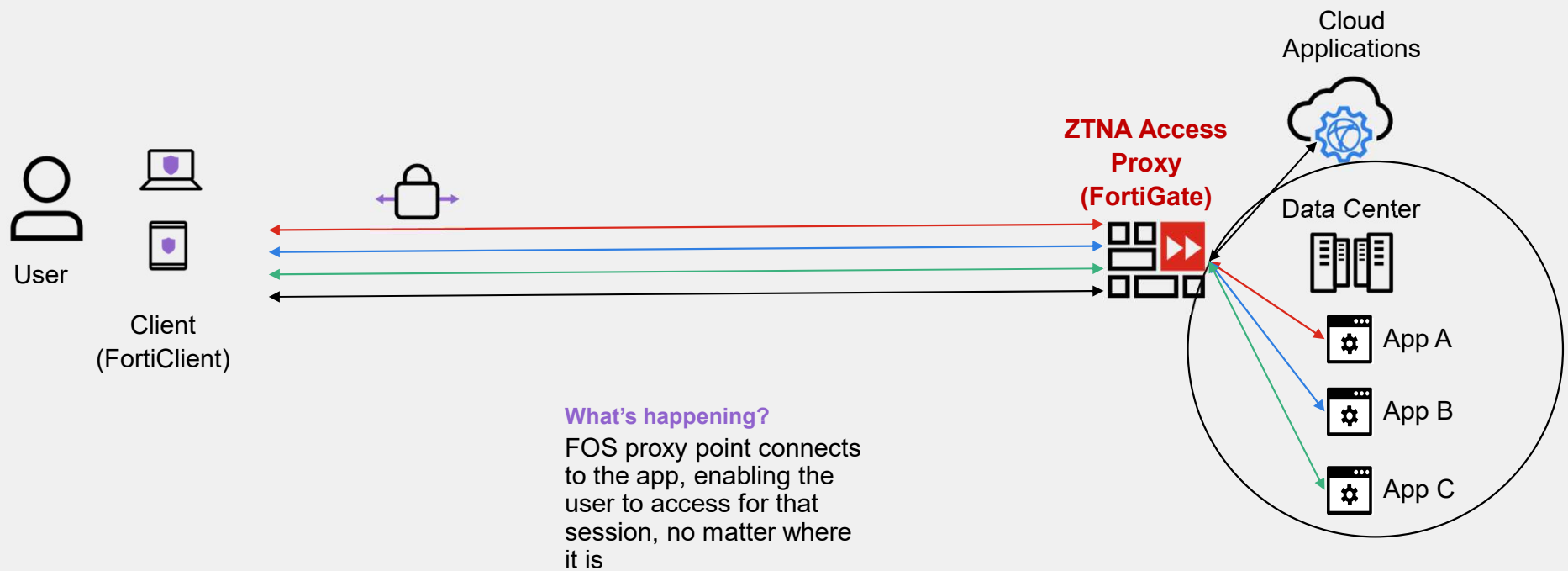
Tunnel and Device Posture Check; Optional Multi Factor Authentication (MFA)



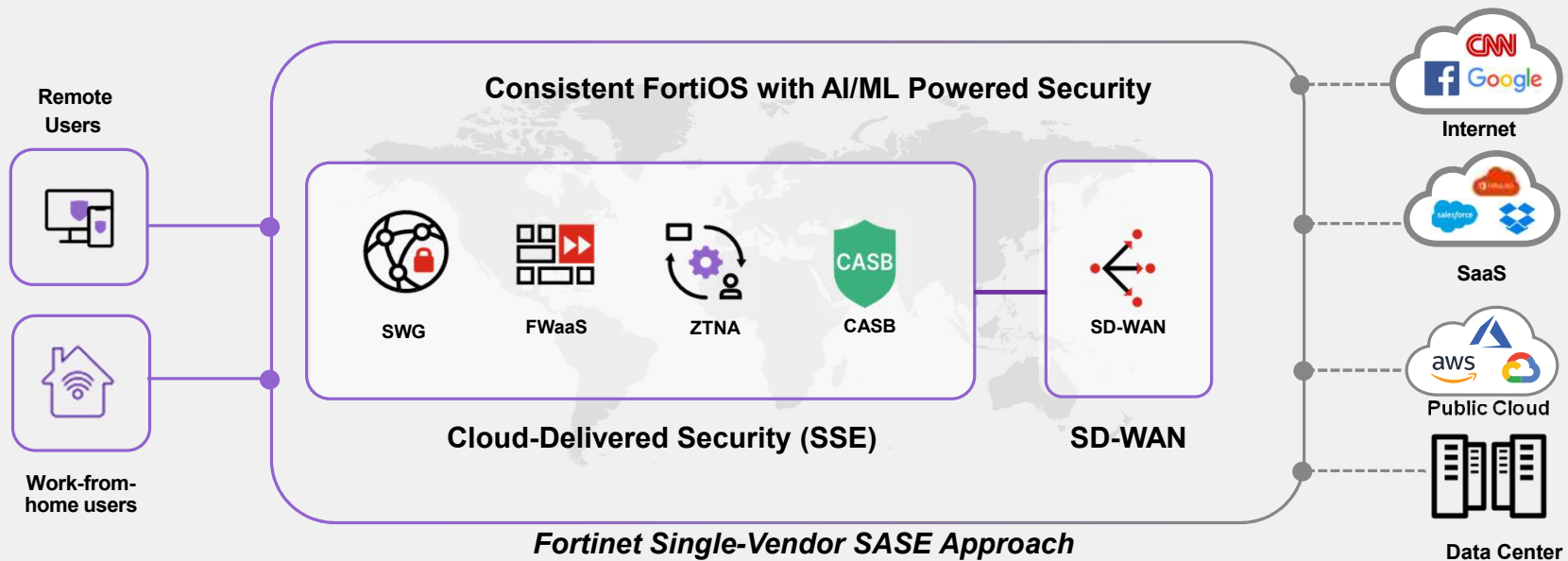
Zero Trust Network Access (ZTNA) Technology



