



Security-Driven Networking

John Maddison

CMO & EVP Products

BMW i Motorsport
Official Partner



Cybersecurity Market Drivers

Digital Innovation



Expanded Infrastructure

Users - WFH
Devices – IoT/OT
Application – Cloud
Networks – 5G/SD-WAN/Wifi 6

Sophisticated Threats



Expanded Perimeter

Volume
Attack Vectors
Social Engineering
Exploits
Insider Threat

Ecosystem Complexity



Point Products

Manual Operations
Staffing
Too Many Alerts
Slow Response
Cost
Closed

Compliance

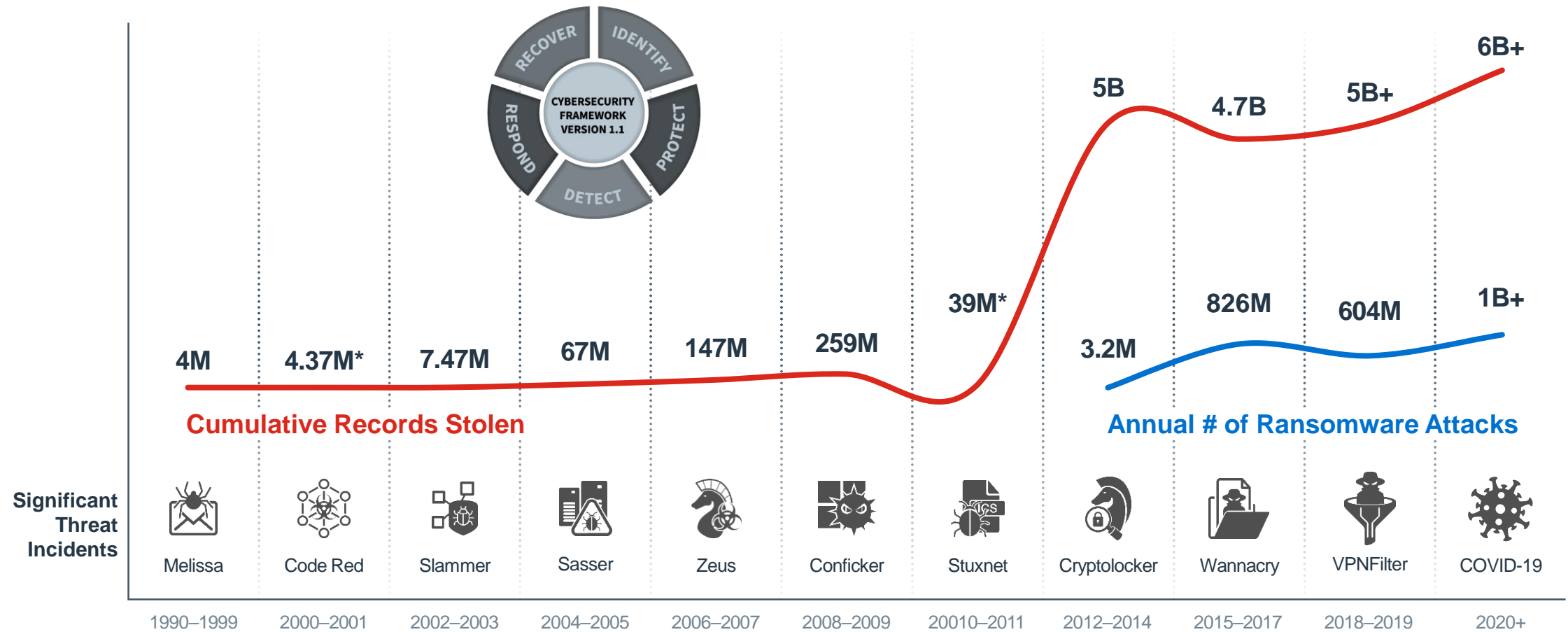


Regulatory Requirements

Global
Country
Industry
Government

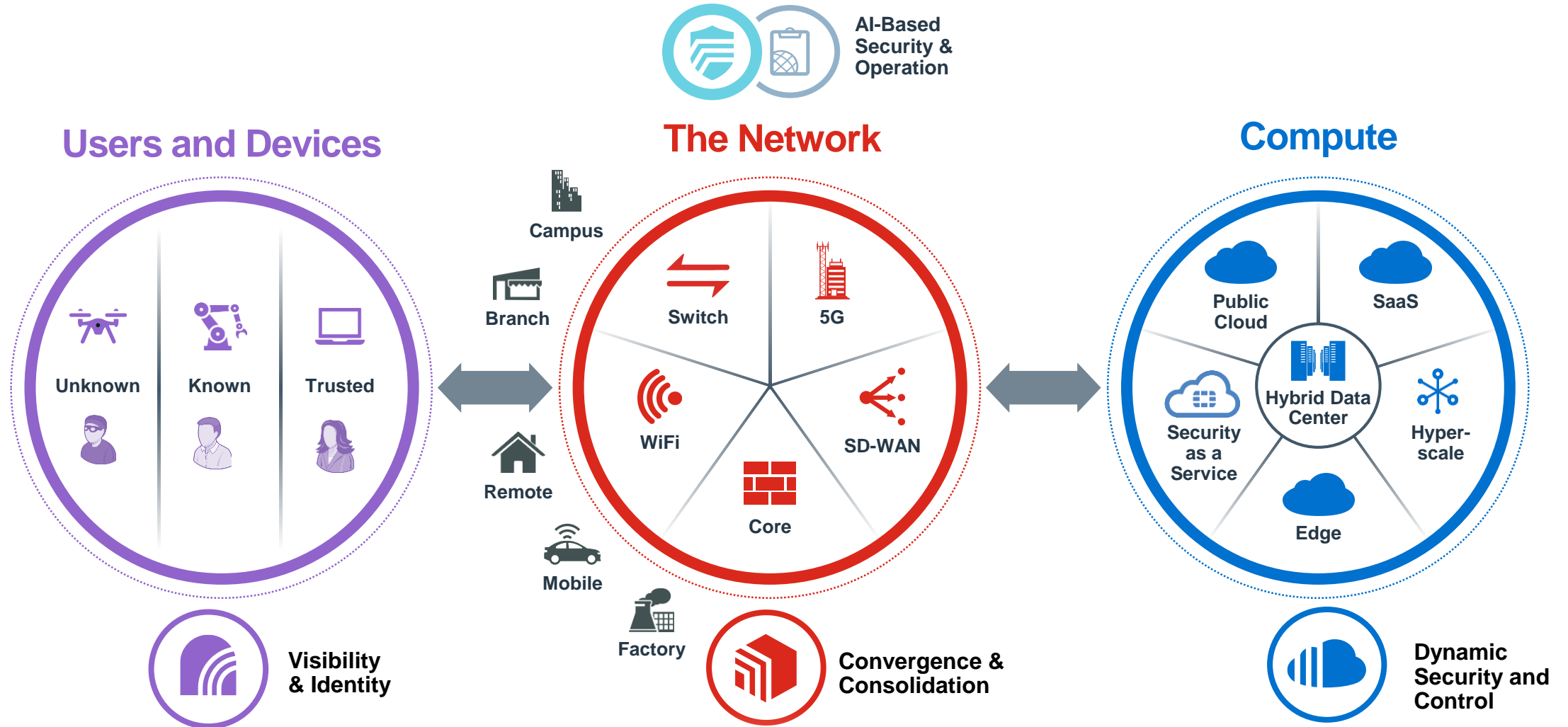
Advanced Threats Continue to Adapt

Social Engineering, Exploits and Insider Threats



*Many undisclosed | Record Stolen Reference—Breach Level Index | Ransomware stats—Statista

Infrastructure will Remain Hybrid and Requires an Integrated Cybersecurity Platform



