



UTM - Unified Threat Management

Aneb jen HW nestačí

Viktor Pleštil
Major Account Manager

Situation

Way to Simplify Network Operations

The events of the past more than year, have driven the need for organizations to adapt to the COVID-19 pandemic; and has accelerated digital transformation for many organizations even faster and further. The need to support remote workers has driven network operations teams to adopt agile network strategies supported by infrastructure automation.

Digital business requires agile networks, but 70% of enterprise networking activities are performed manually.

These data points help explain why [75% of network outages and performance issues](#) are the result of misconfiguration errors.

The percentage of network activities that will be automated will rise from 30% in early 2020 to 50% by 2023.

Key Federal Government Cybersecurity Trends and Challenges



NATION-STATE THREATS: The federal government is under attack by increasingly sophisticated nation-state cyber actors.



MISSION CONTINUITY: Downtime or latency in mission-critical applications and services can impact the lives of millions of citizens.



RESOURCE ALLOCATION: Flat or declining funding levels mean that agencies face dwindling resources, impeding the ability to update technology and retain skills workers.



INTEGRATION OF SECURITY INFRASTRUCTURE: Security based upon sliced point products degrades visibility, interoperability, and slows threat response.



TRANSITION TO CLOUD: Government agencies are looking to cloud services to increase efficiency and stretch their limited resources.



COMPLIANCE REPORTING: Manually documenting compliance consumes scarce resources and cybersecurity talent.

Key State and Local Government Cybersecurity Trends and Challenges



COST OPTIMIZATION: State and local governments operate with limited budgets, and resource allocation is prioritized based upon impact to constituents.



TARGETED THREATS: State and local governments have been a major target of ransomware, which impacts their ability to provide critical services.



DIGITAL GOVERNMENT TRANSFORMATION: Governments' move to the cloud and deployment of Internet-of-Things (IoT) sensors on critical infrastructure creates new security challenges.



INTEGRATION OF SECURITY ARCHITECTURE: Security based upon sliced point products degrades visibility and slows threat response.



MAINTAINING COMPLIANCE: Regulations regarding personal information, critical information protection, and environmental standards all require time-consuming compliance efforts.



SECURE TELEWORK: Few state and local governments are equipped to support large-scale telework, as required for disaster recovery plans.

Key Higher Education Cybersecurity Trends and Challenges



REACTIVE RISK: Tight budgets, change management processes, and a desire to protect students' free expression create reactive security.



GROWING ATTACKS: Student-owned connected devices and a growing use of cloud computing expand the institutional attack surface.



INSIDER THREATS: Attackers take advantage of higher education's support of free expression to launch attacks that threaten it.



RATIONALIZING IT OPERATIONS: Addressing individual threats results in an array of point security products that is complex to operate and maintain.



COMPLIANCE: Institutions must ensure and demonstrate that student data is protected in accordance with a number of regulations.

Key Healthcare Cybersecurity Trends and Challenges



NETWORK LATENCY: Encryption of Electronic Protected Health Information (ePHI) is necessary for regulatory compliance but impacts availability of data for patient care.



DATA INTEGRITY: Incorrect or incomplete medical data can impact patient health and cause clinical risk.



OPERATIONAL EFFICIENCY: Digital innovations secured by point products impact operational efficiency.



PHYSICAL DISTRIBUTION OF SITES AND PARTNERS: Sprawling healthcare organizations must monitor and secure ePHI flowing across their networks.