Tunnel and Device Posture Check; Optional Multi Factor Authentication (MFA)



FortiSASE: Cloud-Delivered Security & Networking



Secure Hybrid Workforce with
Consistent Security

Superior User Experience with
Operational Efficiency

Reduce cost and efforts, shift
CAPEX to OPEX based model





Product Overview





FortiGate Portfolio

FortiGate Portfolio Covers Small Branch to Hyperscale

Entry-Level Appliance FGT 40 – 100 Series



SOC Based

Mid-Range Appliance FGT 200 – 900 Series

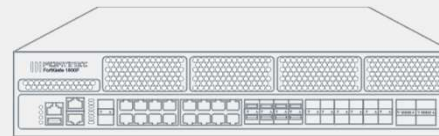


Network Processor



Content Processor

High-End Appliance FGT 1000 – 6000 Series



N x
Network Processor

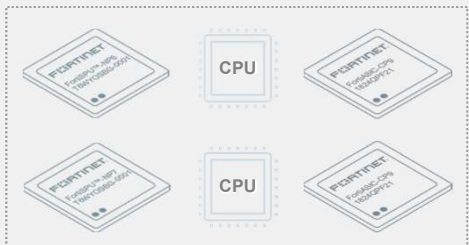
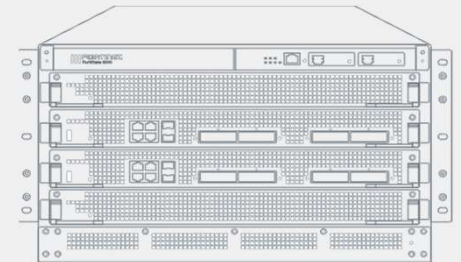


N x
CPU



N x
Content Processor

Chassis FGT 7000 Series



Blades



FortiGate Deployment Modes



FortiGate



FortiGate Hardware Appliance
Accelerated by Security
Processing Unit (SPU)



System
on a Chip



Network
Processor



Content
Processor

FortiGate VM



FortiGate Virtual Machine
Licensed by CPU Cores



1-92
Cores



1-72
Cores



1-32
Cores



1-32
Cores

FortiGate Container



Different Functionality
available in Containers



Linksys
OS



Cloud
Microservices



5G

FortiGate as a Service



FortiGate Delivered as a
Cloud Service






Remote
Users




Branch
Office




FortiGate-VM Models and Services

VM Models		VM-01 VM-02	VM-04 VM-08	VM-16 VM-32
Throughput				
	Threat Protection	Up to 2 Gbps		
	IPSec VPN	Less than 2.5 Gbps		
	Threat Protection		Up to 6.5 Gbps	
	IPSec VPN		Less than 9 Gbps	
	Threat Protection			Up to 14.2 Gbps
	IPSec VPN			Less than 18 Gbps
Services	VPN Gateway	Basic NGFW	Advanced NGFW	Secure SD-WAN
FortiCare Only	✓			
ATP		✓		
UTP			✓	
Enterprise				✓


BYOL



Term-based Subscription





Flex-VM Consumption




Perpetual License

Cloud PAYG





Monthly



Annual

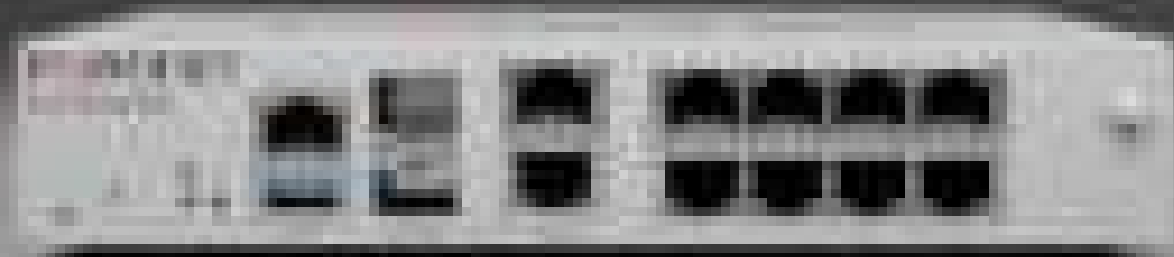


Use cases by FortiGate VM Deployment Type

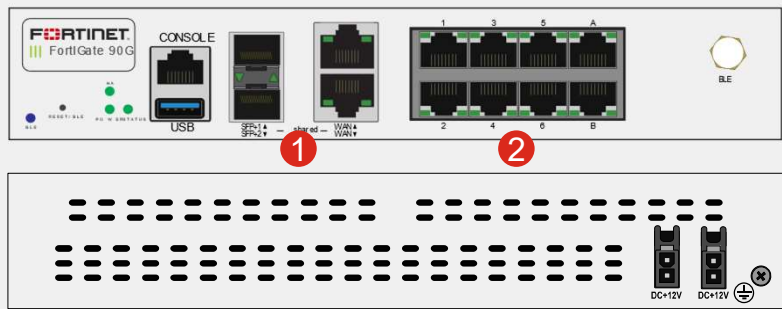
	Hybrid Cloud	Multi-Cloud	MSSP/NSP	Mobile SP
VPN Gateway	✓	✓	✓	
SD-WAN	✓	✓	✓	
North-South Perimeter		✓	✓	✓
East-West Perimeter (<i>Centralized Inspection</i>)		✓		
East-West Perimeter (<i>Service Chain/One-arm FW</i>)	✓			
Secure Remote Access	✓	✓		
Managed Firewall			✓	
Secure Gateway				✓
User Firewall				✓



