



Fortinet Security Fabric a platformová bezpečnosť nielen pre Cloud

Zsolt Géczi, CEH

Regional account manager, Slovakia

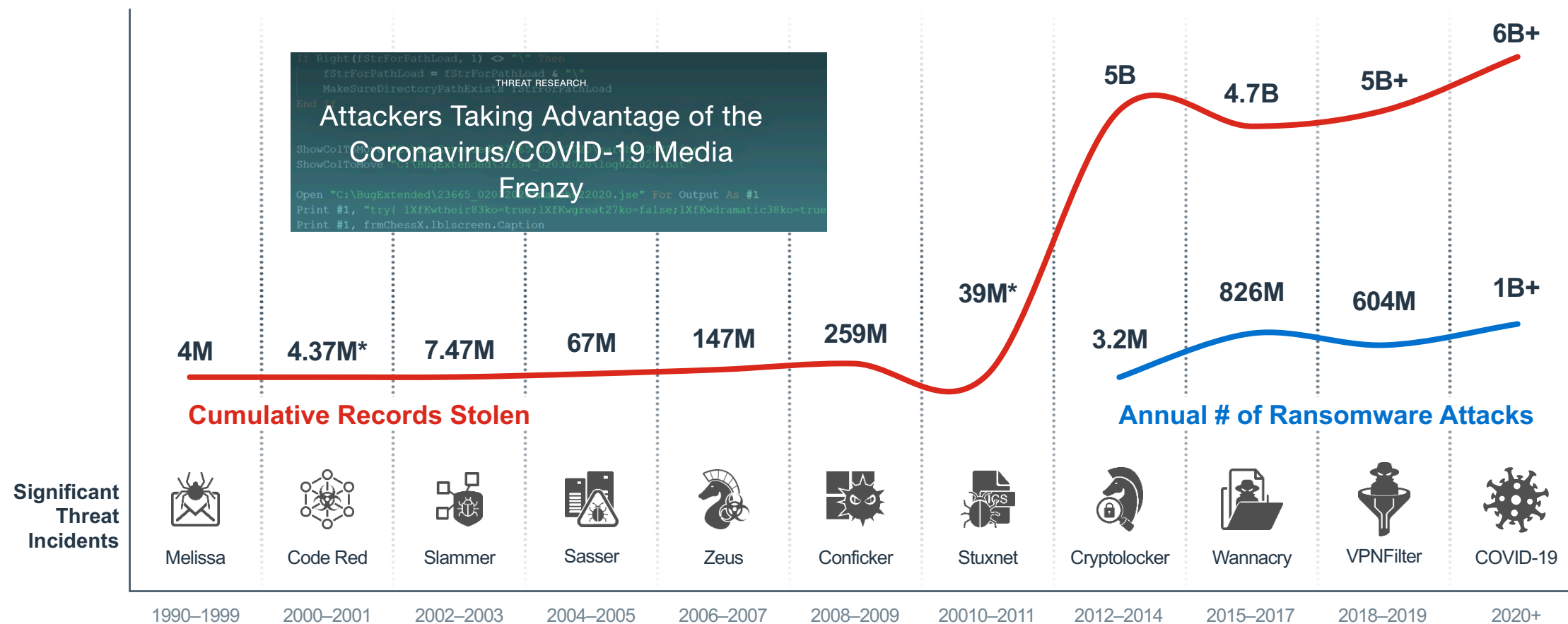
zgeczi@fortinet.com

BMW i Motorsport
Official Partner



Pokročilé hrozby sa nad'alej prispôsobujú

Väčšina hrozieb sa stále silne spolieha na sociálne inžinierstvo



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

Komplexnosť ekosystému je nevýhodou

Automatizácia sa ťažko dosiahne



**Too Many
Vendors**



**Too Many
Alerts**



**Manual &
Slow Response**



**Lack of
Trained People**

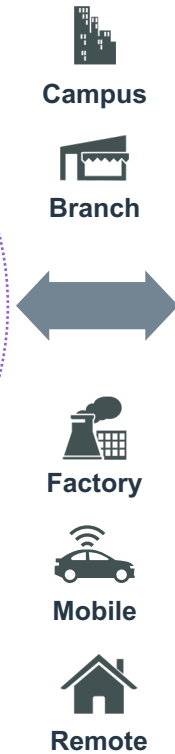


**Cost &
Complexity**

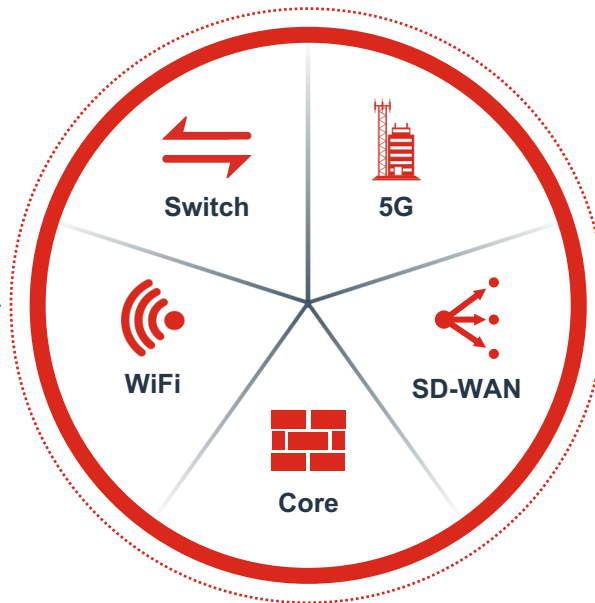
Perimeter je teraz cez celú Infraštruktúru

Fast and Secure Network Critical

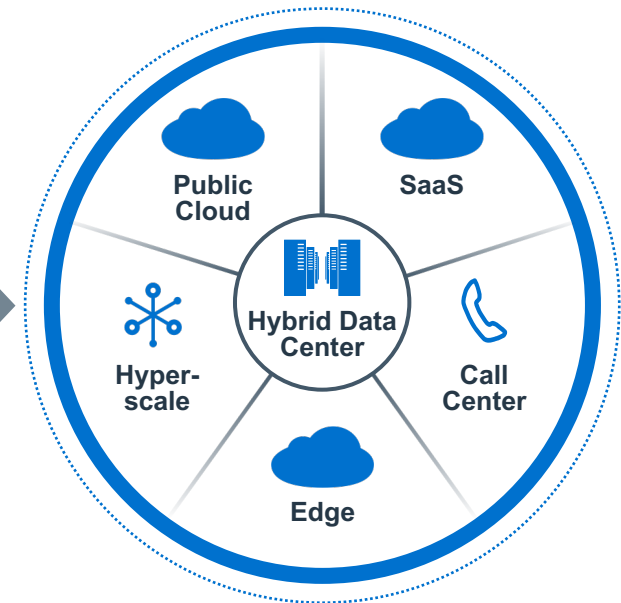
Užívatelia a Zariadenia



Sieť



Cloud



Platformový prístup ku kybernetickej bezpečnosti

Security-driven Networking



Akcelerovaná
konvergencia Siete a
Bezpečnosti

Zero Trust Network Access



Poznať a Kontrolovať
Každého a Všetko v Sieti
i mimo nej

Security Fabric



Management



Ecosystem

Dynamic Cloud Security



Bezpečnosť ktorá
nasleduje Vaše
Aplikácie a Dáta

AI-driven Security Operations



Automaticky predchádzať
kyber hrozbám, odhaľovať
ich a reagovať na ne



Appliance



Virtual
Machine



Hosted
(SaaS)