Fortinet Security Fabric



Zero Trust Network Access

Identify and secure users and devices, on and off network



Security-Driven Networking

Secure and accelerate the network and user experience



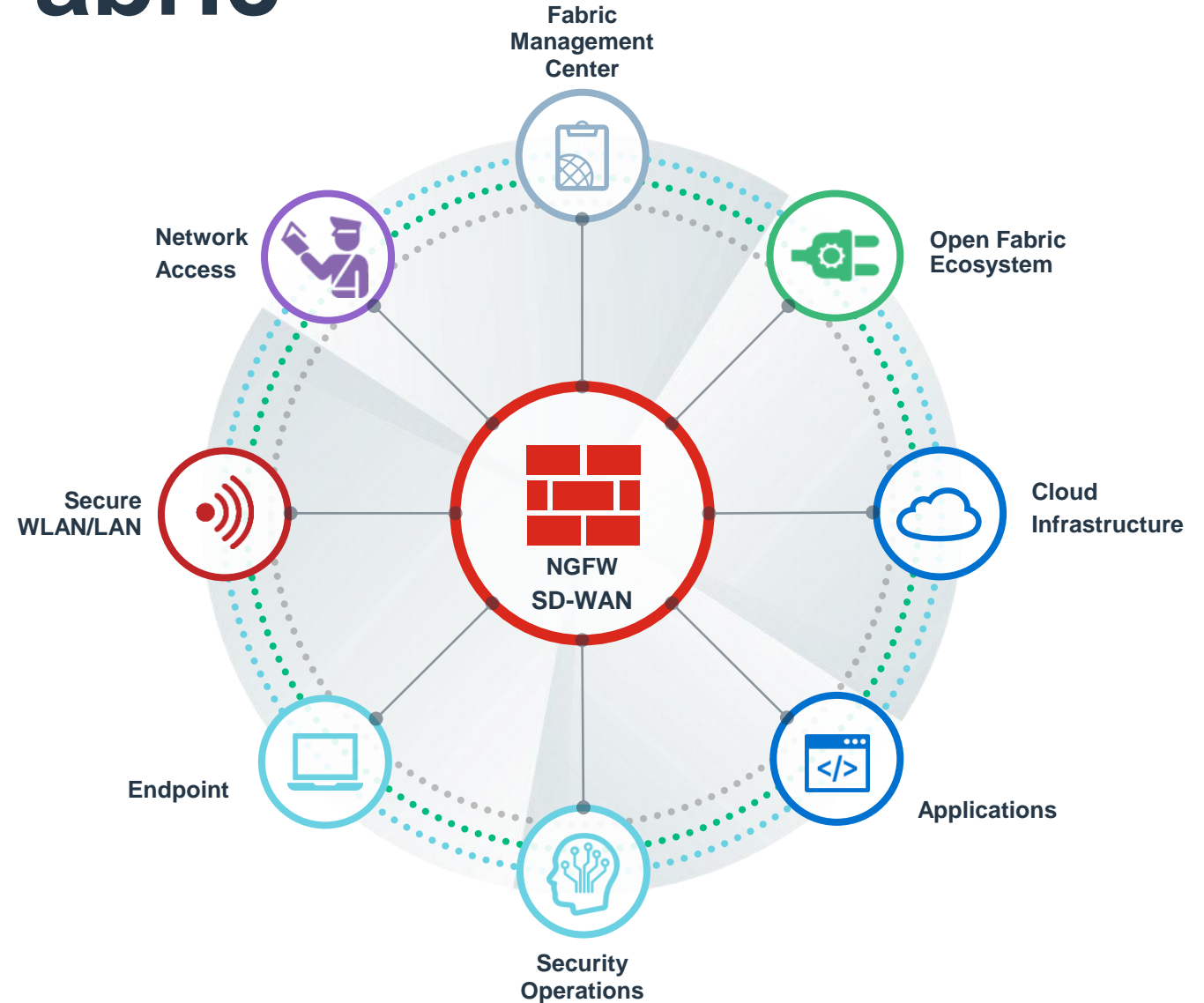
Dynamic Cloud Security

Secure and control cloud infrastructure and applications



AI-driven Security Operations

Automatically prevent, detect, and respond to cyber threats



Hybrid Delivery/Consumption Models

Appliance



Huge Scale



Virtual Machine



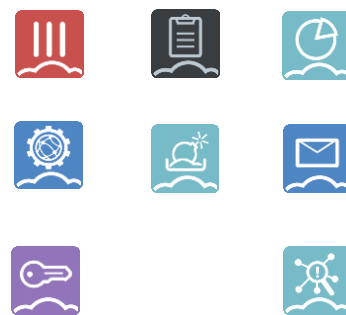
Horizontal and Vertical Scale



Cloud



Market Place (PAYG) & Cloud Native



Security-as-a-Service



Fortinet Hosted



Agent

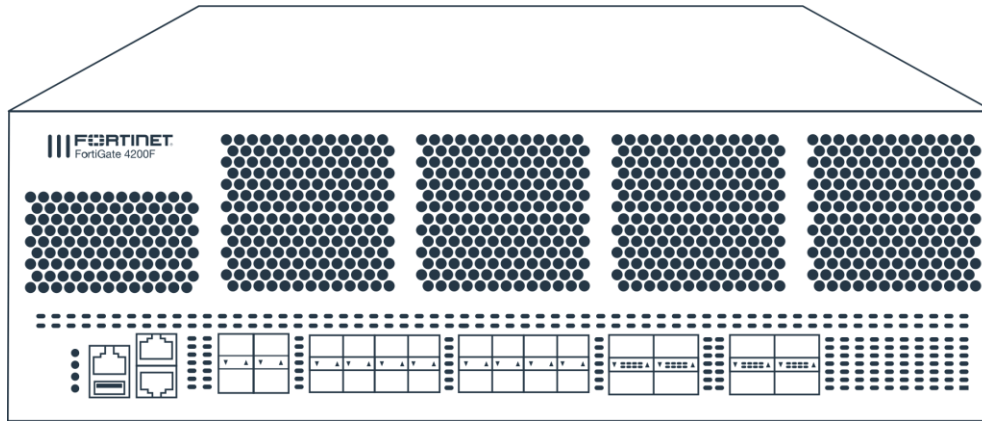


Collector-Cloud



Introducing the FortiGate 4200F NGFW

Powered by NP7



16 x
10/25G

8 x
40/100G



4 x Network
Processor 7

Specification	FortiGate 4201F ¹	Industry Average	Security Compute Rating ³
Firewall	800Gbps	96Gbps	8x
Concurrent Sessions	400M ²	28M	14x
Connections Per Second	8M ²	529k	15x
IPsec VPN	280Gbps	28Gbps	10x
SSL Inspection	38Gbps	8Gbps	5x