Introducing FortiGate 90G



FortiGate 90/91G



- ① 2x 10/5/2.5/ GE RJ45 or 10GE/GE SFP+/SFP Shared Media Ports
- ② 8x GE RJ45 Ports



28 Gbps
Firewall throughput



4.5 Gbps
IPS Throughput



2.5 Gbps
NGFW Throughput



2.2 Gbps
Threat Protection Throughput

124,000
New Sessions/Sec

1.5 Million
Concurrent Sessions



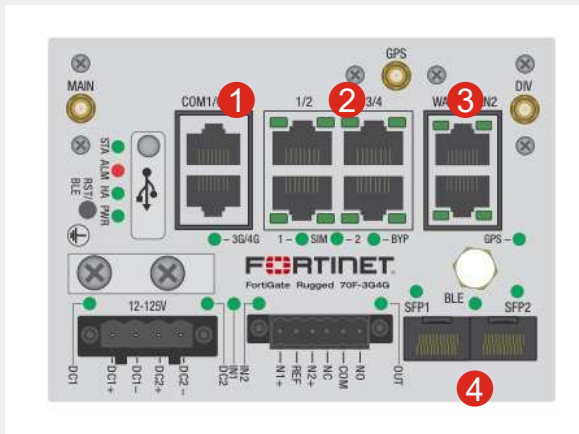
2.6 Gbps
SSL Inspection Throughput



Small Business / Remote Office
NGFW / Secure SD-WAN



FortiGate Rugged-70F-3G4G



- ① 2x Serial Ports
- ② 4x RJ45 Ports*
- ③ 2x RJ45 WAN Ports
- ④ 2x GE SFP Slots

* Port3 and Port4 are default configured as 1x bypass GE RJ45 port pair



8 Gbps

Firewall throughput

35,000

New Sessions/Sec



1 Million

Concurrent Sessions

500 Mbps

SSL Inspection Throughput



975 Mbps

IPS Throughput



950 Mbps

NGFW Throughput



580 Mbps

Threat Protection Throughput

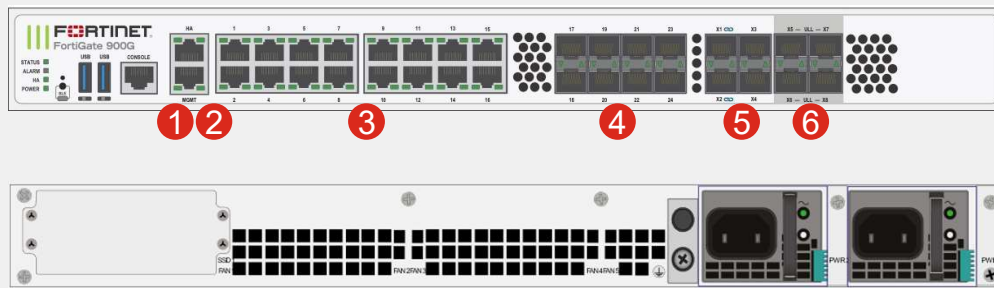


Small Business / Remote Office

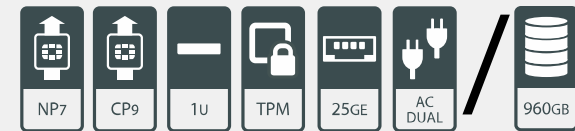
NGFW / Secure SD-WAN



FortiGate 900/901G



- ① 1x GE RJ45 Management Port
- ② 1x 2.5GE RJ45 HA Port
- ③ 16x GE RJ45 Ports
- ④ 8x GE SPF Slots
- ⑤ 4 x 10GE/GE SFP+/SFP Slots
- ⑥ 4 x 25GE/10GE SFP28/SFP+ ULL (ultra-low latency) Slots



164 Gbps
Firewall throughput



26 Gbps
IPS Throughput



22 Gbps
NGFW Throughput



20 Gbps
Threat Protection Throughput

720,000
New Sessions/Sec

16 Million
Concurrent Sessions



16.7 Gbps
SSL Inspection Throughput



Enterprise Branch / Mid Enterprise
NGFW / Secure SD-WAN / IPS / SWG





FortiSwitch Portfolio

FortiSwitch Access Switch Family

Entry

100 Series



- Entry Level Switch
- 8 to 48 gigabit Ethernet ports, POE Capable
- Desktop to wiring closet.
- (2-4) GE SFP or 10GE SFP+ uplink (no MCLAG)

Mid Range

200 Series



- Mid level Switch
- 24 to 48 gigabit Ethernet ports POE+ Capable
- Typical wiring closet switch
- (4) Gigabit Ethernet SFP uplink ports

Premium

400 Series



- Enterprise Switch
- 24 to 48 gigabit Ethernet ports POE+ Capable
- Larger wiring closet or high throughput requirements.
- Up to (4) 10 Gigabit Ethernet SFP uplinks

Aggregation

500 Series



- Aggregation Switch
- 24 to 48 gigabit Ethernet ports POE+ Capable
- Up to (4) 10 Gigabit Ethernet (2) 40 Gigabit Ethernet SFP uplinks
- Dual Power Capable

Small Business

Secure SD-Branch

Small Campus Secure SD-LAN



FortiSwitch Data Center Switch Family

1000 Series



- Data Center Aggregation Switch
- 24 or 48 10 Gigabit Ethernet SFP slots
- Up to four QSFP28 100 GbE Uplinks or Six 40 GbE QSFP+
- Two Dual hot swappable power supplies

3000 Series



- Data Center Switch
- 3000 series offers 32 x 100 Gigabit Ethernet capable QSFP28 slots
- Dual hot swappable power supplies