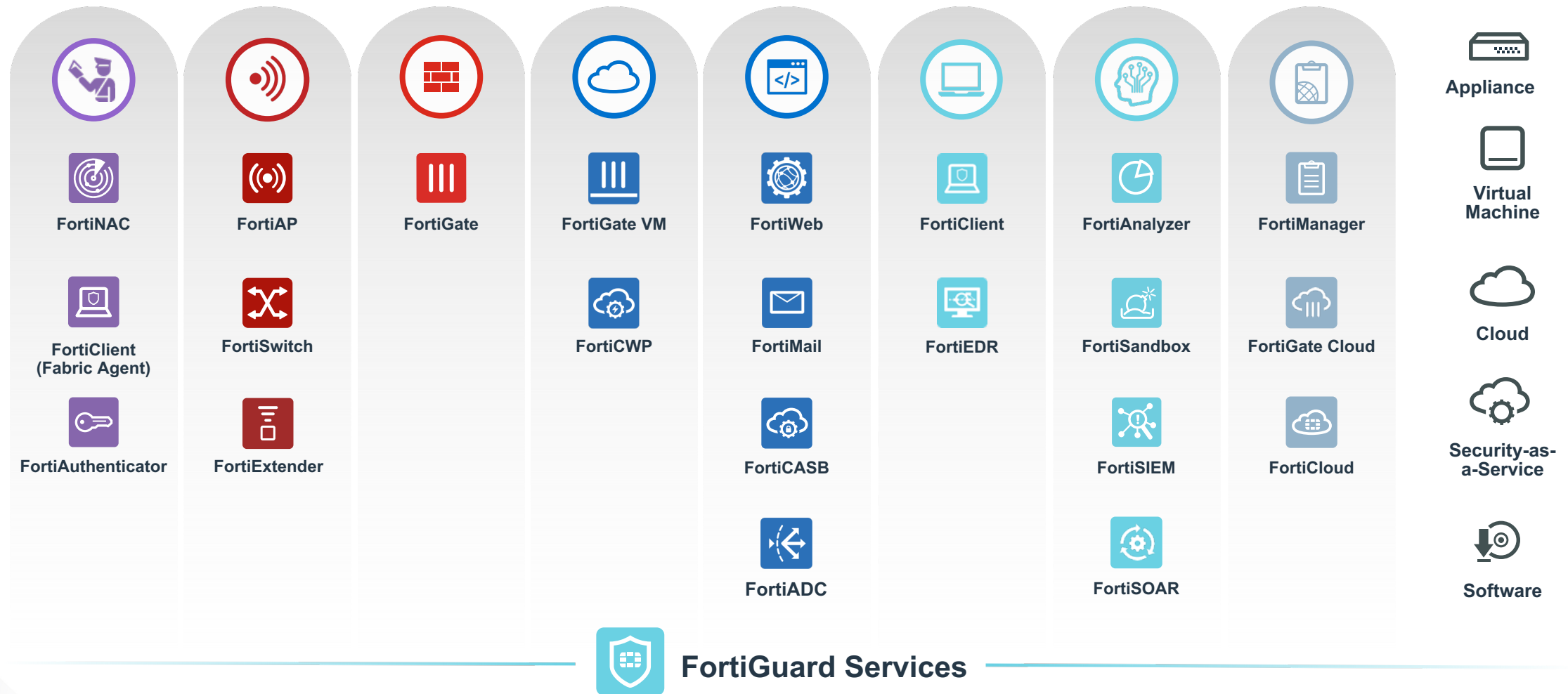
Cloud



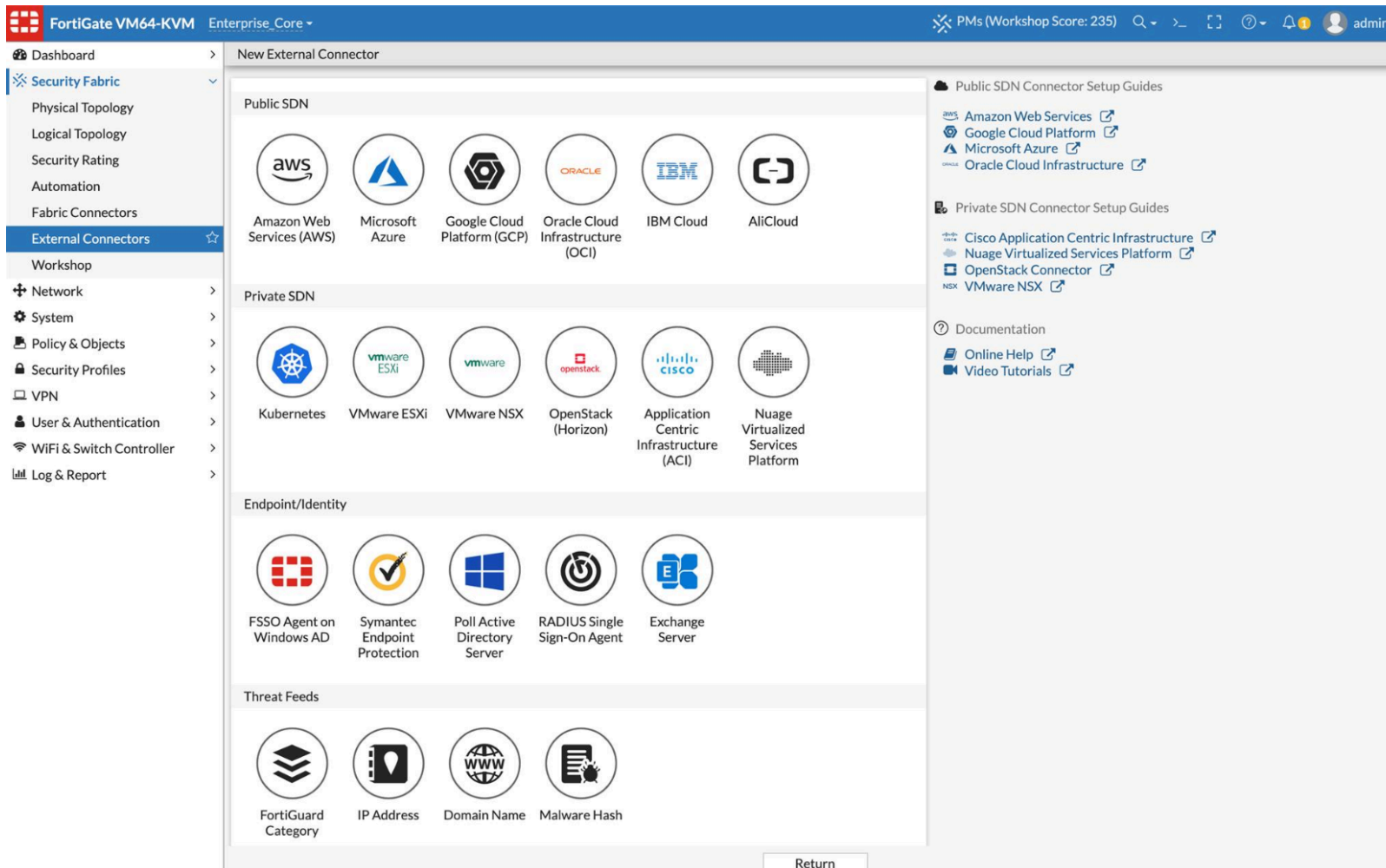
Container

Najširšia end-to-end platforma kybernetickej bezpečnosti

Dostupné v rôznych prevedeniach



Fabric Connectors



Cloud
(Dynamic Cloud Policy)

SDN
(Dynamic SDN Policy)

IaaS Visibility

ITSM

Threat Feeds

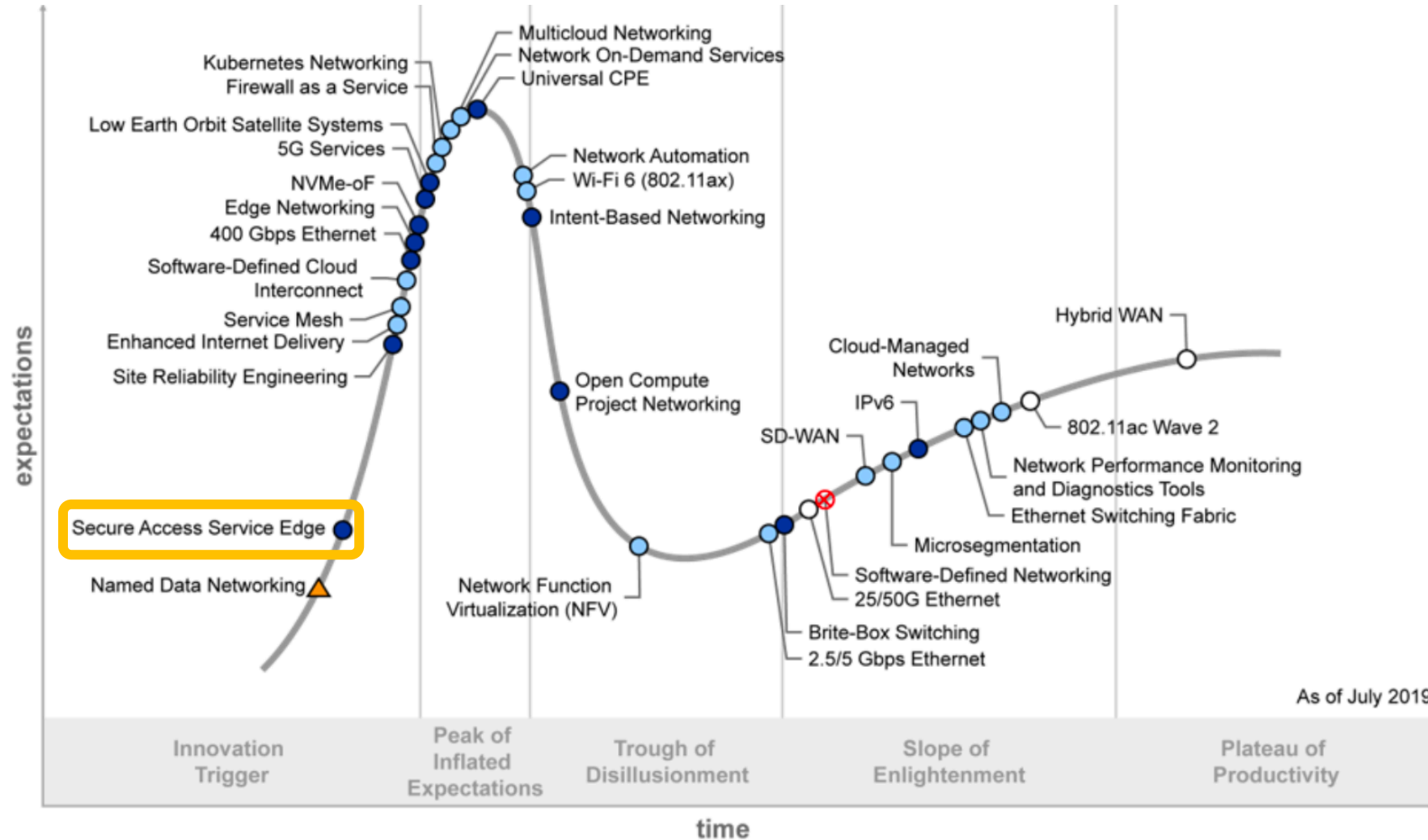
SSO/Identity

Endpoint CVE

Automation Action



Gartner Hype Cycle – Enterprise Networking 2019



Secure Access Service Edge (SASE) Definition

Gartner

This research note is restricted to the personal use of jmadison@fortinet.com.

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

Published: 22 October 2019 ID: G00450814

Analyst(s): Nat Smith, Neil MacDonald, Lawrence Orans, Joe Skorupa

The network security market is under pressure to adapt to digital transformation changes in end-user organizations. Product managers at network security vendors must evolve to deliver secure access service edge capabilities to remain relevant in coming years.

Key Findings

- Digital transformation, cloud adoption, edge computing and mobile mean that appliance-based network security models (designed originally to protect on-premises architectures) are being replaced.
- With demands for simplicity, scalability, flexibility and low latency, network security and WAN edge market segments are converging. The framework to handle this convergence is a cloud-based service delivery model known as secure access service edge (SASE, pronounced "sassy").
- SASE requires as-a-service offerings, with consumption-based pricing models and cloud-native, scalable architectures.

Recommendations

Product managers at network security vendors focused on emerging technology and trends impact on products and services must do the following:

- Adopt a flexible cloud-based architecture that gives buyers the flexibility to easily adapt their network security capabilities to changing end-user environments and use cases, particularly involving hybrid cloud and multicloud.
- Build out a network of distributed points of presence (POPs) through colocation facilities, service provider POPs and infrastructure as a service (IaaS) to reduce latency and improve performance for network security services.
- Introduce product offerings, priced as short-term subscription services, and compensate sales teams accordingly.

This research note is restricted to the personal use of jmadison@fortinet.com.

The secure access service edge is an emerging offering combining comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA — see Note 1), with comprehensive WAN capabilities to support the dynamic secure access needs of organizations.

SASE capabilities are delivered largely as cloud-based services driven by the identity of the entity, real-time context, organization security/compliance policies and continuous assessment of risk/trust (see "Seven Imperatives to Adopt a CARTA Strategic Approach") throughout the sessions. Identities of entities can be associated with people, groups of people (branch offices), devices, applications, services, Internet of Things (IoT) systems or edge computing locations.

Core capabilities: SD-WAN, SWG, CASB, ZTNA and FWaaS, all with the ability to identify sensitive data or malware and the ability to decrypt content at line speed, at scale with continuous monitoring of sessions for risk and trust levels.

Recommended capabilities: Web application and API protection (WAAP), remote browser isolation, recursive DNS, network sandbox, API-based access to SaaS for data context, and support for managed and unmanaged devices.

Optional capabilities: Wi-Fi hot spot protection, network obfuscation/dispersion, legacy VPN and edge compute protection (offline or cached protection)

SASE vo svojej súčasnej fáze na trhu predstavuje prechod od nasadenia „ťažkých pobočiek“ k „tenkými pobočkám“ s podporou „silného cloudu“.

SASE - Security Access Services Edge

Figure 1. SASE — Convergence and Inversion of the Network and Security Architectures