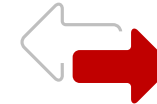
100G
Elephant
Flows



Micro
Second
latency



Hardware
Logging



Accelerated
VXLAN

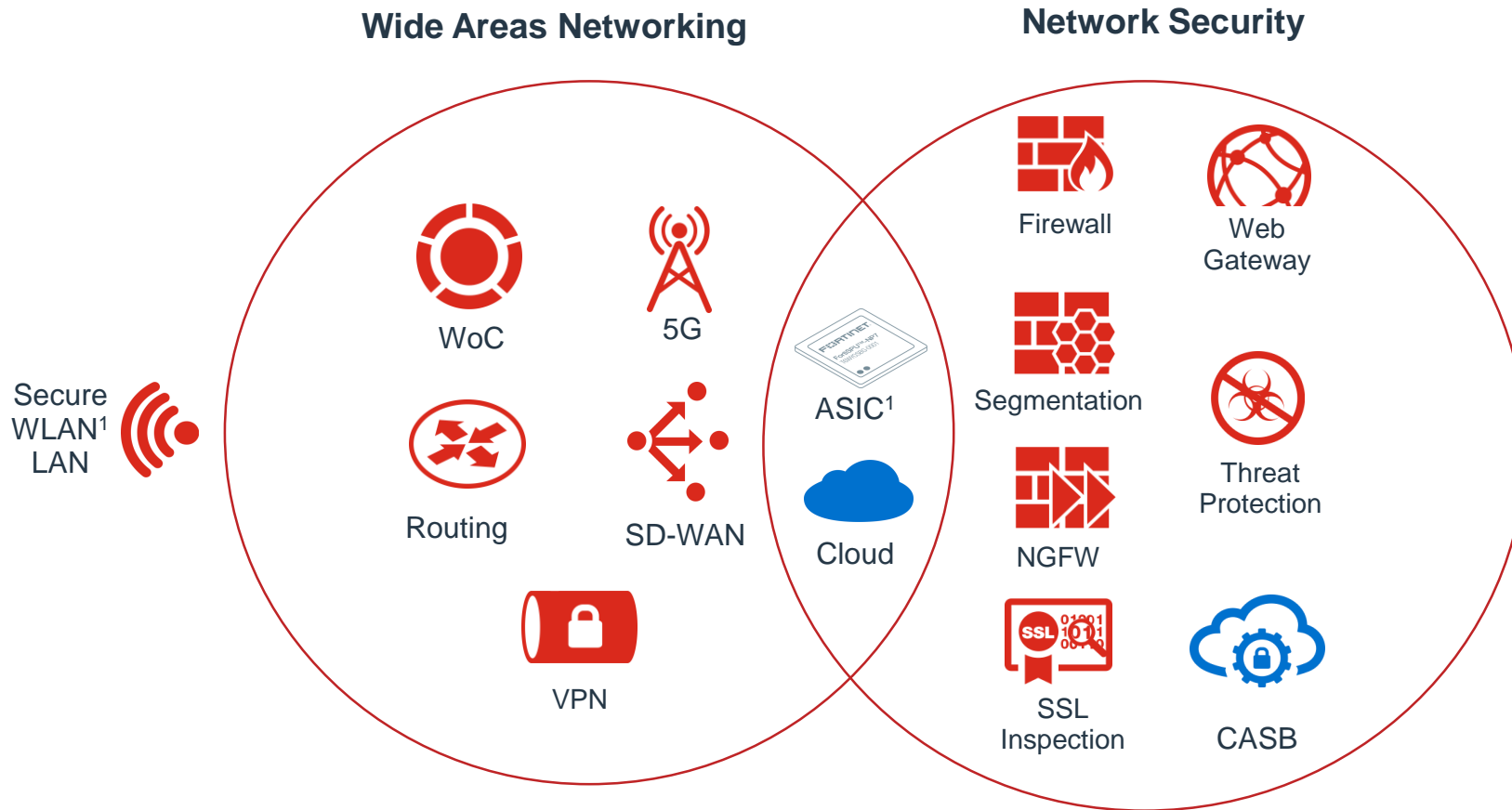


Carrier
Grade NAT



Reduced
power

Baseline SASE Definition



The secure access service edge (SASE) is an emerging offering combining comprehensive network security functions with comprehensive WAN capabilities

Goal: to support the dynamic secure access needs of organizations