Small Business Data Center

Small Campus Secure SD-LAN Top of Rack Aggregation





FortiAP Portfolio



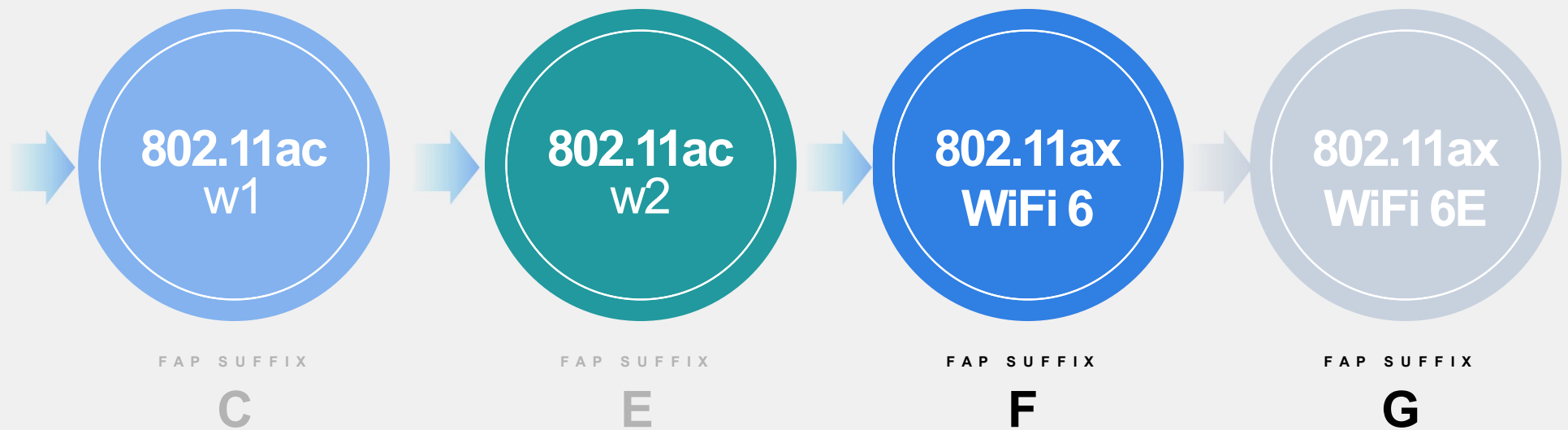
Access Points You Expect From Enterprise Wi-Fi



- Latest Wi-Fi 6 & 6E technology
- 4x4 models for high throughput
- 2x2 models for price sensitivity
- Internal or external antenna
- Dual 5GHz operation
- IP67 models for Outdoor installations and meshing
- Wall Plate form factor for in-room installations