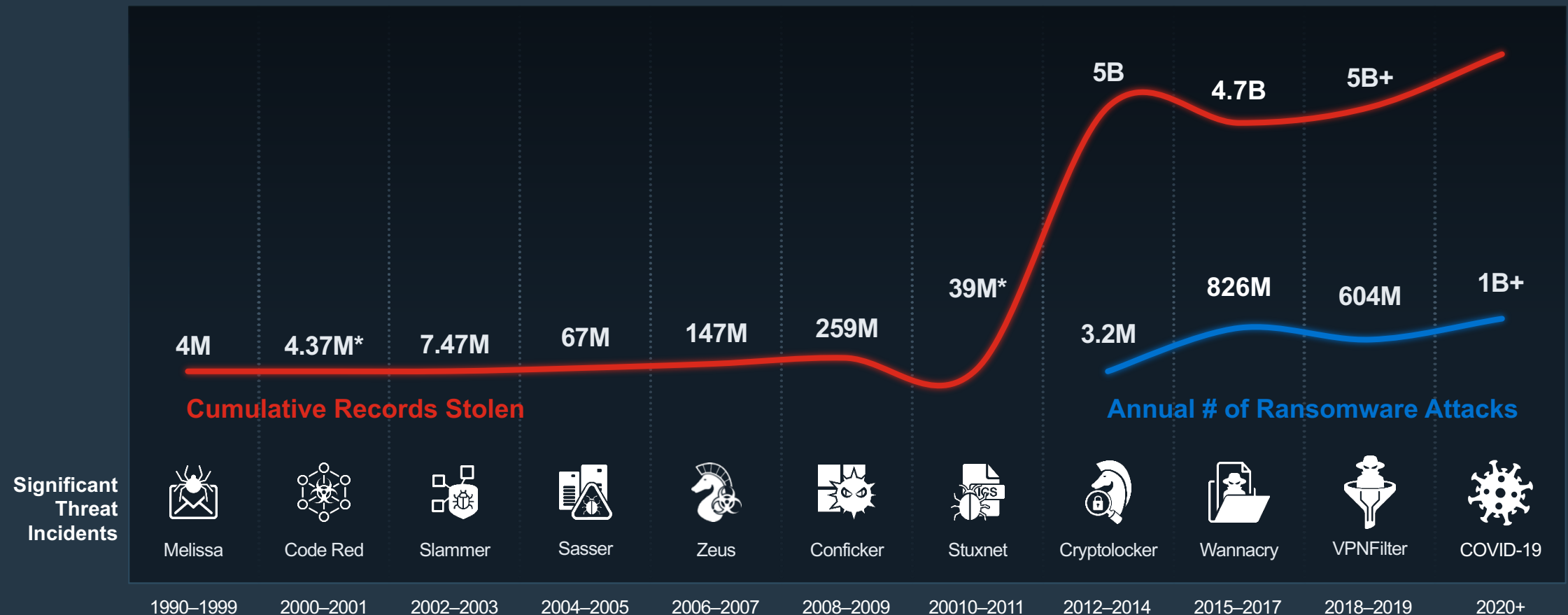
COST: As insurance and government reimbursement program payments decline, healthcare organizations must operate with tighter budgets.



COMPLIANCE REPORTING: Healthcare organizations must protect a variety of sensitive data in accordance with a patchwork of privacy laws and regulations.

Advanced Threats Continue to Adapt

Even advanced threats still rely heavily on social engineering



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

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

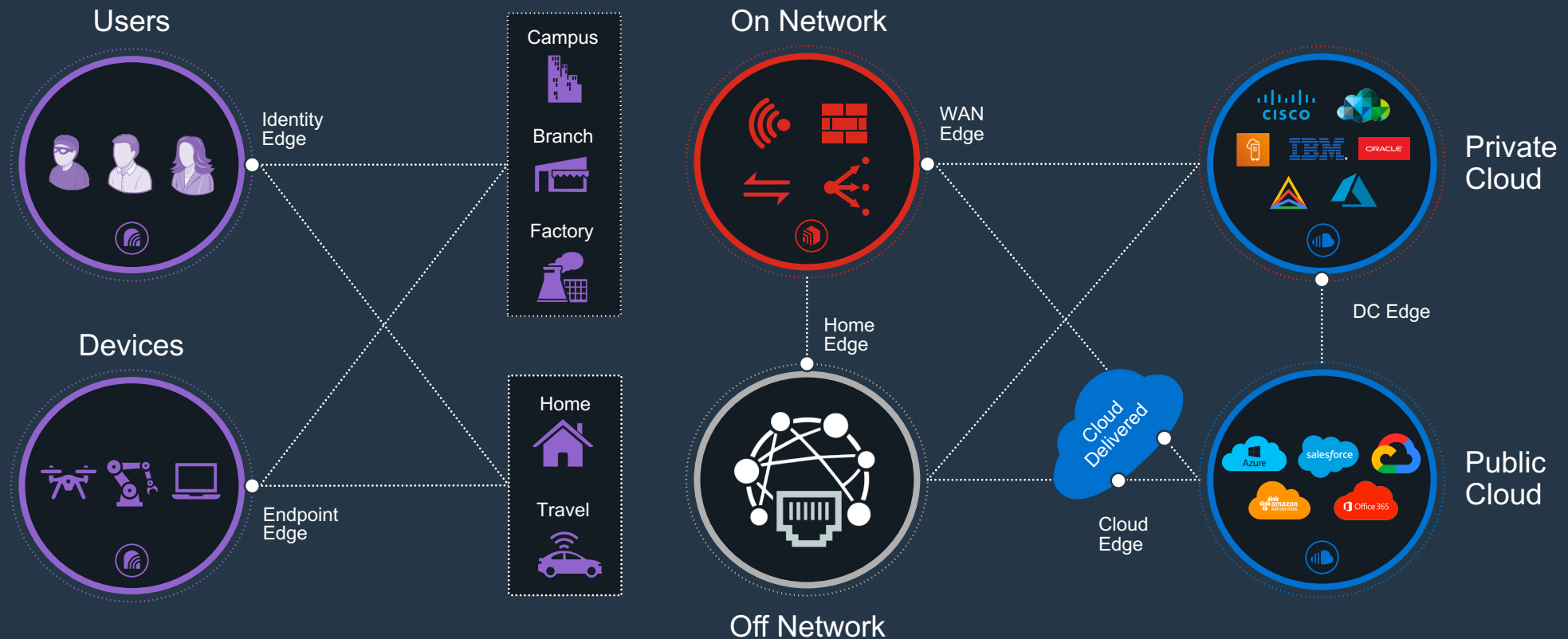
Too many vendors and too many alerts, **not** enough skilled people