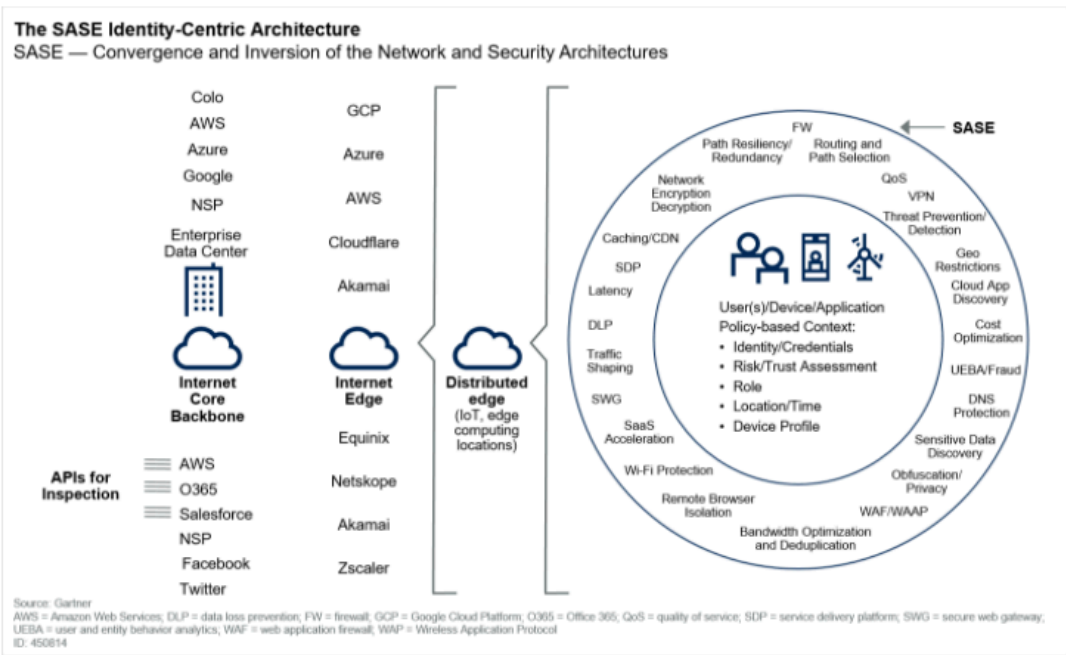


Figure 2. Heavy-Branch Shifting to Thin-Branch/Heavy-Cloud Model

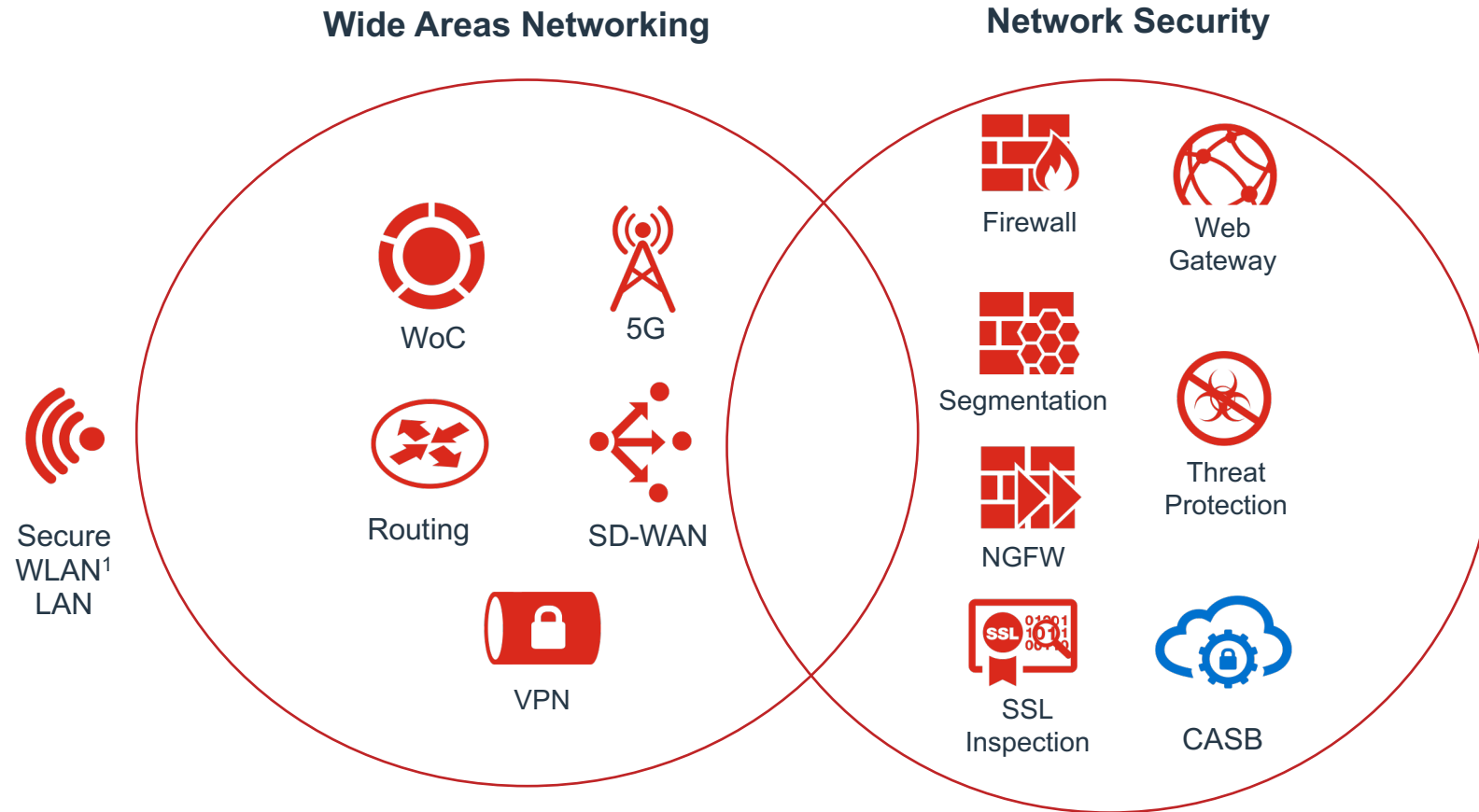
From Traditional Heavy-Branch to Cloud-Centric Thin-Branch/SASE Models

Heavy-Branch Model Shifting to Thin-Branch/Heavy-Cloud Model

Heavy Branch	Thin Branch	Heavy Cloud
Router	SD-WAN/FW	CASB
VPN	Simple WOC	FWaaS With IPS
FW		ZTNA/SDP
WOC		SWG
SWG		DLP
DLP		Threat
		VPN
		WAAPaaS
		Sandbox
		RBI

Source: Gartner
CASB = cloud access security broker; DLP = data loss prevention; FW = firewall; FWaaS = firewall as a service; IPS = intrusion prevention system; RBI = remote browser isolation; SDP = software-defined perimeter; SD-WAN = software-defined WAN; SWG = secure web gateway; threat = threat intelligence; VPN = virtual private network; WAAPaaS = web application and API protection as a service; WOC = WAN optimization controller; ZTNA = zero trust network access
ID: 450814

Základná charakteristika SASE



Novinkou je služba zabezpečeného prístupu, ktorá kombinuje komplexné funkcie zabezpečenia siete s komplexnými funkciami WAN

Cieľ: podporiť potreby organizácií v oblasti dynamického zabezpečeného prístupu

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

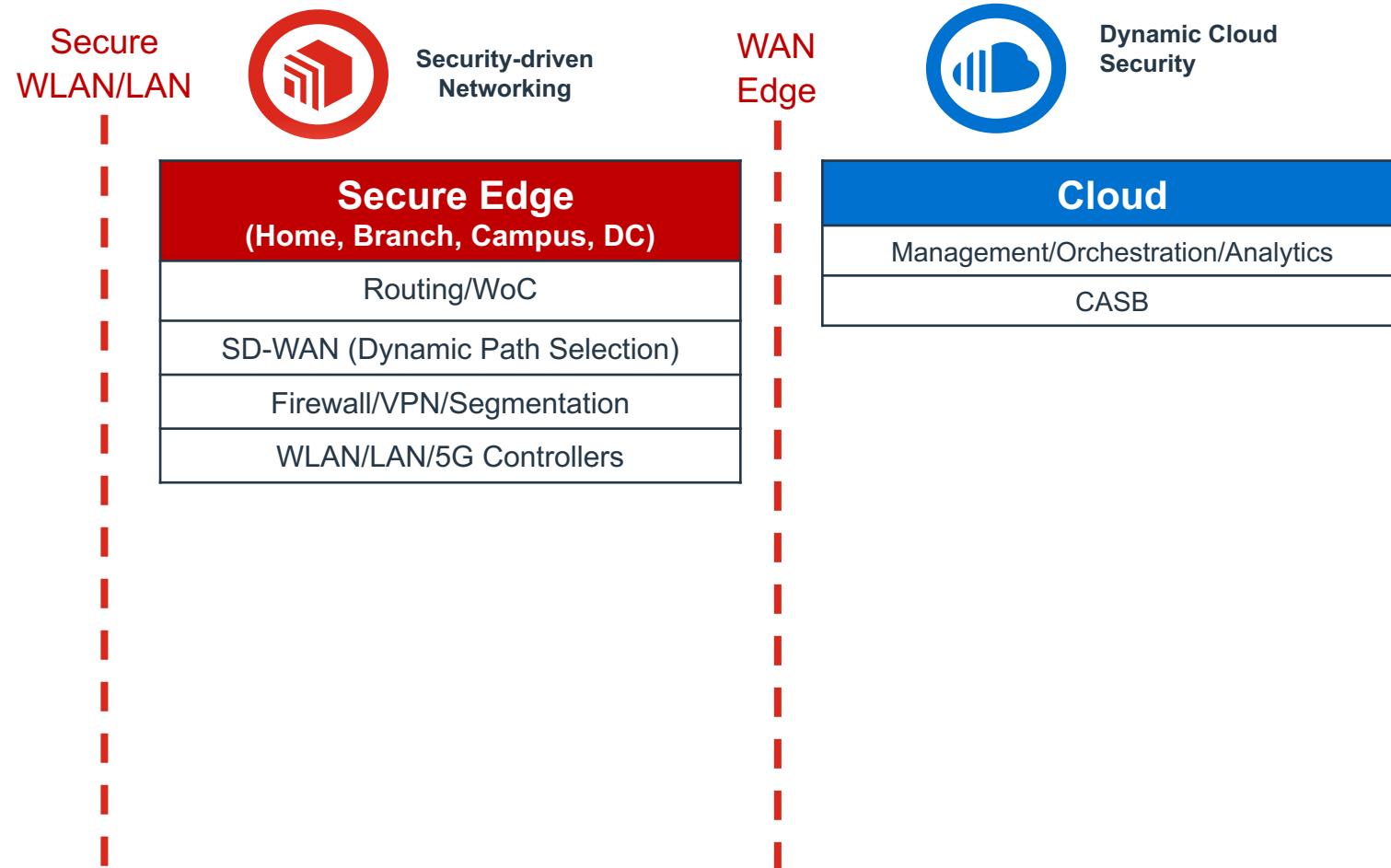
¹Fortinet View

SASE – Základné Funkcionality

	ZTNA ¹	SD-WAN	FWaaS	SWGaaS	CASB
Core Capabilities					
Consumption Model	• API's • Cloud • Token	• 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