Wi-Fi Technology



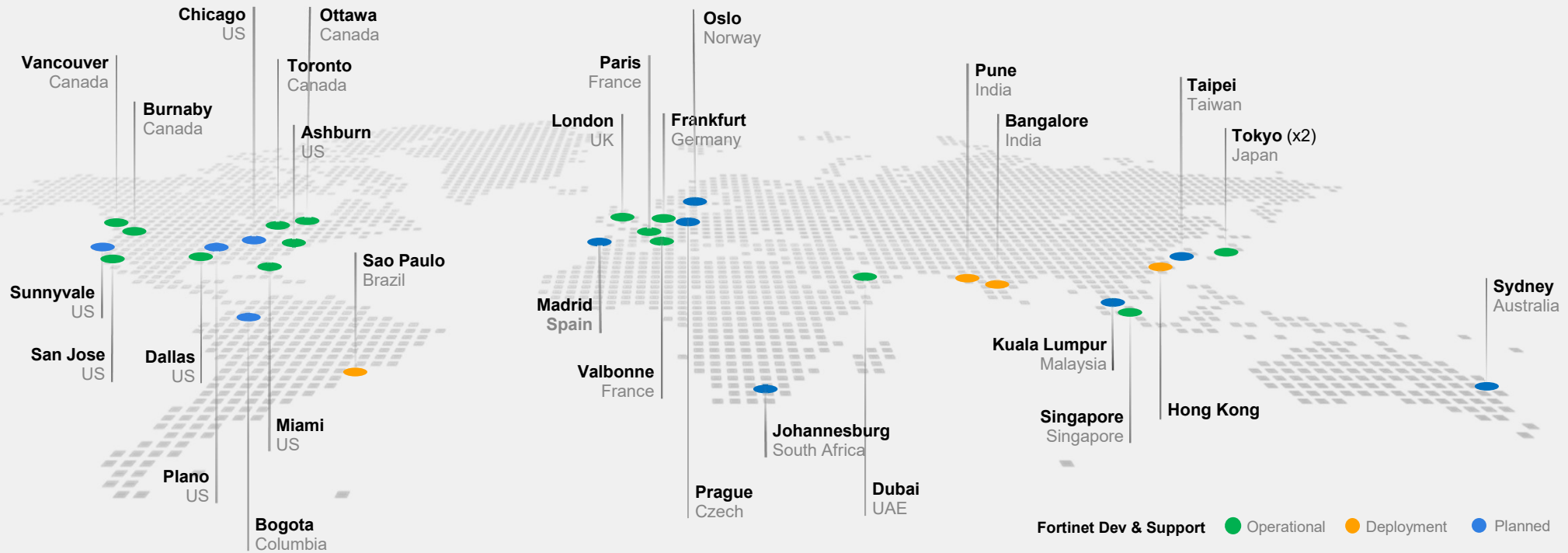


FortiSASE



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

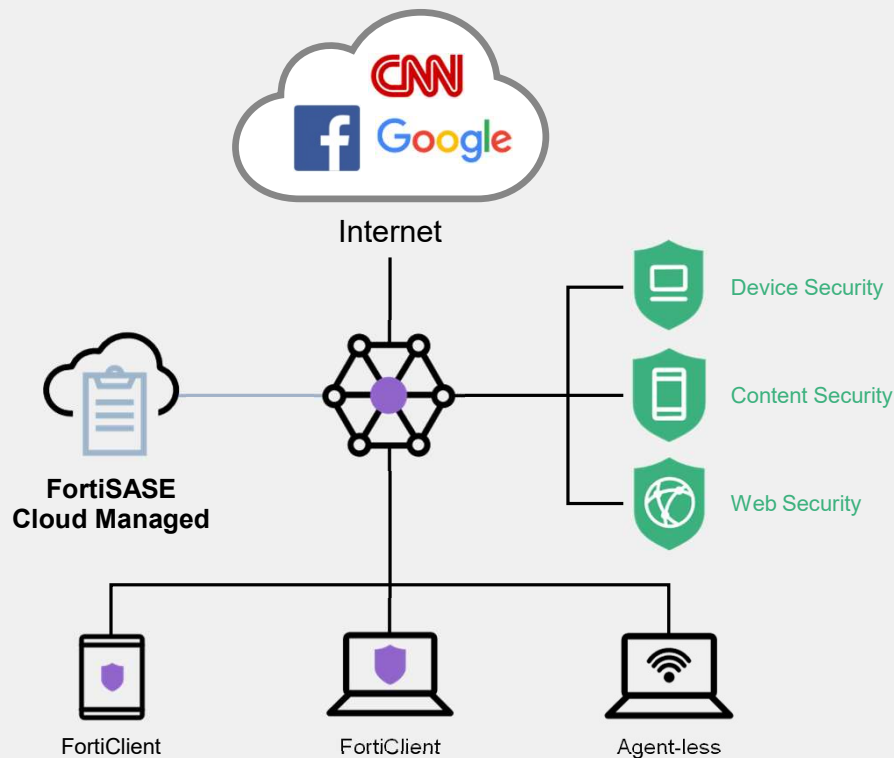
40 datacenters in 2024

Regional coverage



Secure Internet Access for Remote Users

USE CASE 1



Work from Anywhere

Safe browsing from anywhere



Malware & Ransomware prevention

Continuously assess the risks and automatically respond and **counter known and unknown threats**



Deep inspection of end-user activity

Constant inspection of web activity for threats, even when using secured https access