Compliance

Global, country, province, industry, and government regulation

Numerous Edges Must Be Secured and Protected



Fortinet Technology Vision

Fortinet Security Fabric

Converged

Networking + Security
delivered by:



Appliance
(ASIC)



Virtual Machine



Cloud Delivery

Security Anywhere
Costs Reduced

Platform

That protects:



Users and Devices



Networks



Applications
and Cloud

Operational Efficiency
Automated Response

AI-driven

Automation for:



Security
Operations (SoC)



Network
Operations (NoC)

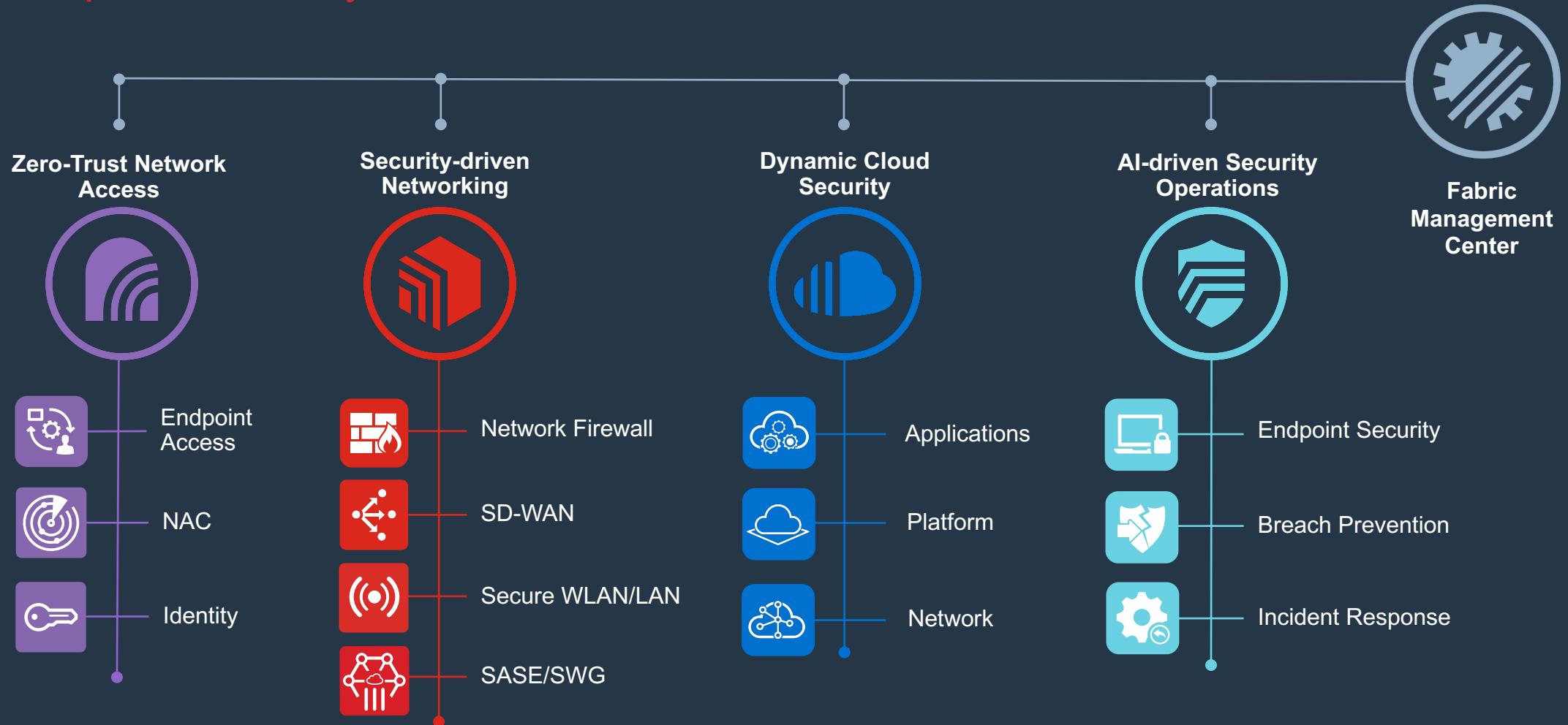


Open
Ecosystem

Predictive Security
Optimized User Experience

Fortinet Cybersecurity Platform

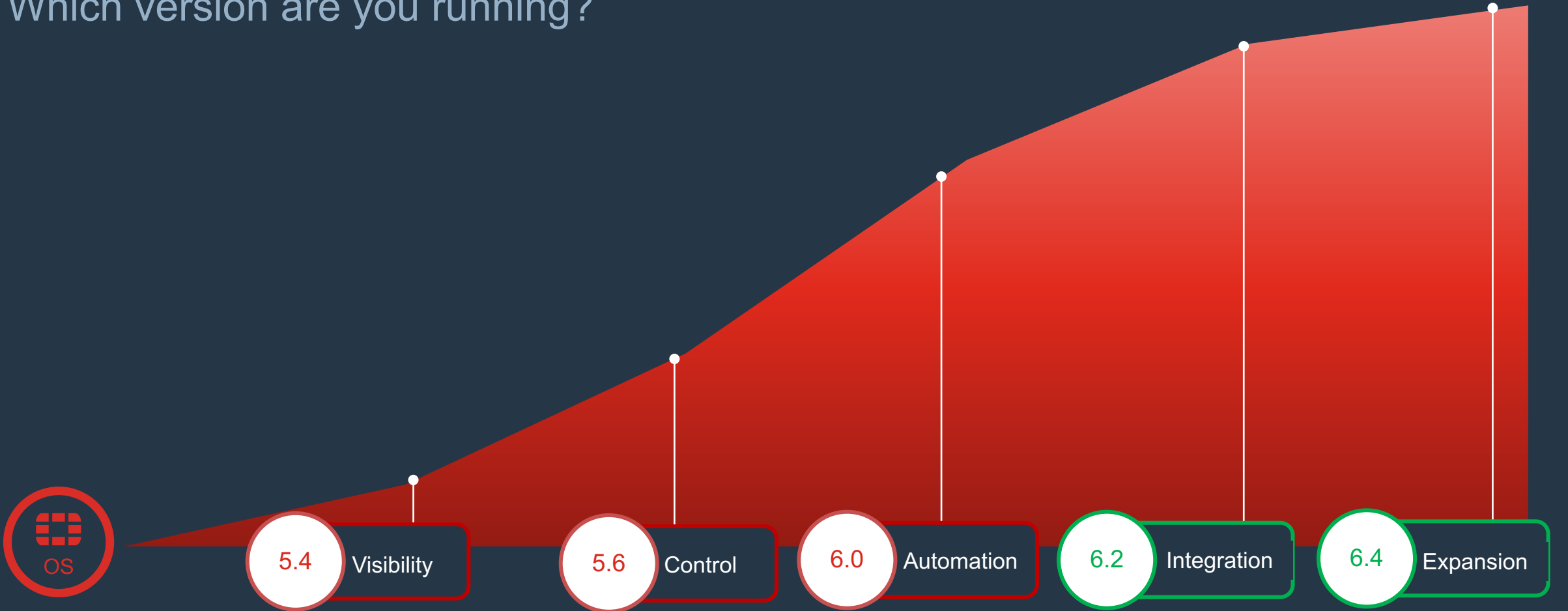
Enterprise Security Fabric



Evolution of the Security Fabric



Which version are you running?