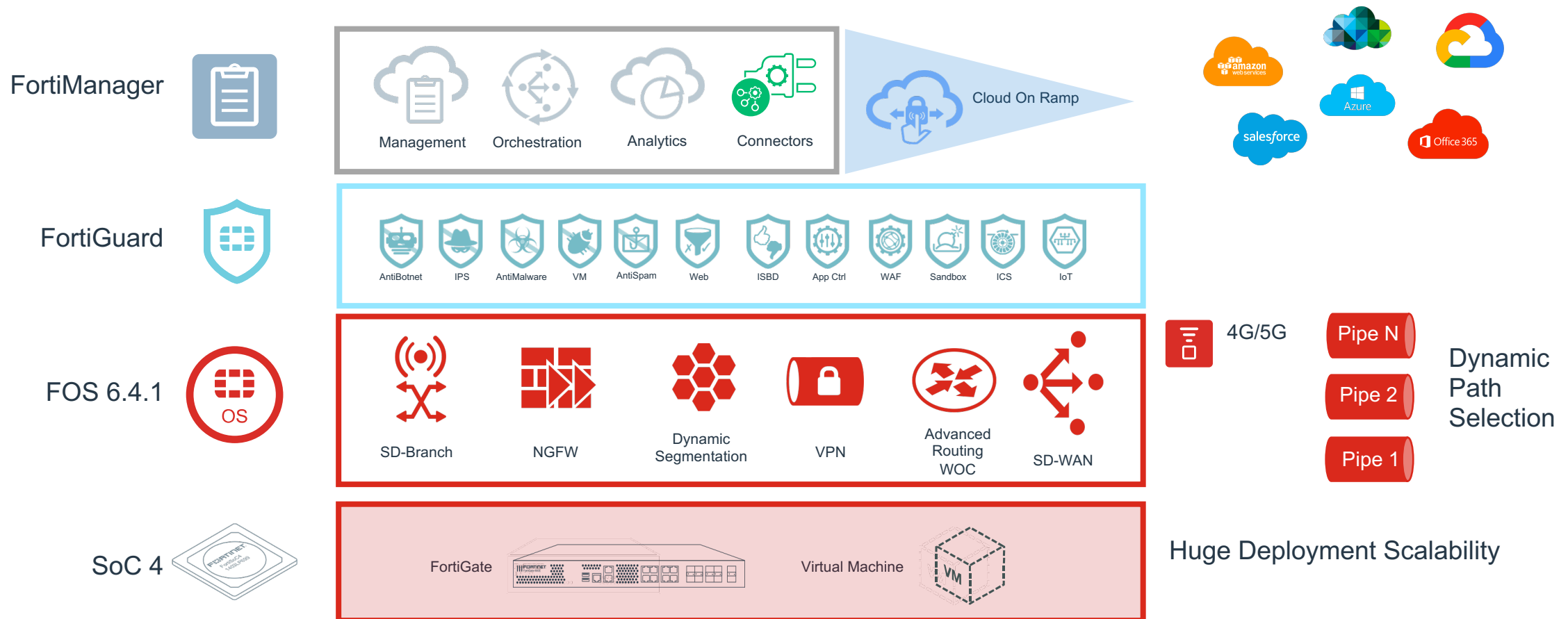
¹Fortinet View

SASE Základná Funkcionalita: SD-WAN



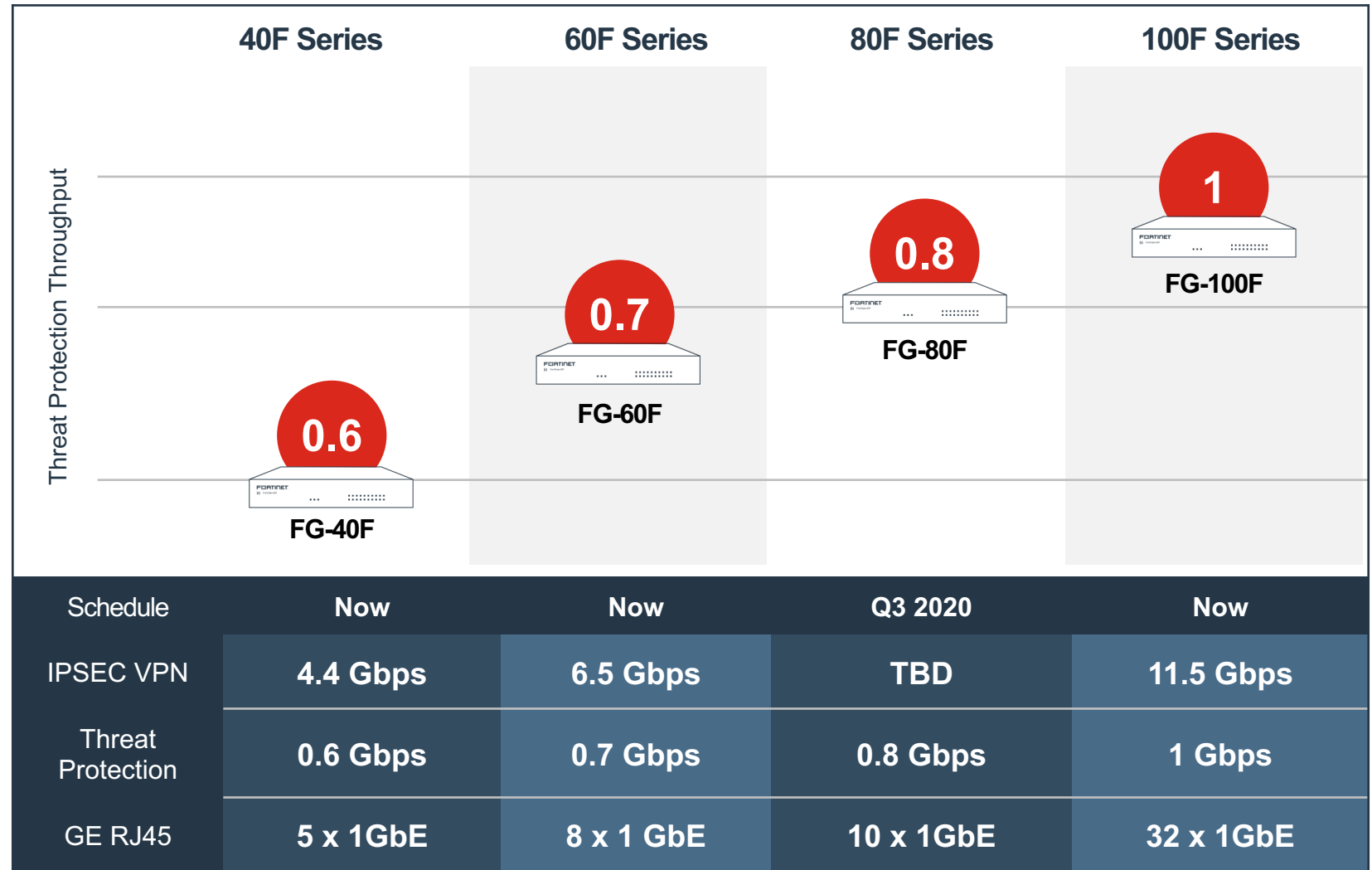
Market Leading Secure SD-WAN

Škálovateľné od Home-office, cez Pobočku až po Distribuovaný Cloud



FortiGate Secure SD-WAN Powered by SOC4

System on a Chip 4 (SoC4)



FortiGate 60F Security Compute Rating

Similar Priced SD-WAN and NGFW Products

Specification	FortiGate 60F (SOC4 ASIC)	Industry Average	Security Compute Rating ¹	Palo Alto Networks PA-220	Checkpoint SG-1550	Cisco Meraki MX67	VMWare VeloCloud 520	Juniper SRX 340
Firewall	10Gbps	1.23Gbps	8x	0.5Gbps	1Gbps	0.45Gbps	Not Published	3Gbps
IPsec VPN	6.5Gbps	0.48Gbps	13x	0.1Gbps	1.3Gbps	0.2Gbps	0.2Gbps	0.6Gbps
Threat prevention	0.70Gbps	0.18Gbps	4x	0.15Gbps	0.45Gbps	0.3Gbps	Not Published	Not Published
SSL Inspection	0.75Gbps	0.065Gbps	11x	0.065Gbps	Not Published	Not Published	Not Published	Not Published
Concurrent Sessions	700,000	273333	3x	64,000	500,000	Not Published	Not Published	256,000
Connections per second	35,000	7650	4x	4200	14,000	Not Published	2400	10,000

FortiOS – Enable Advance SD-WAN and Routing Capabilities

WAN Path Control



Application Identification
Active Path Measurement
Dynamic Path Selection

WAN Path Remediation



Forward Error Correction
Packet based Distribution
Flexible SLA

Segmentation



Multi-Tenancy (VDOM)
Identity-Based Policy
VRF Enabled

Secure Connectivity



Automated VPN Overlay
Accelerated IPSEC Tunnels
On-Demand Full Mesh

Fabric Management Center – Single Pane of Glass

Centralized Management



SD-WAN Orchestrator
Intuitive Work-flows
Multi-Tenancy

Analytics and Reporting



Application Analytics
WAN path Utilization
Anomaly identification

Zero Touch Deployment



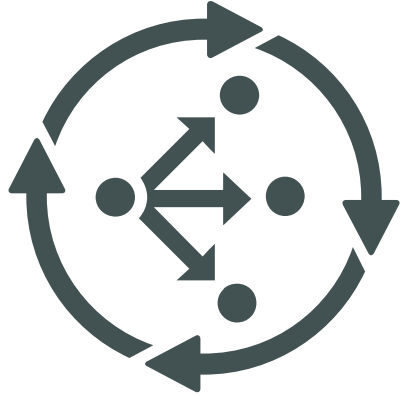
Zero Touch Provisioning
SD-WAN and SD-Branch
Firmware Ratification

Compliance



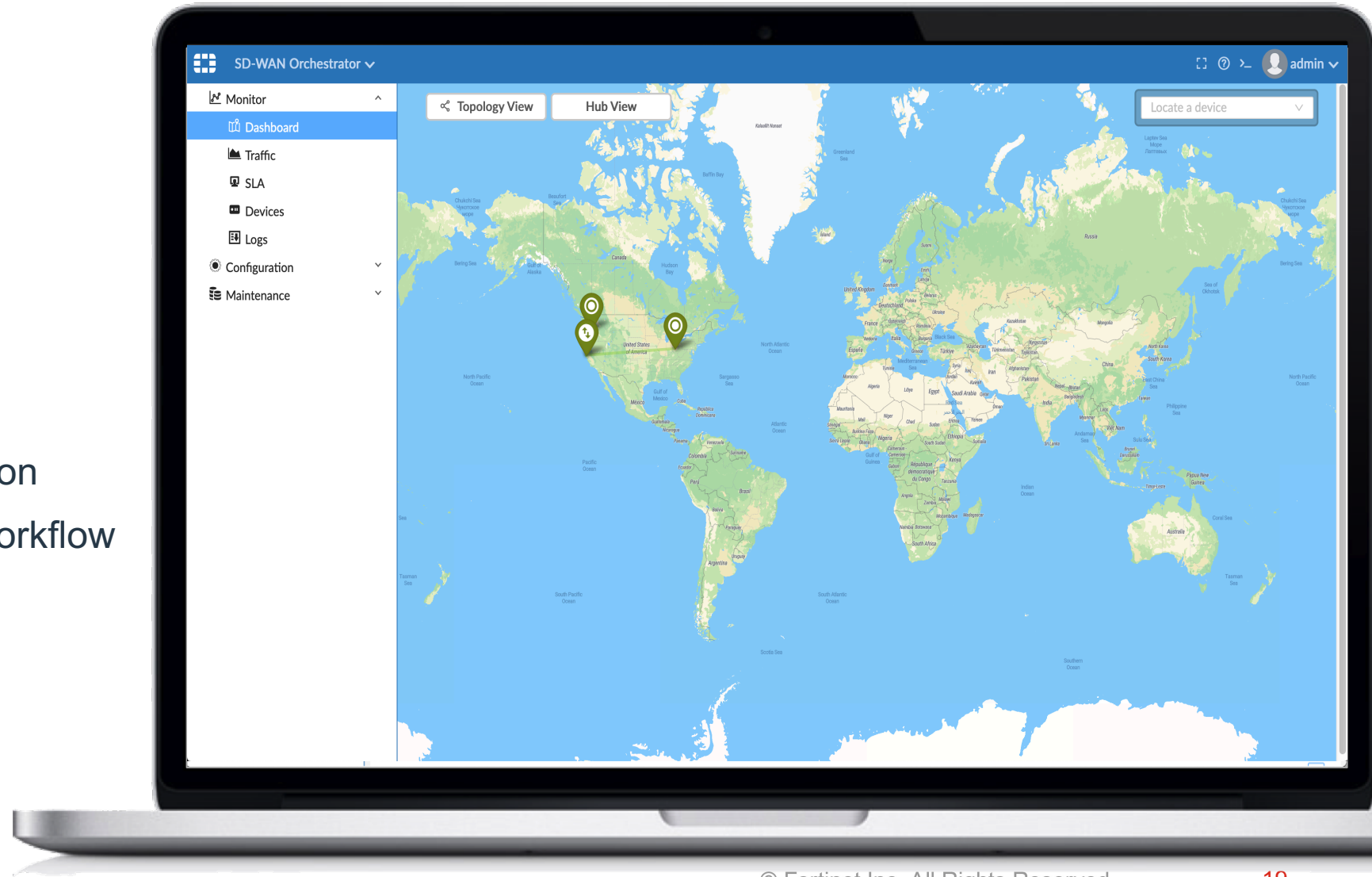
Security Rating Service
PCI/HIPAA Frameworks
Security Best Practices

New SD-WAN Orchestrator to Simplify WAN Operations



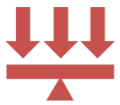
SD-WAN Orchestrator

- Overlay Control & Automation
- Simplified, Configuration Workflow
- Intuitive Business policies
- Integrated Analytics & Visualizations



Enhanced SD-WAN Analytics for Faster trouble-shooting

- Immediately understand the benefit of enabling SD-WAN across multiple WAN interfaces