Ref: Gartner Emerging Technology Analysis: SASE Poised to Cause Evolution of Network Security







¹Fortinet View

Three Levels of SASE Function – Framework (Fabric)

Level	Functionality	Function				
1	Core	SD-WAN	NGFW FWaaS	SWGaaS	CASB	ZTNA
2	Recommended	Network Sandbox	Browser Isolation	WAF/API Security	Managed Devices	Unmanaged Devices
3	Optional	Secure WiFi	VPN		Edge Compute Security	

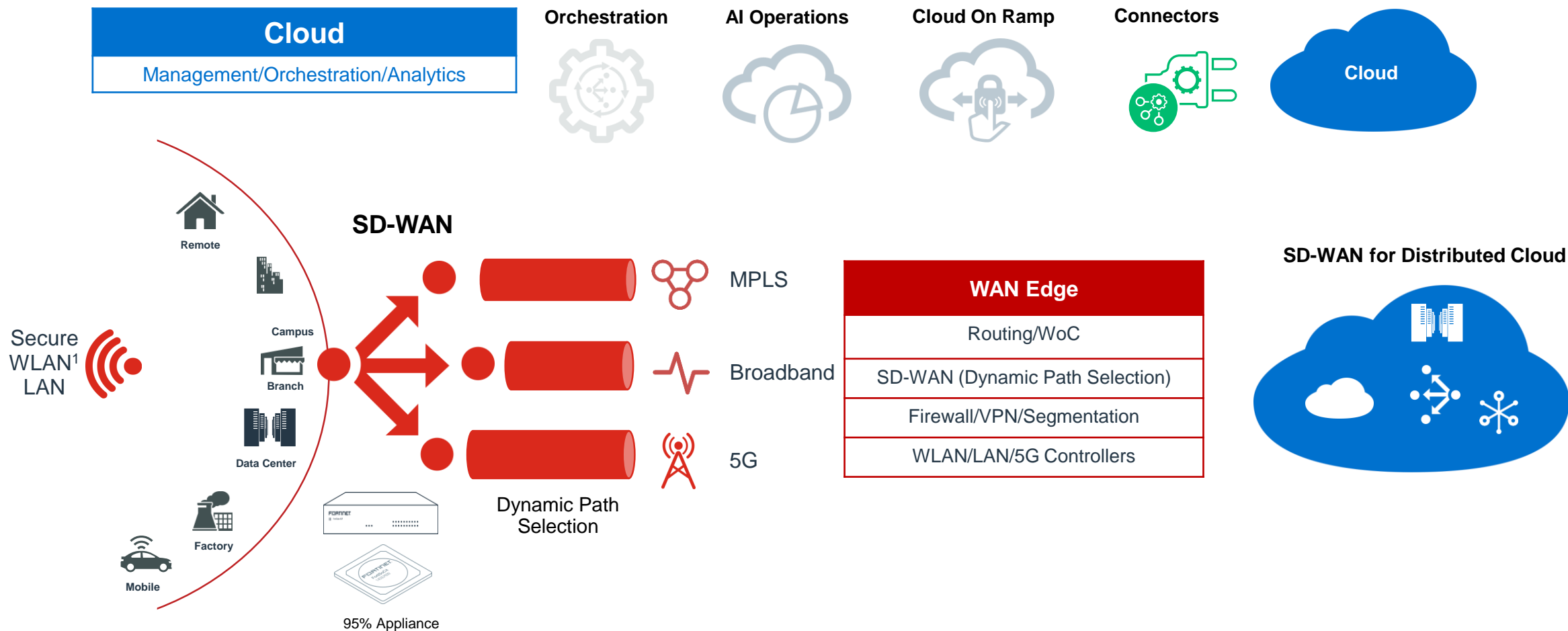
Ref: Gartner Emerging Technology Analysis: SASE Poised to Cause Evolution of Network Security