"I'm blind!"	"I need single pane"	"Insufficient resources"	"I already defined that in another system"	"Digital innovation comes with too much complexity!"
Proactive APT	Streamline controls	Automation	Business Context	Workflows & Simplification



FortiGuard Labs and how it works

Visibility + Innovation = Actionable Threat Intelligence

FortiGuard Labs Overview



Telemetry
 Network
 Web
 Sandbox
 Email
 Endpoint

CERTs

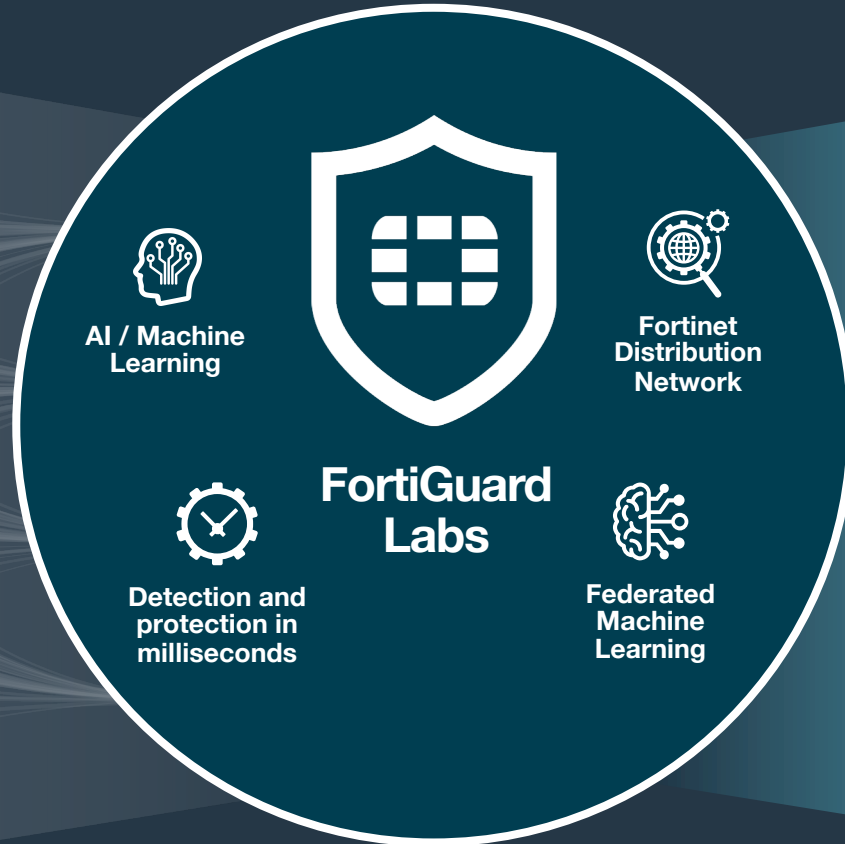
Enforcement Partnerships

Zero-Day

OSINT

CTA feeds

Trusted Partnerships



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 CONSULTING SERVICES

- Penetration Testing
- Phishing Service
- Incident Response

Innovation

AI and ML Driven Detection and Protection



Delivering **1B Updates**
Every Day

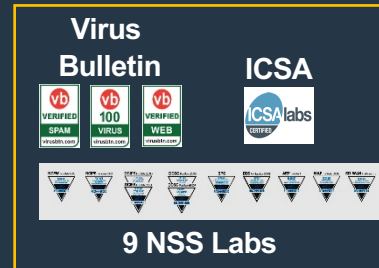
FortiGuard Labs

Proven, Effective, Innovative

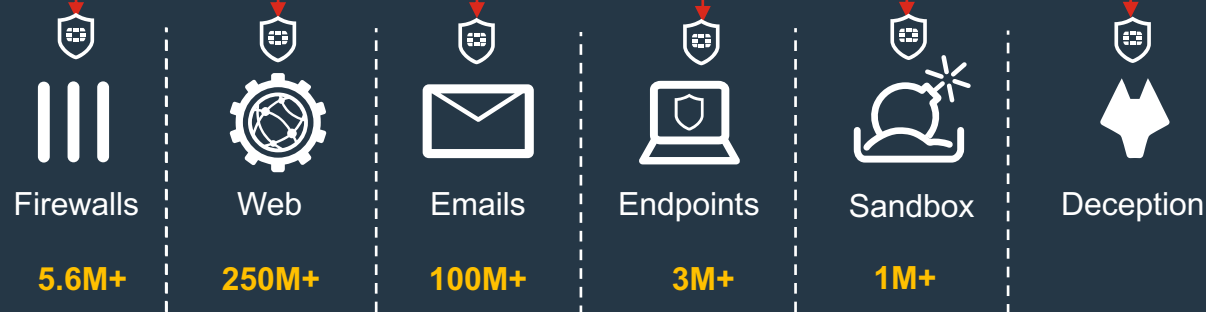
Analytics and Artificial Intelligence

Best-in-Class Technologies


Sustained 3rd party certification YoY




Multi-billion Node AI Systems
5.5 Years to Train
Connected AI Fabric