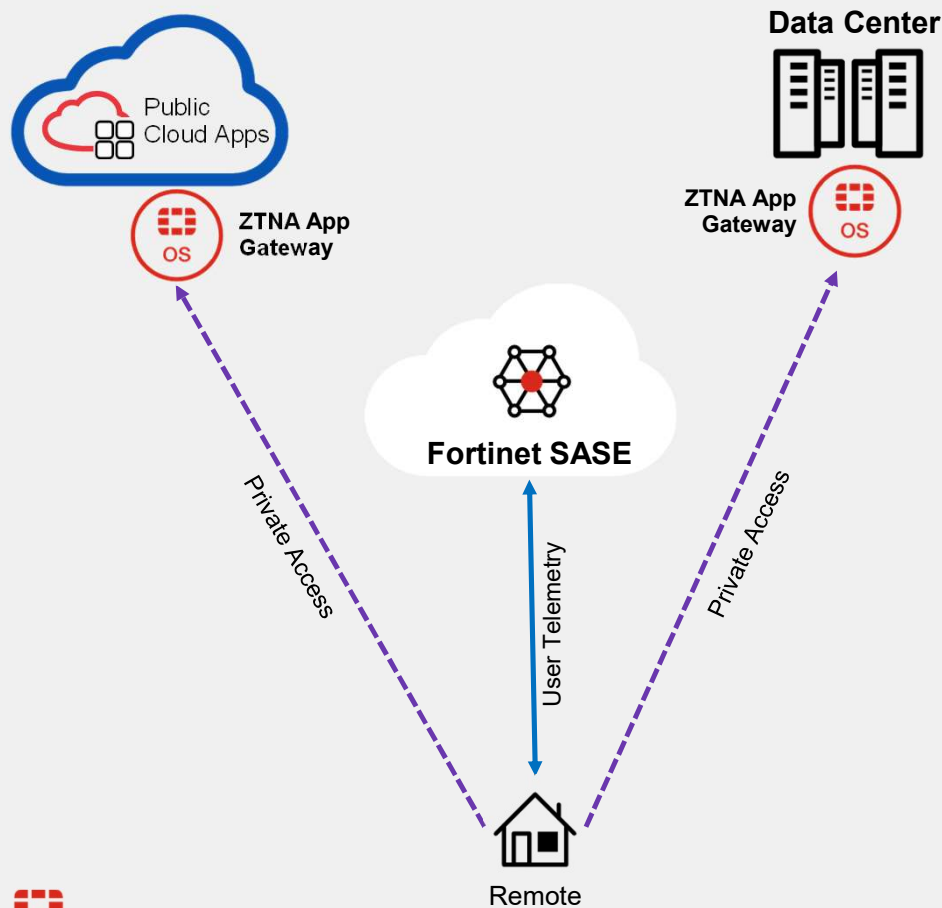
Market Leading Security as a Service

Fortinet best-in-class Cloud security powered by FortiGuard Labs



Secure Private Access With Natively Integrated ZTNA

USE CASE 2



Enabling Universal ZTNA



Cloud provisioned ZTNA connections



Device attributes, **user** info, **security posture** based security



Granular per-session posture checks

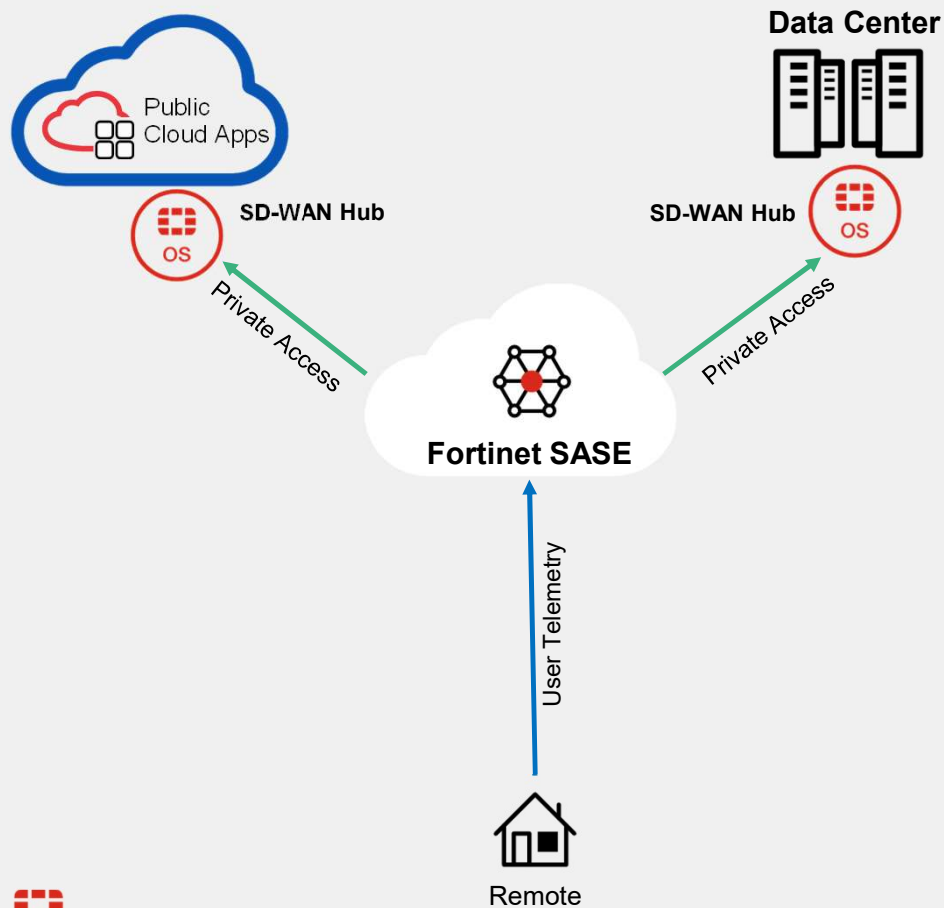


Continuous posture re-assessment

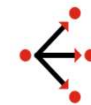


Secure Private Access with SD-WAN

USE CASE 3



SD-WAN Private Access



Augment to existing **SD-WAN**



Intelligent routing & steering

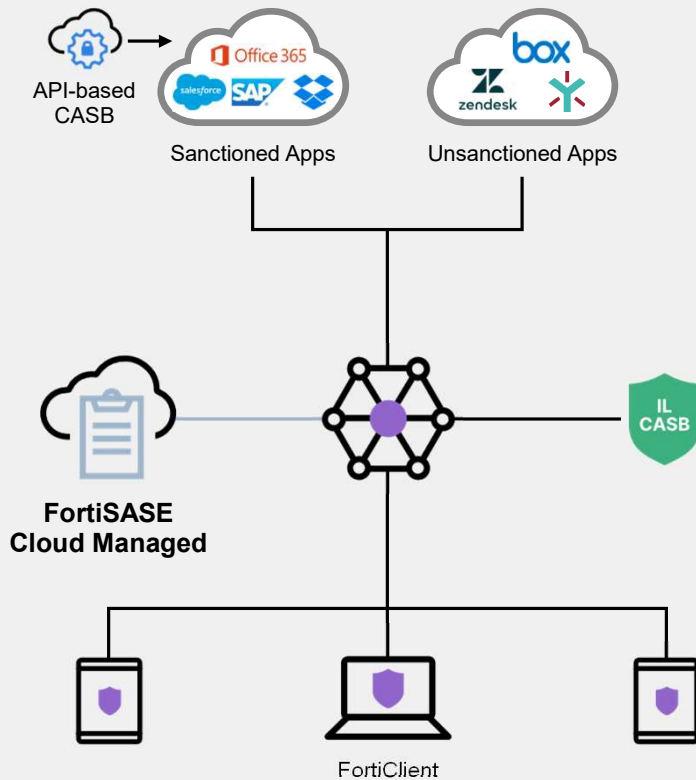


Broader app support (UDP-based, video, UC)



Secure SaaS Access for Visibility & Control

USE CASE 4



Secure Access to Cloud apps & files



Cloud App Access Control

Safe Cloud Application access and blocking of malicious apps with in-line CASB feature



Deep control & view of apps content

Control over app content and files with API-based CASB for enhanced security and threat detection



Unified agent for anywhere detection

FortiClient Agent covers all the use-cases from SASE, Zero-trust, SaaS security, and End-Point Protection