Link Availability



Performance SLA



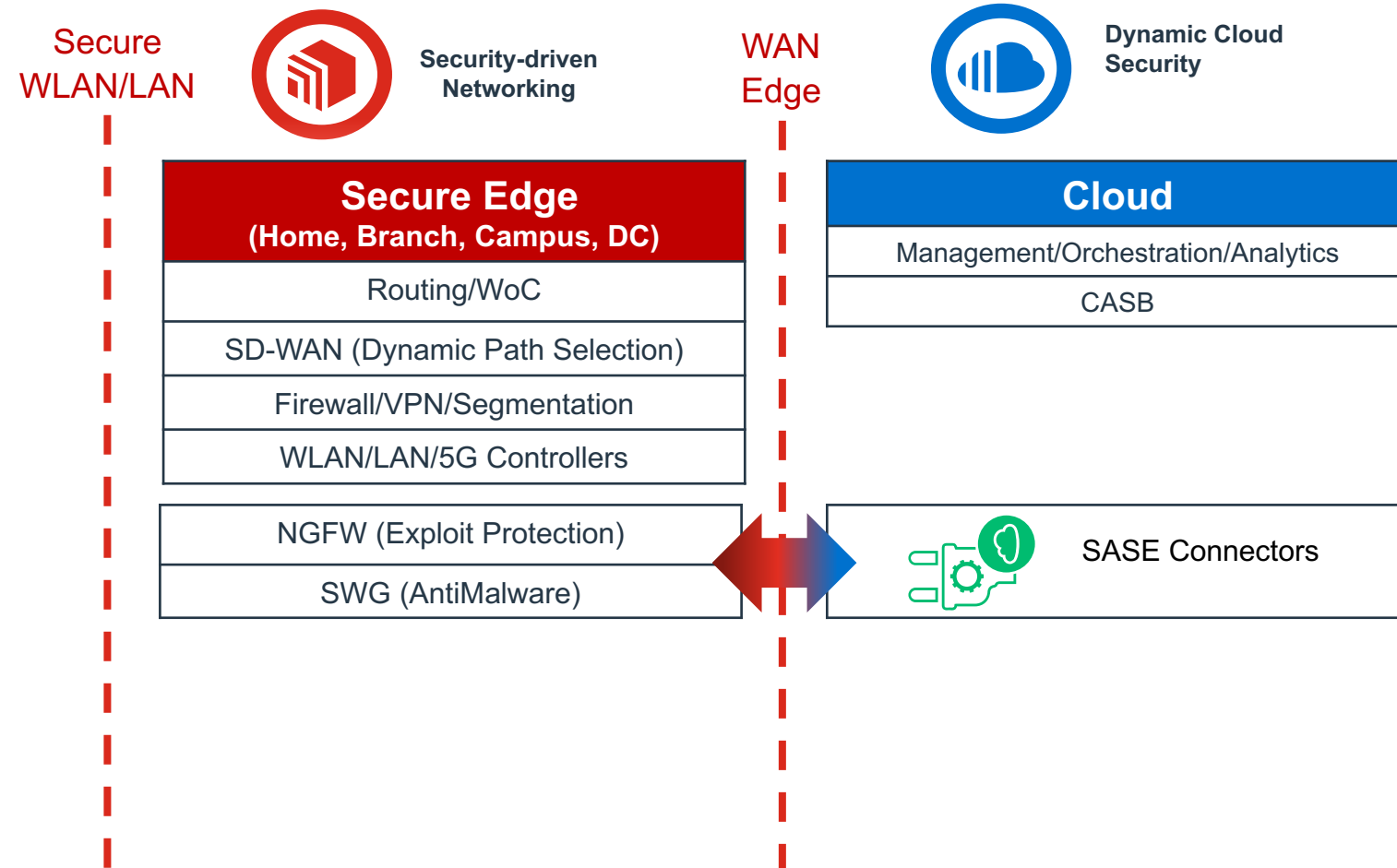
Bandwidth & Traffic Stats



Troubleshoot & Debug



SASE Základná Funkcionalita: SWGaaS



FortiGuard Labs & Subscriptions

Visibility

Global Real-time Intelligence


Firewalls


Web


Emails


Endpoints


Sandbox


4M+
Sensors


WORLD ECONOMIC FORUM
CYBERSECURITY


CYBER THREAT ALLIANCE


INTERPOL


EUROPOL


NATO
OTAN


200+

Threat Intelligence Partnerships

FORTINET

Innovation


FortiGuard Labs


Largest AI/ML
5.5M Nodes


100B+
Events Analyzed
Per Day


820+
Zero-day
Discovered
to Date

Most Certified Protection



Fortinet Confidential

Actionable Threat Intelligence



Security Subscriptions


App Control


AV


IPS


URL


IoT


IoC


Security Rating


Sandbox


Security-driven Networking


Dynamic Cloud


Zero-Trust Network Access


AI-driven SOC

Response


Adversary Playbooks


Zero-day Research


Intelligence Briefs

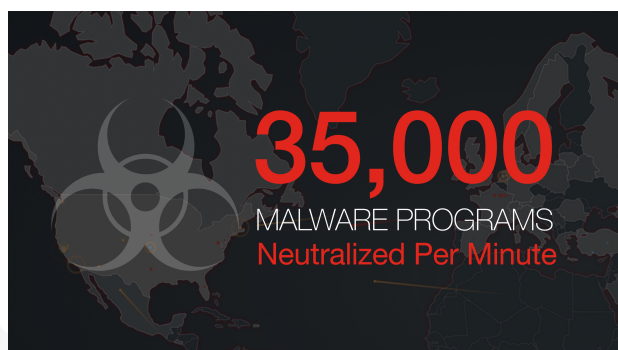
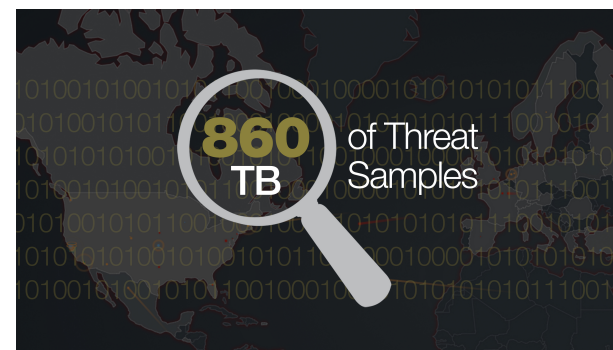
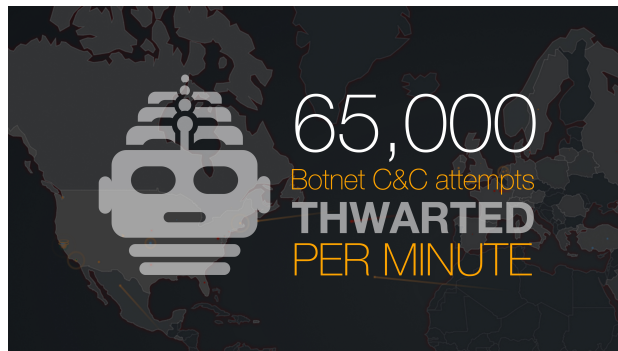

Threat Signal


Threat Blogs

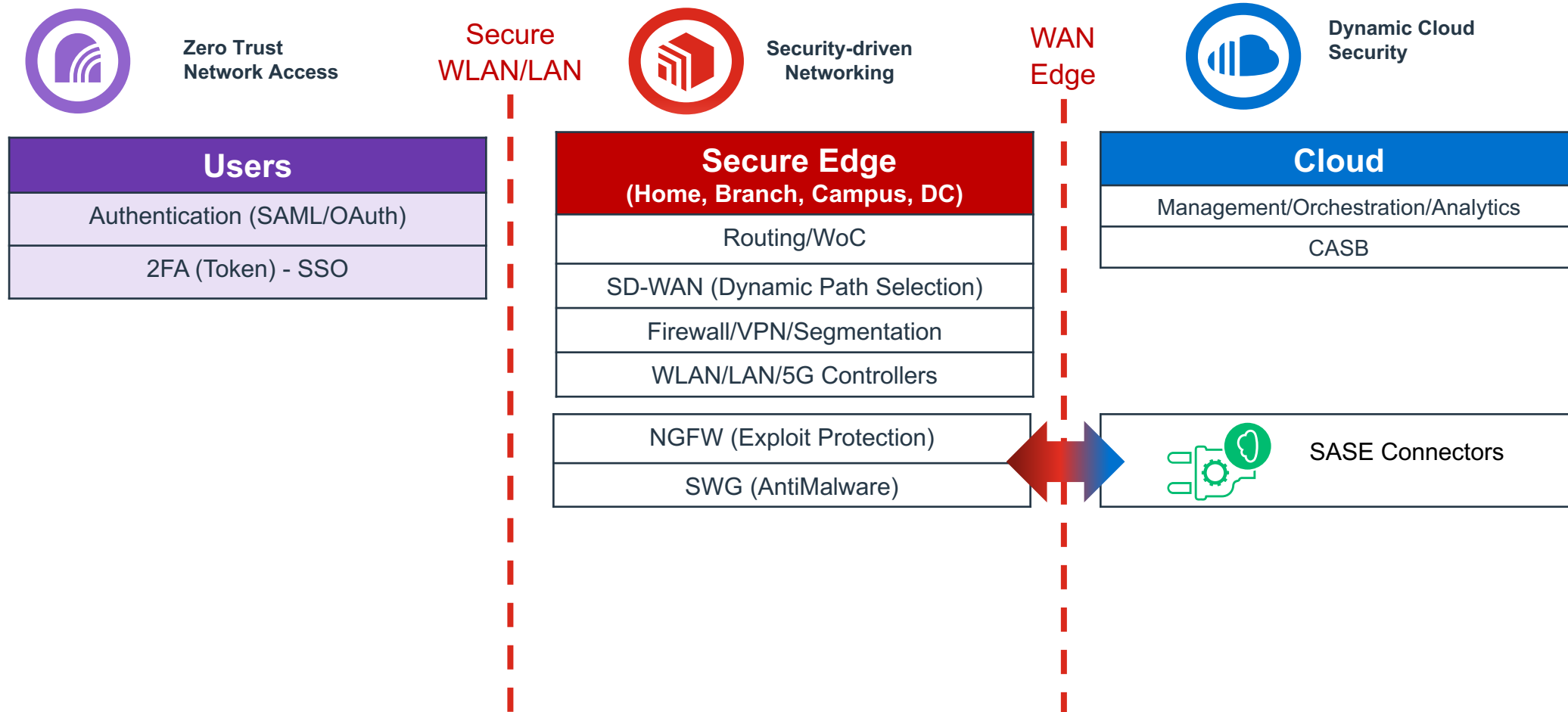

Threat Podcasts

© Fortinet Inc. All Rights Reserved.