Actionable Threat Intelligence – Q2 2020



17 Million
Botnet C&C attempts
THWARTED
PER MINUTE



565,000
SPAM
Blocked Per Day



195,000
Malicious Website
ACCESSES
Blocked Per Minute




885
ZERO DAY
THREATS DISCOVERED



18 Million
NETWORK INTRUSION
ATTEMPTS
resisted per minute




18 Million
PHISHING
Blocked Per Day



1.1
PB Of Threat
Samples



609,000
HOURS
of Threat Research
GLOBALLY PER WEEK



173,000
MALWARE PROGRAMS
Neutralized Per Minute

FortiCare Advanced Support

Flexible Right-sized
Options



24x7 Support

Around the clock support. Firmware updates. FortiGuard dynamic policies subscriptions



Advanced Support Engagement

Support Engineer designated to document customer support plan. Faster resolution with higher ticket servicing & SLA. Flexible Points for complementary services



Premium RMA

Next-day RMA and delivery. 4-hour RMA and delivery with option for physical swaps via engineer on-site. Secure RMA for self-disposing old parts (no returns to Fortinet needed)



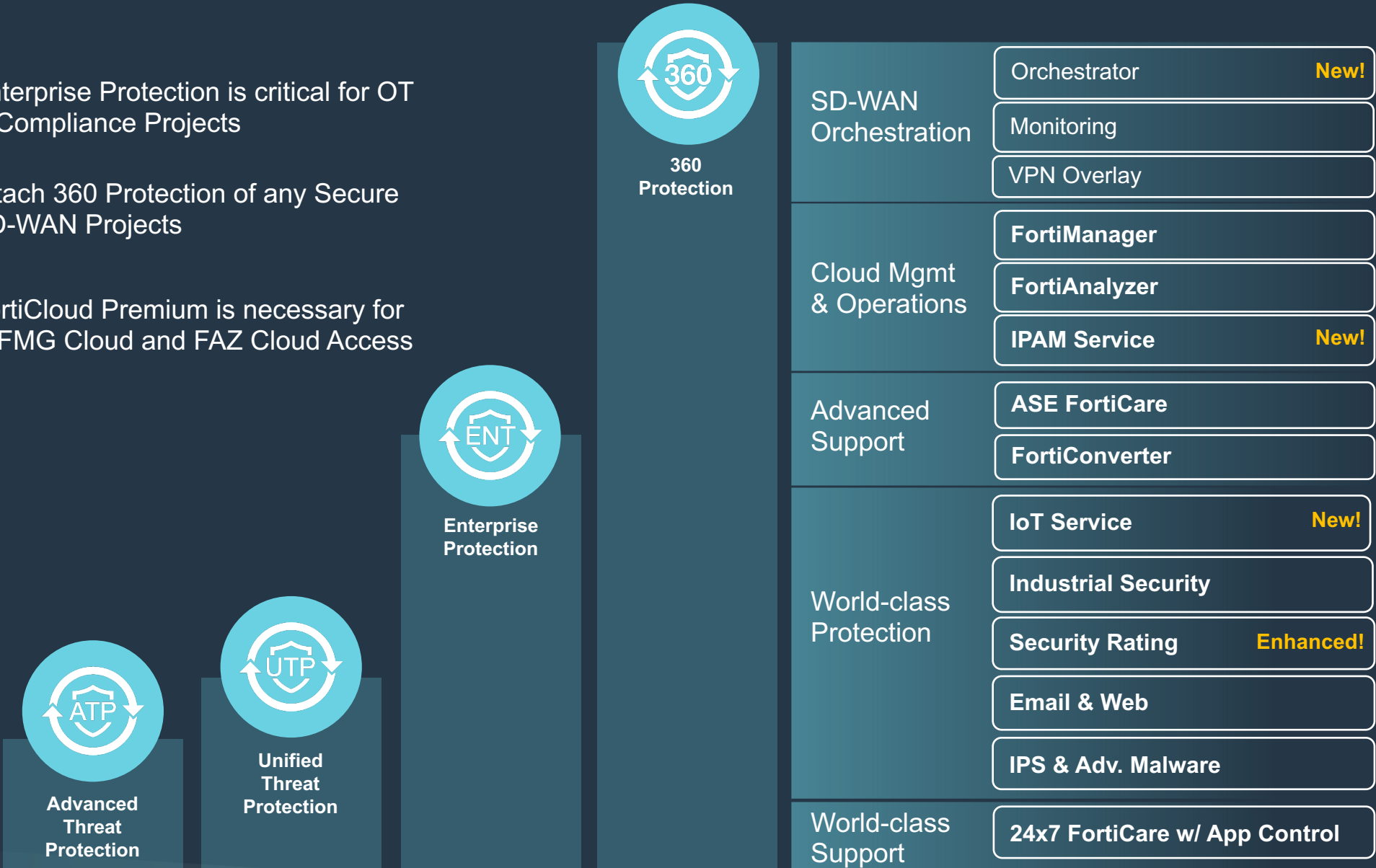
Professional Services & Resident Engineer