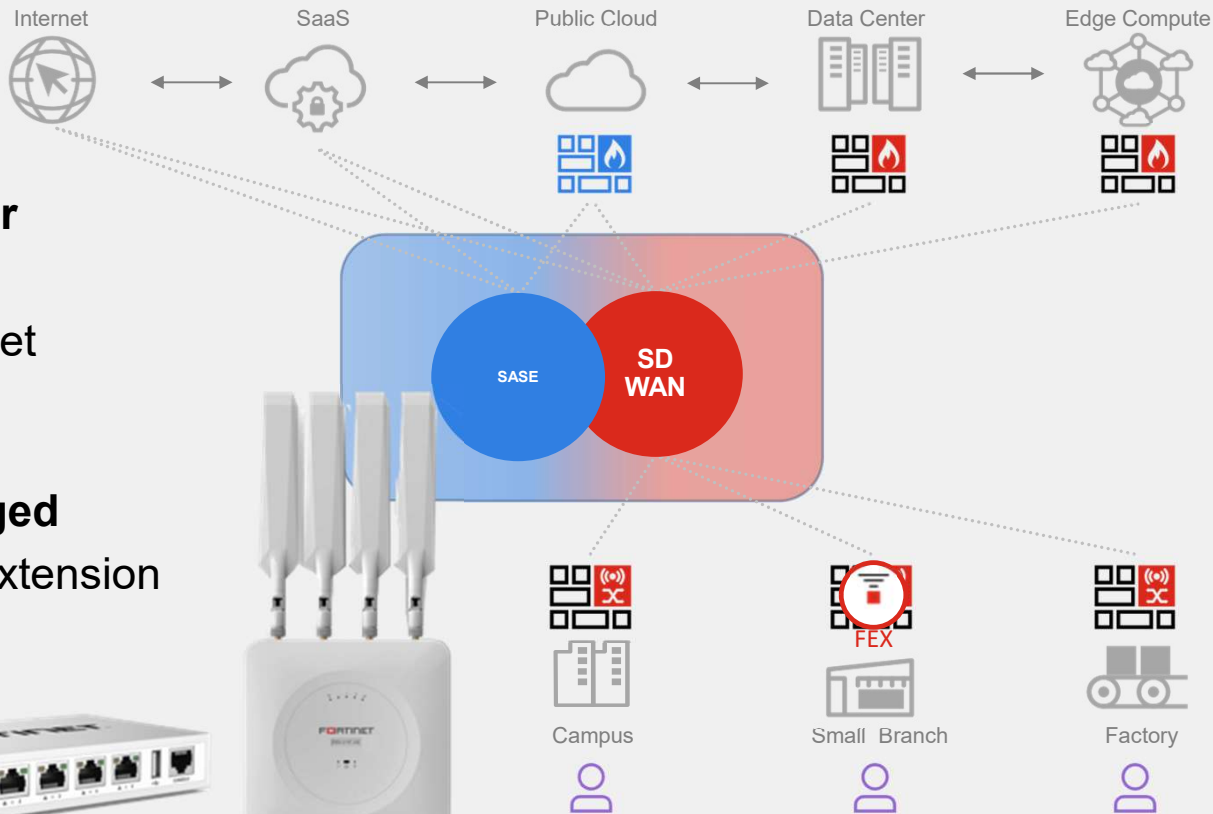
FortiSASE Thin Edge

FortiExtender

- 5G
- Ethernet
- DSL

Cloud Managed

- LAN Extension



Consistent Security



Application Aware
Intrusion Prevention
Web Filtering
DNS Protection
Sandboxing
In-Line Sandboxing
Network Access
Control (NAC)
OT and IoT Security