FortiGuard v číslech

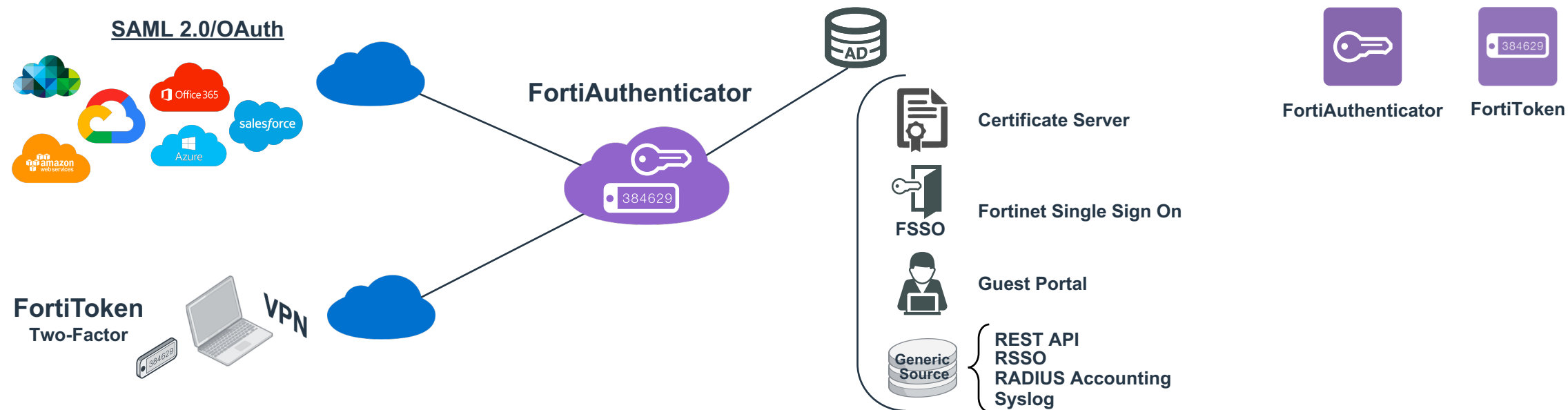


SASE Základná Funkcionalita: ZTNA



Zero Trust Network Access—Identifikácia užívateľa

Knowing **who** is on the network



Authentication

Establish identity through user log-in, certificate, and/or multifactor input

Role-based Access

Provide information from authentication source for use in privileged access

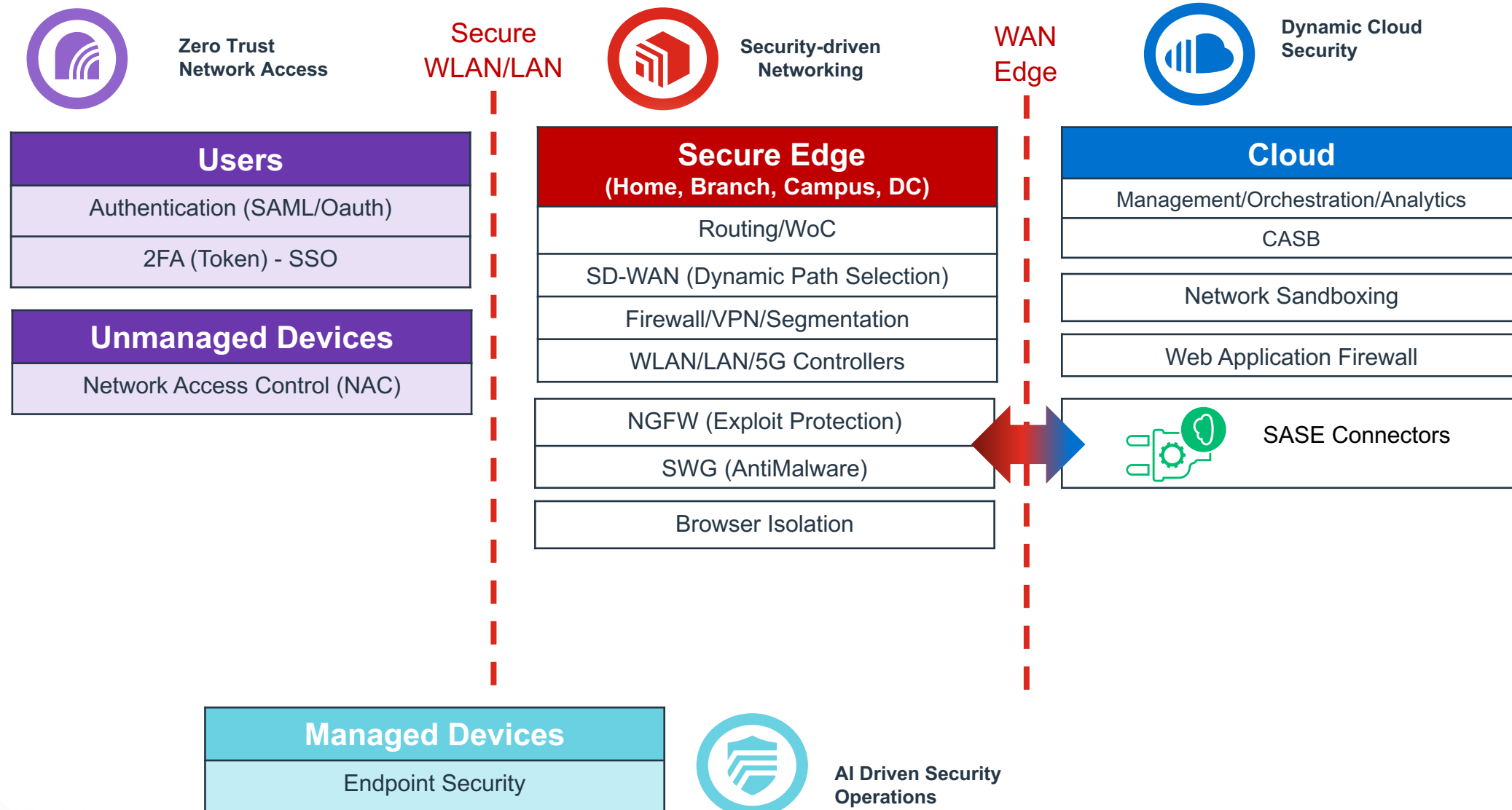
Single Sign On

Reduce end user fatigue while maintaining security

SASE Definition – Odporúčané Funkcionalita

Recommended Capabilities	Unmanaged Devices 	Managed Devices 	Network Sandboxing 	Browser Isolation 	WAF/API 
Consumption Model	• Appliance • Virtual Machine • Cloud	• Agent • Cloud	• Appliance • Virtual Machine • Cloud • SaaS	• Appliance • Virtual Machine	• Appliance • Virtual Machine • Cloud • SaaS
Use Case	Network Access Control (NAC) Device and User Identity + Context	Endpoint Protection Platform (EPP) + Endpoint Detection and Response (EDR)	Advanced Malware Detection	Secure Web gateway as a Service (Web Filtering)	Web Application Firewall and API Security

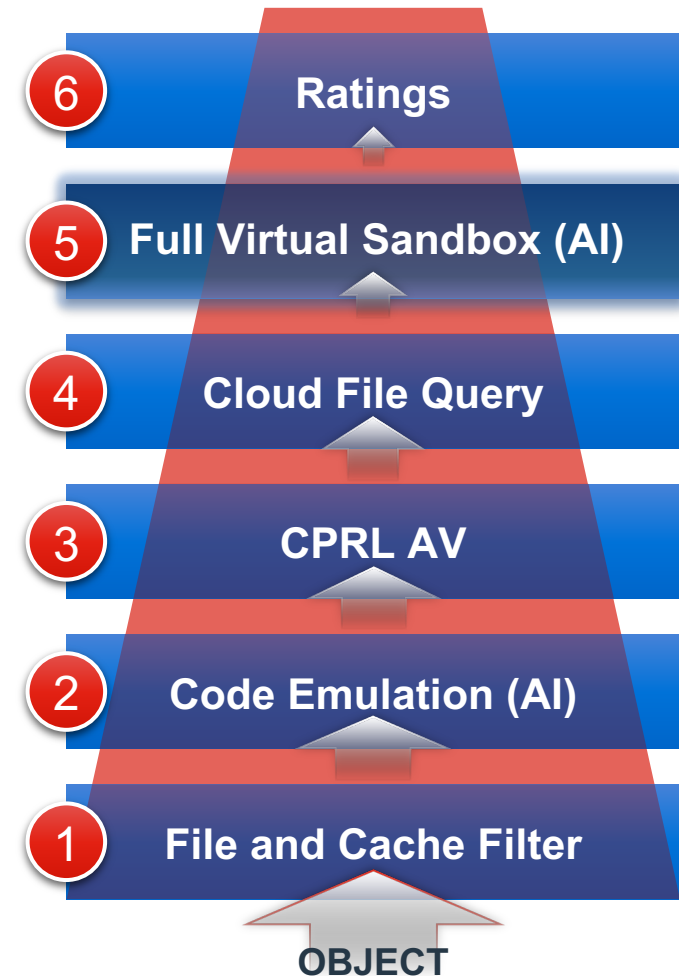
SASE Odporúčané Funkcionalita

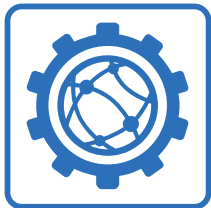


FortiSandbox: Advanced Threat Protection



- Examines real-time behavior, not just static attributes
- Runs files and follows URLs in a virtual environment
- Applies ML models to behavior to assign risk
- Returns risk ratings and shares dynamic threat intelligence
- Integrated across the digital attack surface

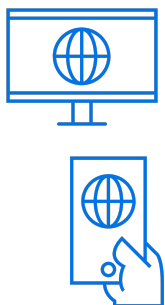




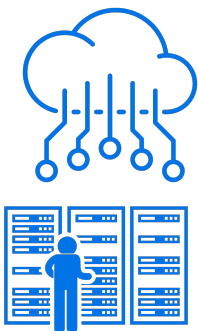
FortiWeb Ochrana Webových Aplikací a API

Protection for Web Applications and APIs everywhere you deploy them

Your applications and APIs



Deployed in the cloud or on-premise



Delivering Line of Business Capabilities



To your users, anywhere, from any device



Protected by FortiWeb's unique AI-powered detection engine, that minimizes false positives and reduces administrative overhead



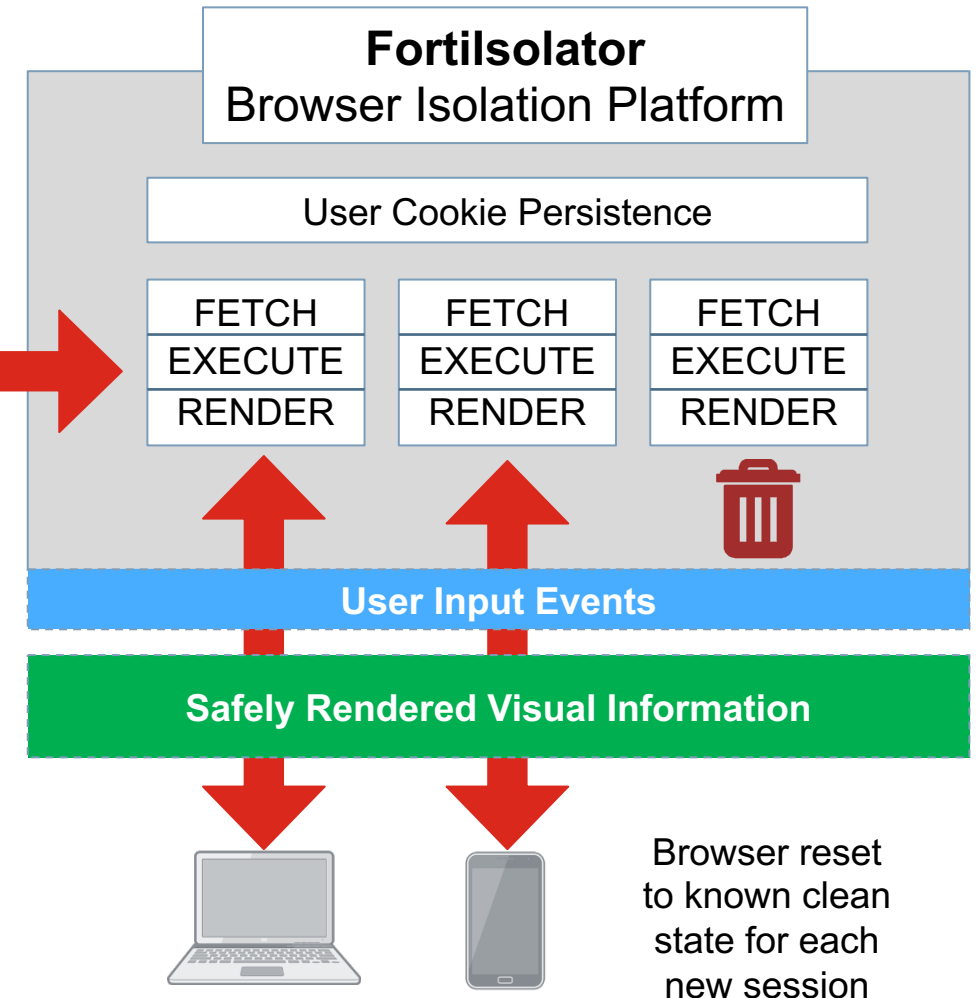
Extending the protection of Fortinet's Security Fabric across your application attack surface.



Fortisolator: Bezpečné Browsovanie Užívateľov

- 
- Separates the browser session from the device
 - Remotely renders safe content to the end user
 - Supports any HTML 5 compatible browser
 - Protects the user from malicious sites and code

Malicious Web Page

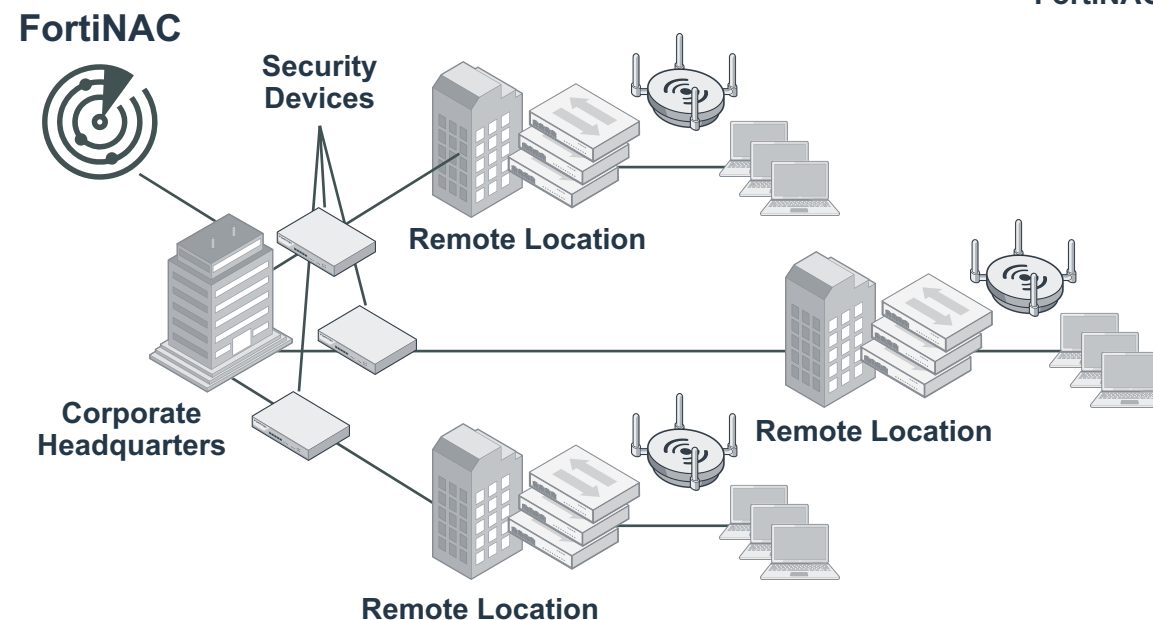
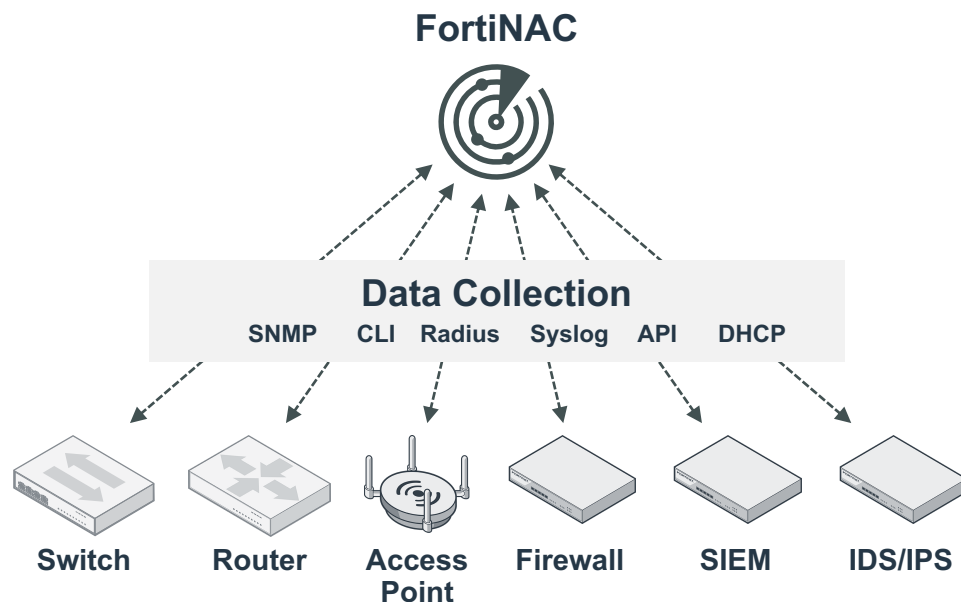