SASE Definition – Core Capabilities

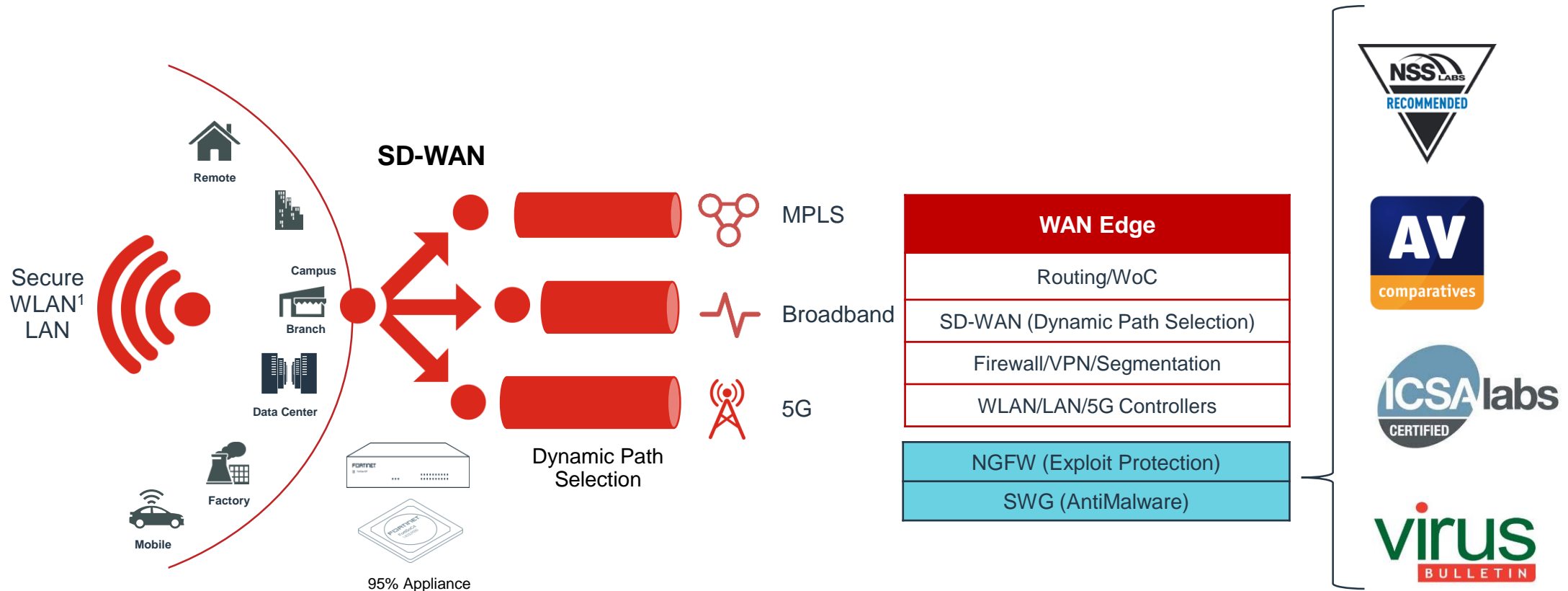
Core Capabilities	ZTNA ¹ 	SD-WAN 	FWaaS 	SWGaaS 	CASB 
Consumption Model	<ul style="list-style-type: none"> • API's • Cloud • Token 	<ul style="list-style-type: none"> • Appliance • uCPE 	Increasing Cloud Bias ¹ 		
Use Case	User Authentication to the Application	Dynamic Path Selection	Firewall as a Service	Secure Web gateway as a Service (Web Filtering)	Cloud Access Security Broker