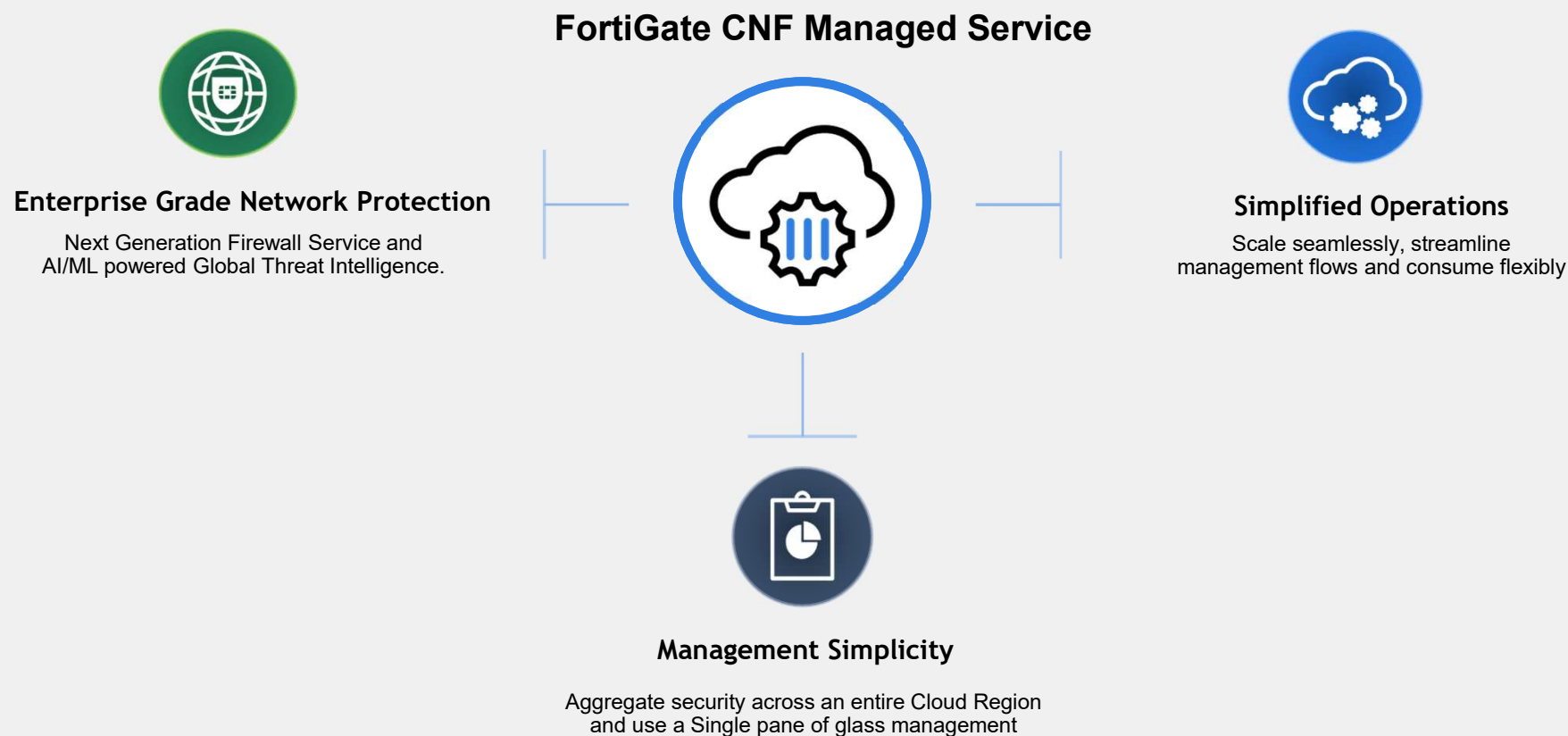


FortiGate CNF

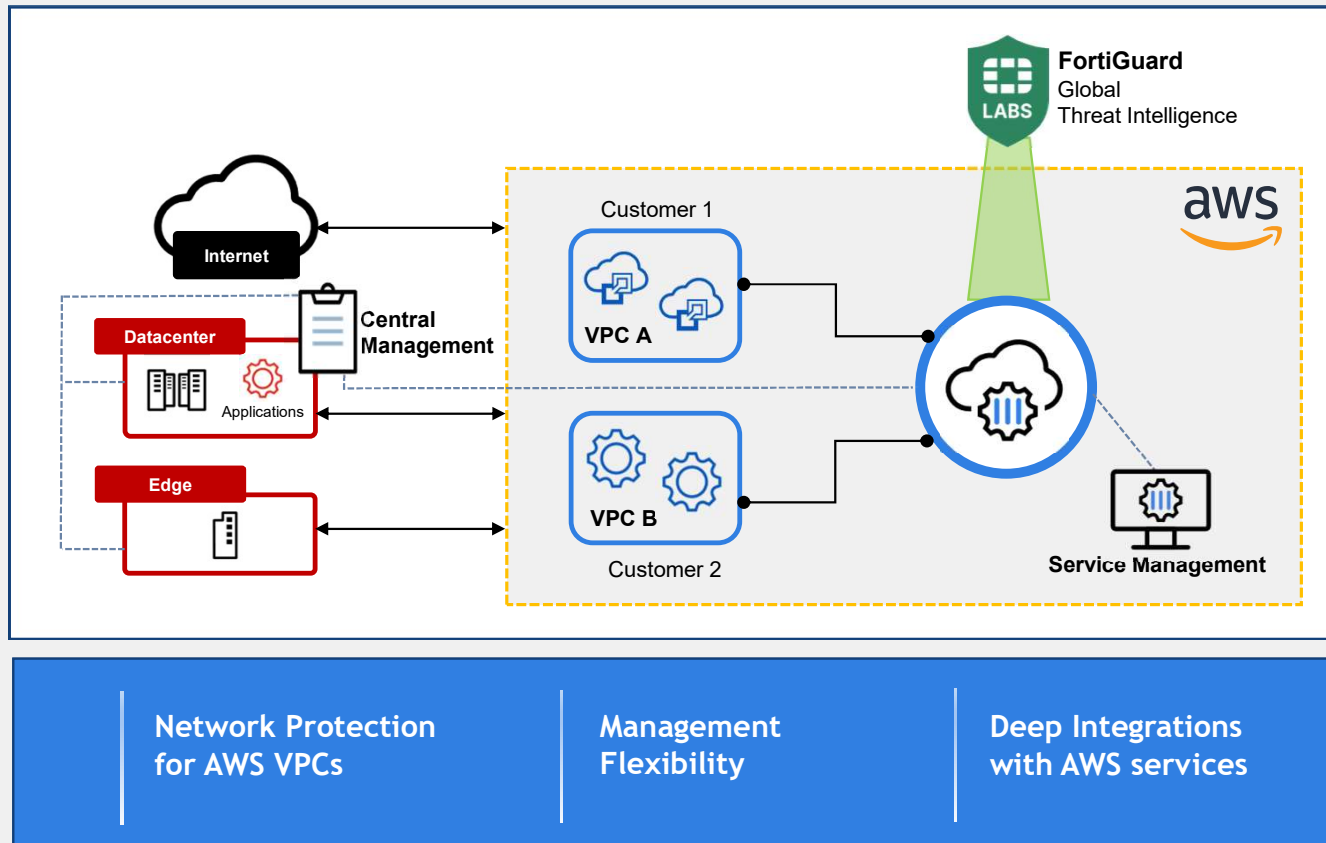
Cloud-Native Firewall Service



Introducing FortiGate Cloud-Native Firewall Service



Simplify and Modernize Network Security on AWS



Key Use cases



Outbound Traffic Inspection

Content Inspection of outgoing traffic from AWS workloads to the Internet



Inbound Traffic Protection

Deep visibility into incoming traffic and advanced security measures to protect AWS workloads



East-West Traffic Protection

Inspect and control traffic between AWS VPCs and prevent lateral spread of threats



Service Components

Fortinet Management Solutions

FortiGate CNF Console



Management Console for FortiGate CNF Service management and basic security policy management

FortiManager (Supported: mid Feb'23)



Centralized Console to only define and manage security policies for FortiGate CNF on AWS. Manages on-premise FortiGate physical, FortiGate virtual appliances

Optional for customers

Cloud Native Integrations

AWS Gateway Load balancer



For scaling, resiliency and availability

Transparent to customers

AWS Firewall Manager



For provisioning CNF and simplifying security policy management workflow

Optional for customers

AWS Marketplace



For agility, frictionless consumption



Key Differentiators



Security Aggregation

Protect many subnets, VPCs in a cloud region with a single CNF instance



Single Pane of Glass

Ensure consistent security policies in AWS environments, between on-premise locations and cloud



Dynamic Policies

Apply security policies that follow workloads and abstract away network dependencies



Predictable Costs

Easily estimate spend with simple pricing and linear charges. No hourly charges for advanced security levels





FORTINET®