Deployment, migration, and integration. Standard and Custom Statement of Work (SOW). Resident Engineers to augment staffing needs onsite or remote

Support, Subscriptions and Bundles

Summary: FortiGuard Subscriptions & Bundles

- 1 Enterprise Protection is critical for OT & Compliance Projects
- 2 Attach 360 Protection of any Secure SD-WAN Projects
- 3 FortiCloud Premium is necessary for all FMG Cloud and FAZ Cloud Access



Advanced Malware Protection (AMP)

Most Advanced Core Security Protection Package



CAPABILITIES

- Cloud sandboxing for unknown threats
- Detection between AV signature updates
- Strip all active content from files in real-time
- Automated content updates & latest malware and heuristic detection

BUSINESS BENEFIT



Core Cutting-edge protection capabilities that defend against known and emerging threats managing risk

Advanced Threat Protection (ATP)

Threat Protection against known and unknown threats

AMP



IPS



Application
Control

CAPABILITIES

- Provides granular control to block access to unauthorized and risky application
- Visibility and control over application usage
- Protect against known and zero-day vulnerabilities
- Virtual patch through IPS signatures

BUSINESS BENEFIT



Protect business-critical applications and assets

Unified Threat Protection (UTP)

Pure Next-Generation Firewall Security Package



Web Filtering



AntiSpam

CAPABILITIES

- Protection against threats delivered through email
- Block access to malicious and unauthorized websites
- Granular controls and multiple categories to define policy constructs

BUSINESS BENEFIT



Protect against the latest attacks from all vectors to minimize business disruption

Enterprise Protection (ENT)

Deliver Compliance & OT Protection



Security
Rating



Industrial
Security



FortiConverter
Service



IoT Detection

CAPABILITIES

- Provide visibility into security posture based on CIS and NIST Control benchmarks
- Identify most of the common ICS/SCADA protocols for granular visibility and control
- Ability to automatically discover and segment IoT devices based on FortiGuard intelligence, and enforce appropriate policies
- One-Time Configuration Migration Service

BUSINESS BENEFIT



Protect the entire attack surface and delivers compliance and risk management

360 Protection

Simplify SD-WAN Operations



FMG Cloud



SD-WAN Orchestrator



SD-WAN Cloud Monitoring



IPAM



FAZ Cloud

What's Included:

1. **Cloud-Based Network Management** for SD-WAN and other projects
2. **Analytics, Orchestration & Automation** for SD WAN Network Management
3. **24x7x365 ASE FortiCare** Advanced Support Ticket handling and RMA Service

Helps:

- **Self-Service Customers** to reduce risk, improve TCO and increase efficiency
- **Mid-Market MSSPs** to offer the most comprehensive security & operational services to their customers
- Bundle **Priced 100%** per FortiGate subscription

FORTINET®