Zero Trust Network Access - Identifikácia zariadení

Vedieť, čo je v sieti



FortiNAC



Visibility

Device identification, profiling,
and vulnerability scanning

Dynamic Control

Dynamic micro-segmentation
Supports intent-based
segmentation

Continuous Response

Automated response and
network orchestration
Extends Security Fabric

FortiClient: Vizibilita, kontrola a bezpečnost'



- Assess device state, communicate to the Security Fabric
- Provide secure remote access to the corporate network
- Protect the end user device with traditional EPP stack



FortiEDR: Protect, Detect and Respond

Real-time Automated Security with Orchestrated Incident Response

✓ REAL-TIME PROACTIVE RISK MITIGATION

- Discover and track applications and IoT devices
- CVE and application rating data enrichment
- Risk based proactive policies enabling attack surface reduction

✓ REAL-TIME ORCHESTRATED INCIDENT RESPONSE

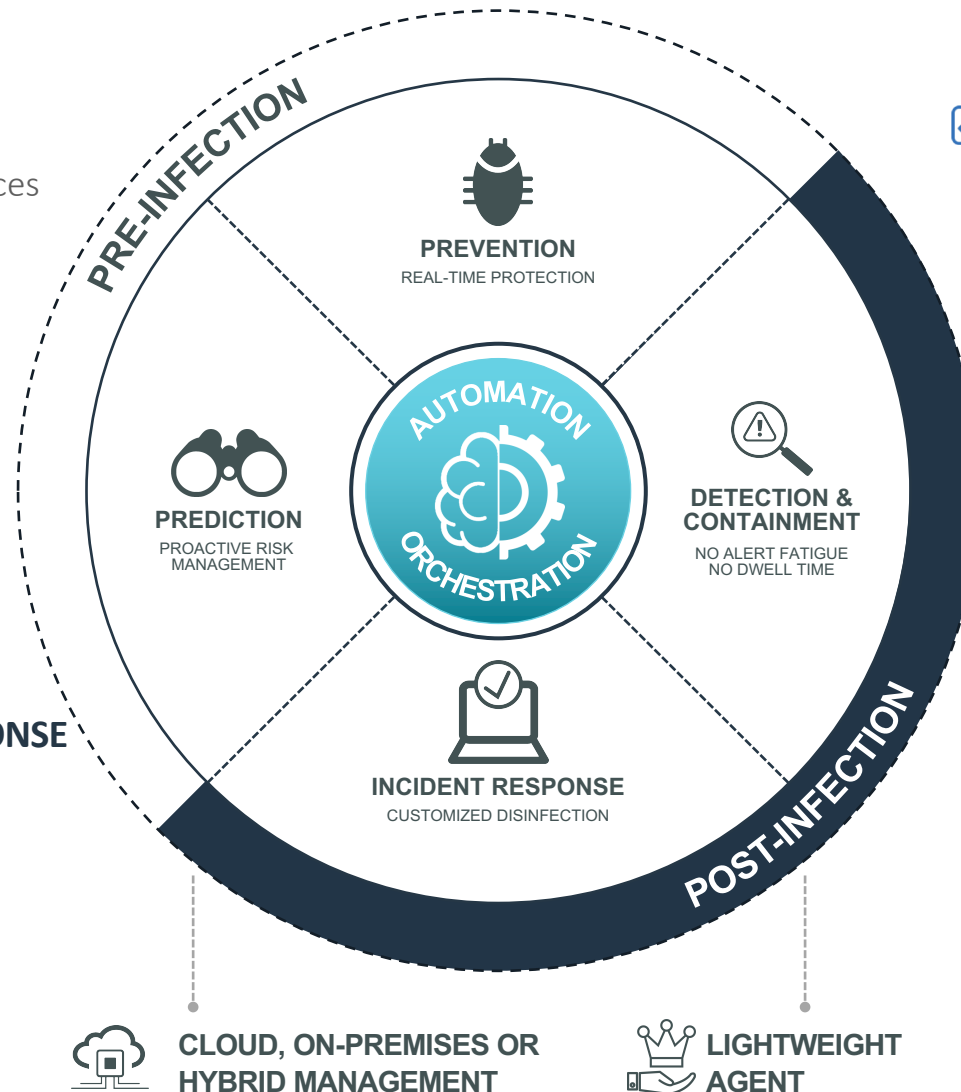
- Automated event classification
- Automated remediation (notify users, isolate device, remediate device, open ticket)
- Automated investigation with minimal interruption for user

✓ REAL-TIME PREVENTION

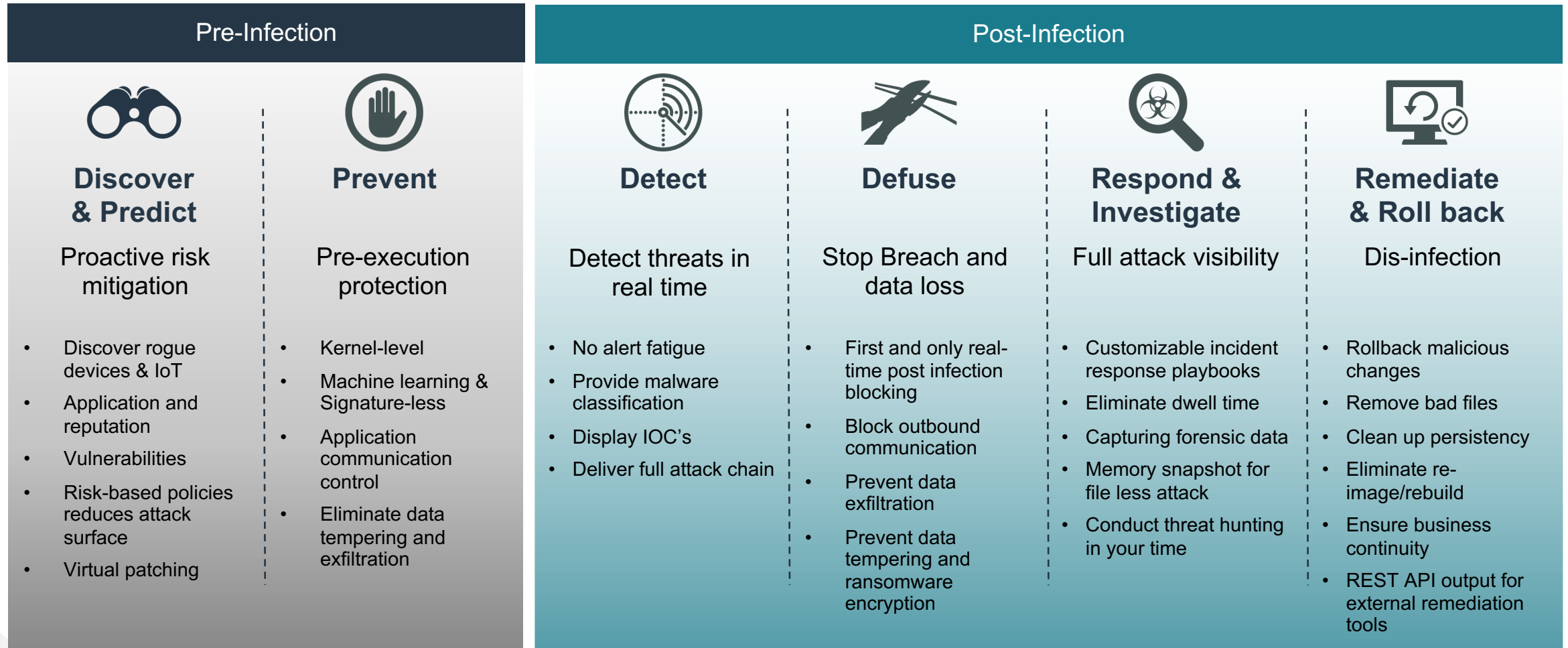
- Machine learning, Kernel-based Next Generation AV
- Feeds from a continuously updated cloud database
- Real-time automated prevention of ransomware encryption

✓ REAL-TIME DETECTION AND CONTAINMENT

- Automated post-infection detection and blocking
- OS-centric technology
- Analysis of entire log history
- Surgical containment