¹Fortinet View

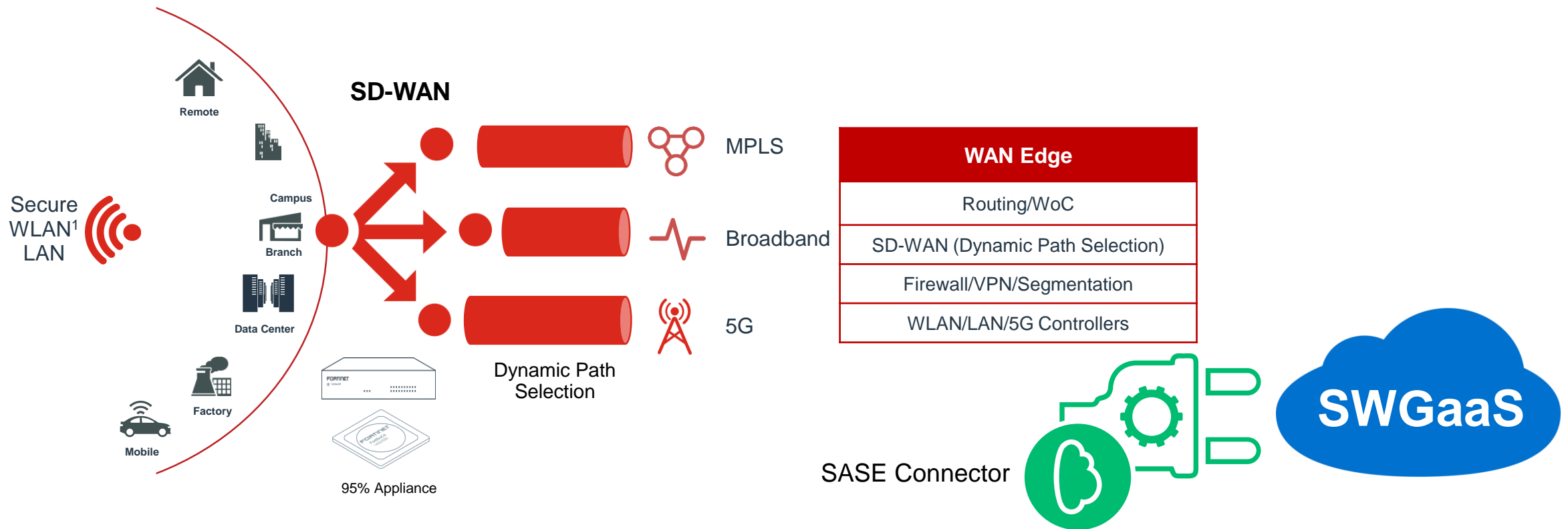
SD-WAN has to sit on the EDGE of the Customer Network