FortiEDR – Real-time Endpoint Protection at Pre- and Post-Infection

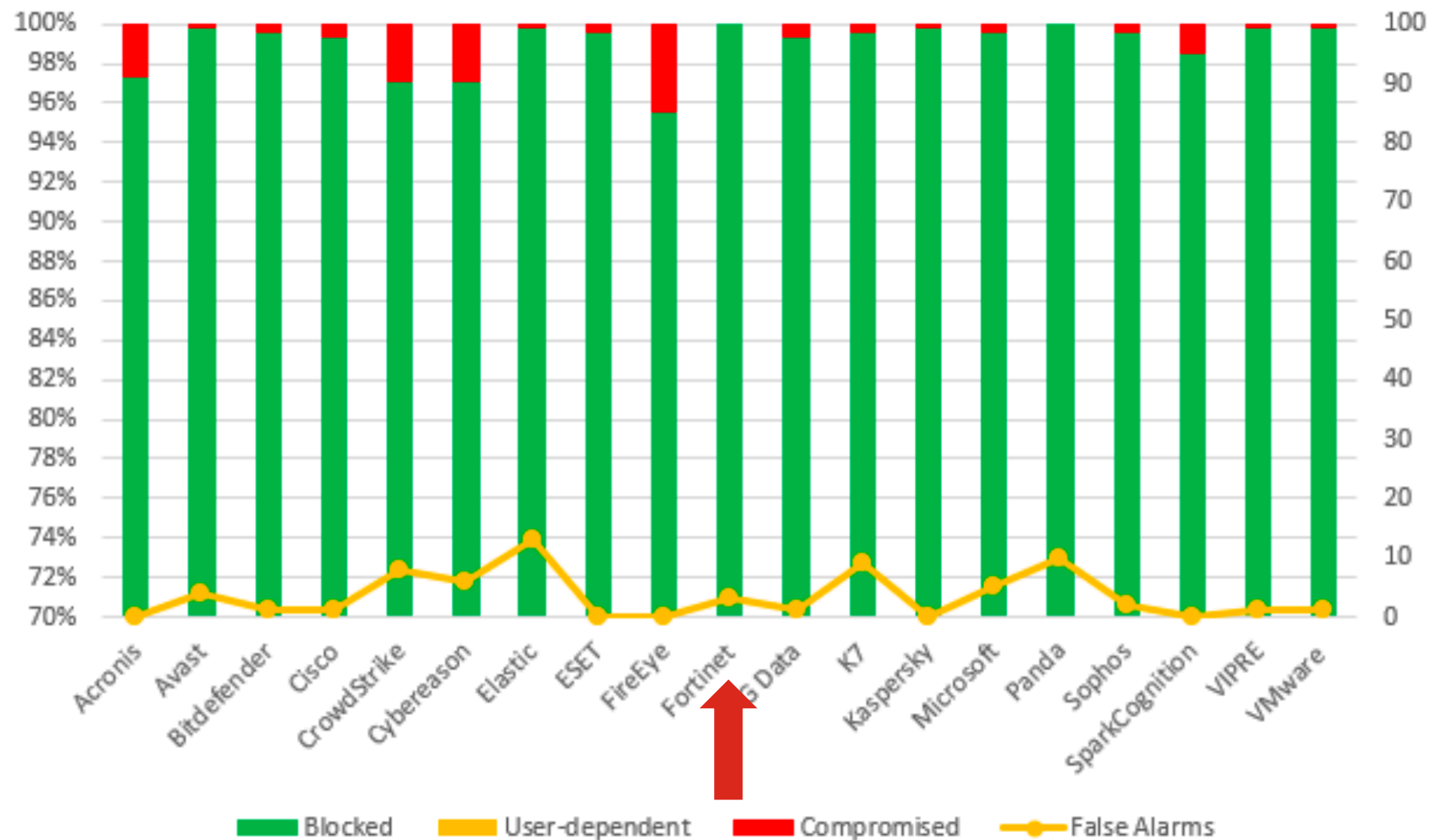


Independent Tests of Anti-Virus Software

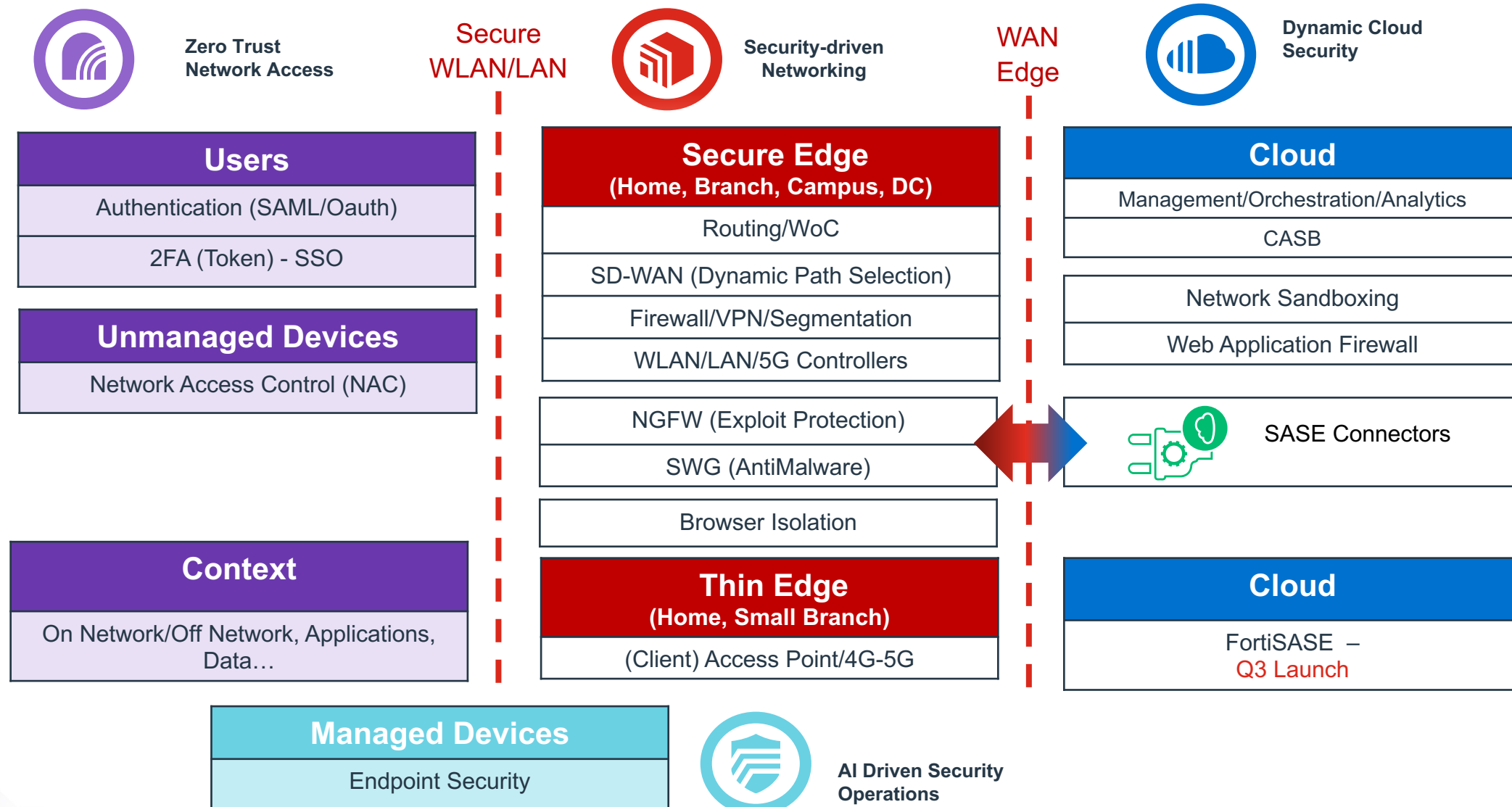


TEST PERIOD: MARCH – APRIL 2020
LANGUAGE: ENGLISH
LAST REVISION: 12TH MAY 2020

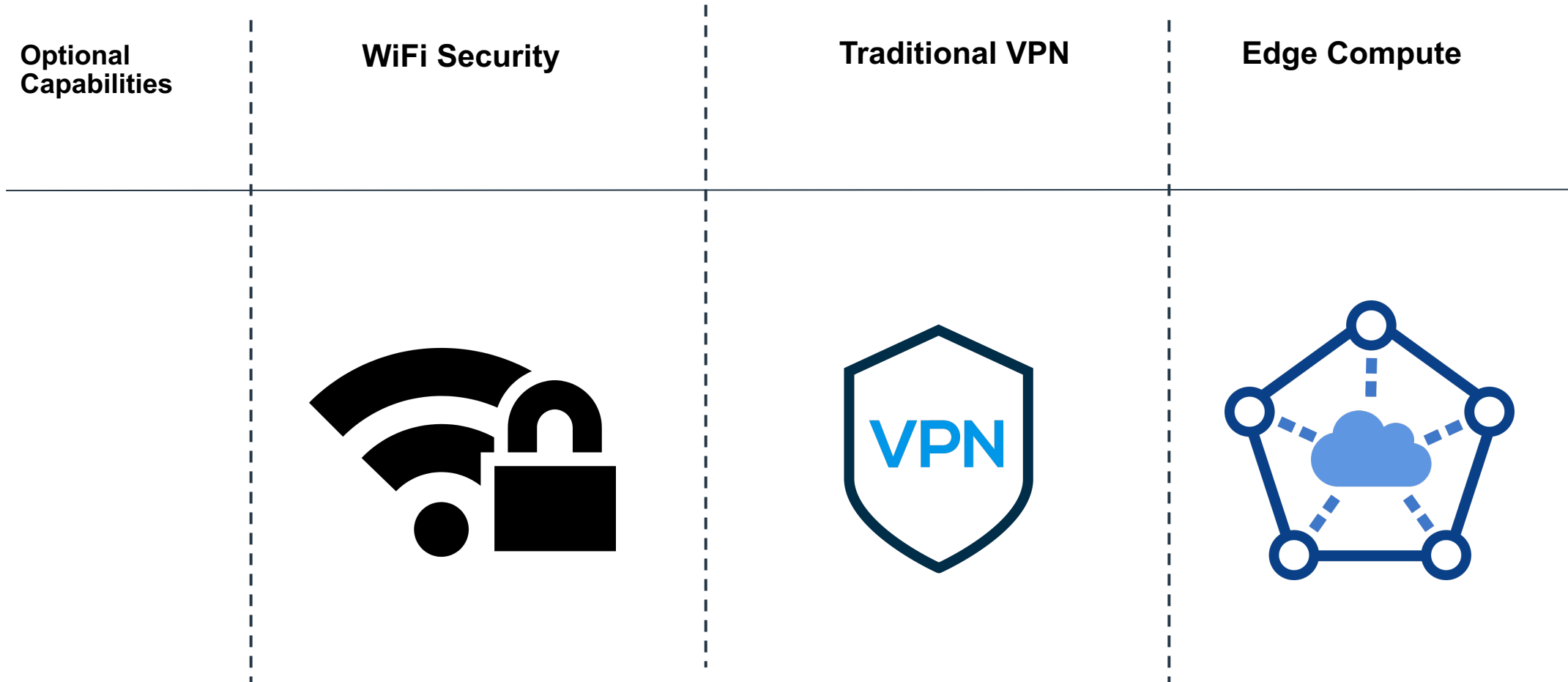
WWW.AV-COMPARATIVES.ORG



SASE Odporúčané Funkcionality

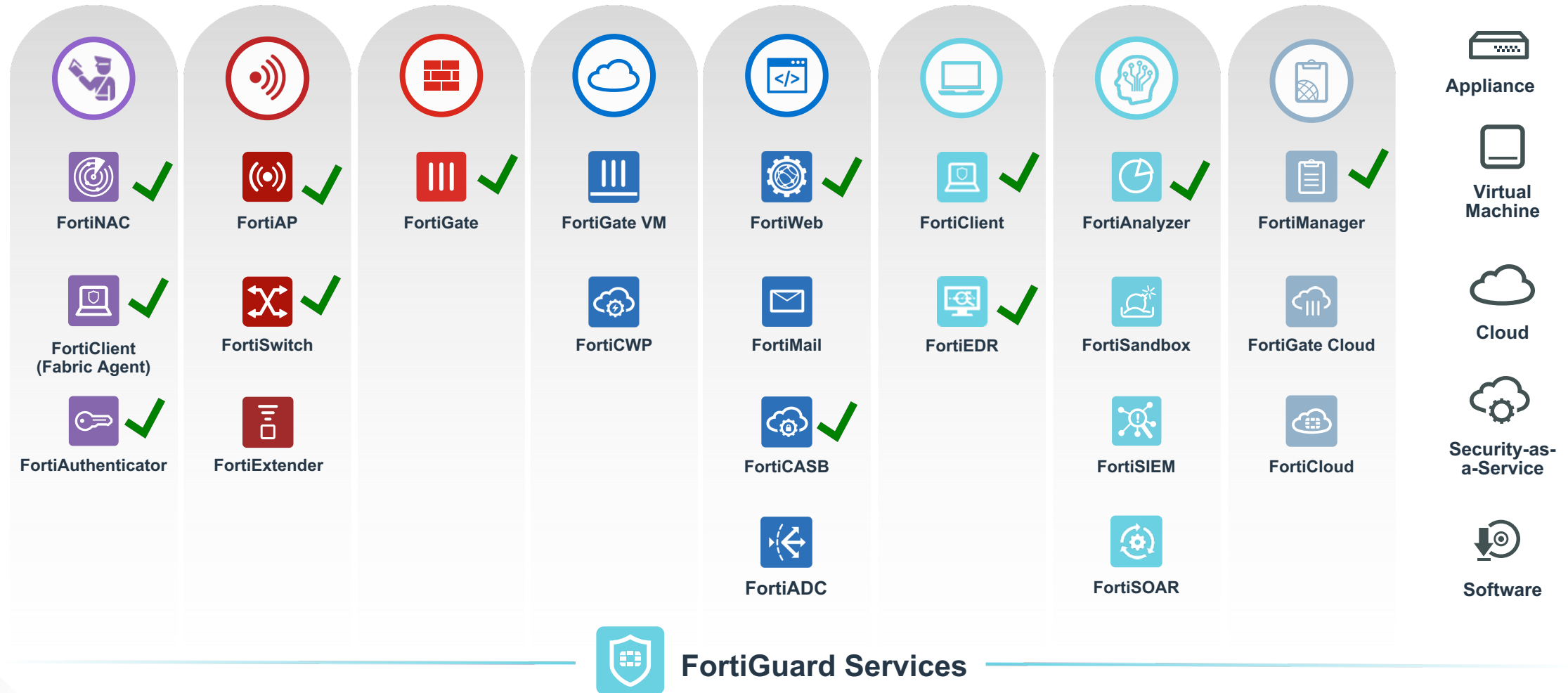


SASE Definition – Voliteľné Funkcionalita



SASE je špecifická implementácia Fabricu

Základné, Odporúčané a Voliteľné Funkcionality



FORTINET®

Ďakujeme za pozornosť!

BMW i Motorsport
Official Partner