Too Many Security Offerings are not Tested/Certified

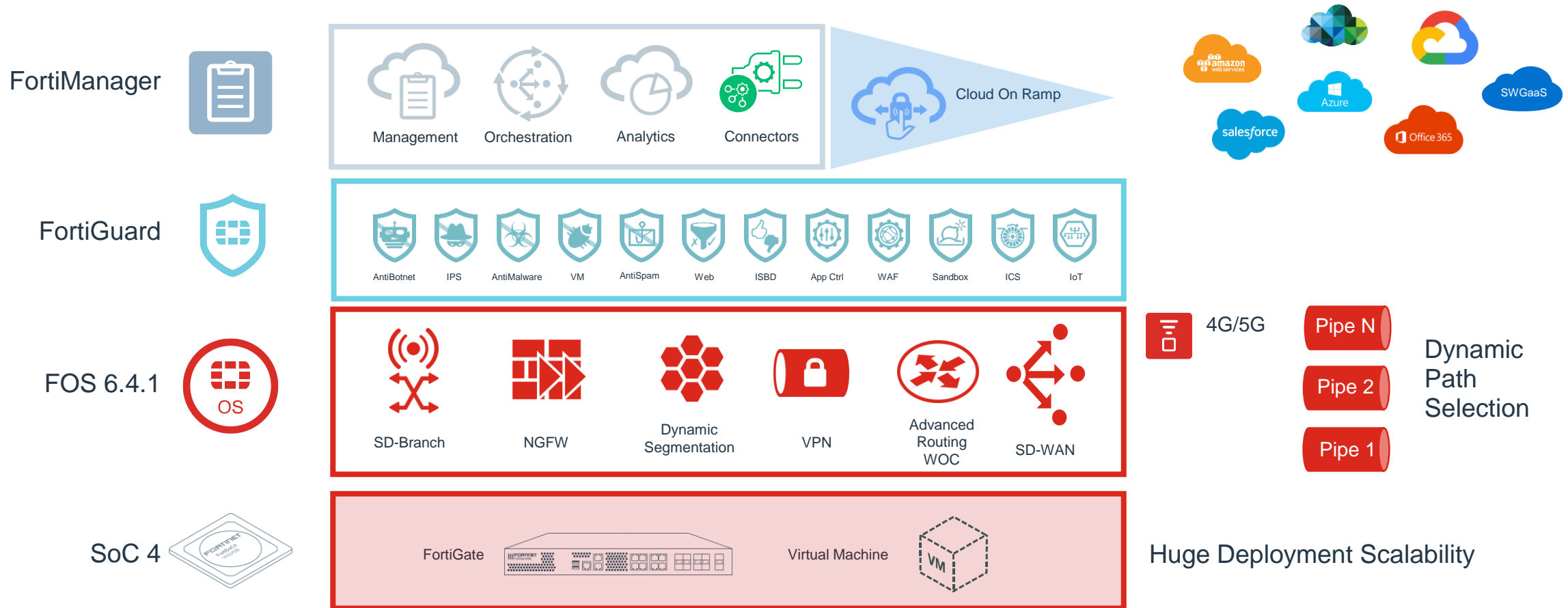


Too Many Security Offerings are not Tested/Certified



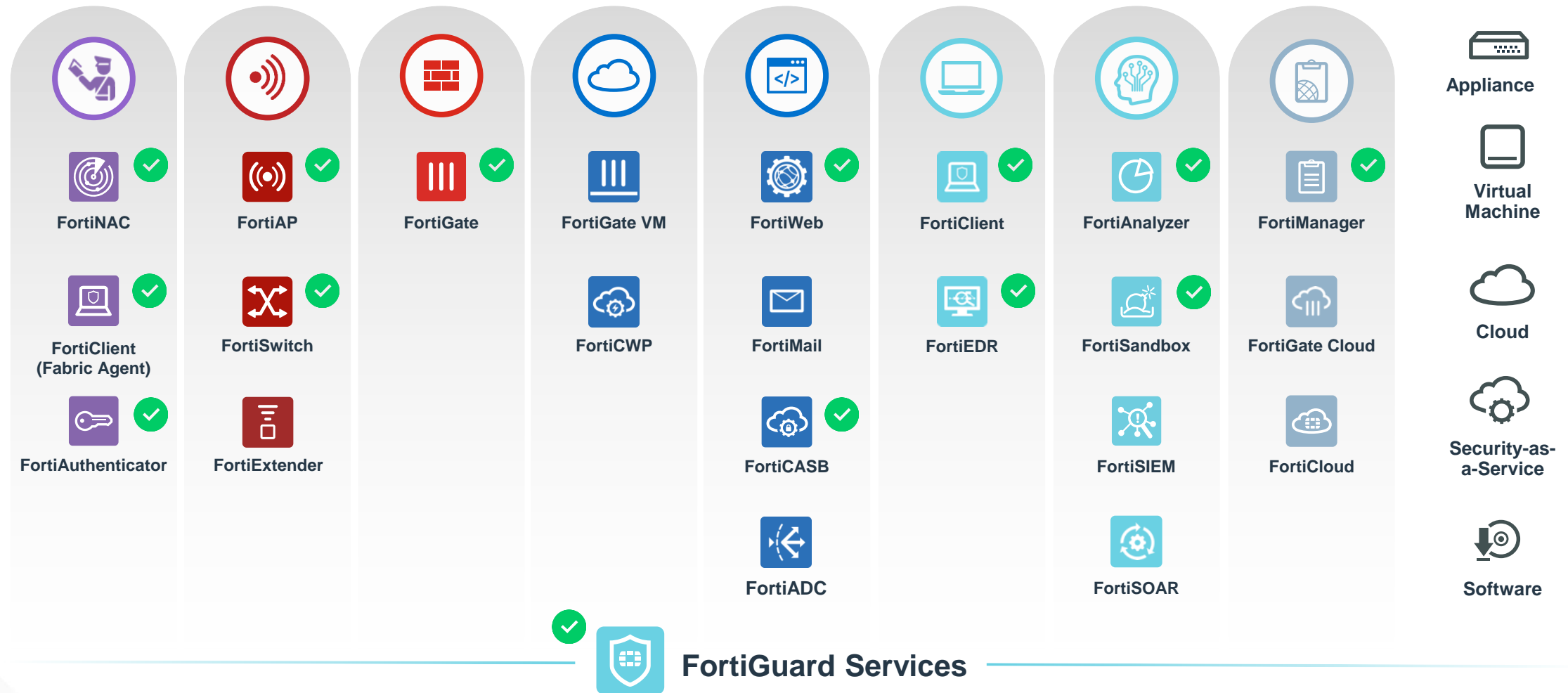
Fortinet SD-WAN Solution

Scales from Home to Branch to Distributed Cloud



SASE is a Specific Implementation of the Fabric

Core, Recommended and Optional Capabilities



FORTINET®

BMW i Motorsport
Official Partner

