



Prípadová štúdia: Opatrenia na elimináciu alebo mitigáciu rizík informačnej bezpečnosti podľa ISO 27001/27005 (ref. štandard ISO 27001, ISO 27002, ISO 27005)

8. 9. 20
Zsolt Géczi, CEH
Regional Accounts Manager, Slovakia

BMW i Motorsport
Official Partner





\$22.2B Market Cap
Nasdaq: FTNT

S&P 500

\$2.6B
FY2019 Billings

Fastest Growing, Solid Profitability

680+
Patents

Top Innovator

**#1 Cybersecurity
Company in the World**
**Leading Every Evolution
of Cybersecurity**

- ✓ *Most Deployed*
- ✓ *Most Validated*
- ✓ *Most Patented*
- ✓ *Broadest Portfolio*

30%
Global Firewall Shipments

Huge Scale

465,000+
Customers Worldwide

Massive Sensor Network

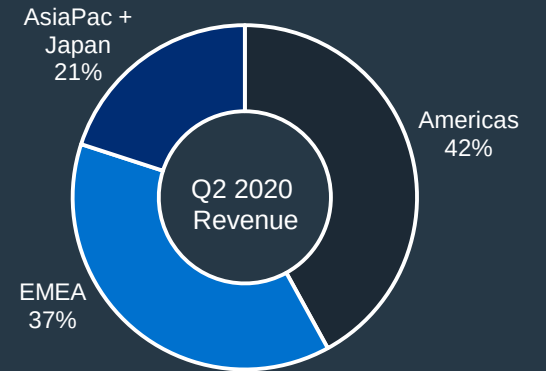
30+
Cybersecurity Product Lines

Broadest Attack Surface Coverage

Source: Company data, Figures as of March 31, 2020

Broad Global Footprint—Balanced Global Growth

Huge R&D investment and global presence



- Headquarters
 - Dev Centers
 - Support Centers
 - Centers of Excellence
-  **FortiCare**

US
based

7,700+
employees

24x7
support

59,000+
partners

At the Forefront of Innovation

2019 was 10th time in a row that Fortinet is in the Gartner Magic Quadrant for Network Firewalls

Gartner Magic Quadrant for Network Firewall, Rajpreet Kaur, Adam Hills, Jeremy D'Hoinne, John Watts, 17, September 2019.

This report was previously titled the Magic Quadrant for Enterprise Networks Firewalls.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties.

Additional reports:

Magic Quadrant for Security Information and Event Management (February 2020), Magic Quadrant for Web Application Firewalls (September 2019), Magic Quadrant for Wired and Wireless LAN Access Infrastructure (September 2019), Magic Quadrant for Endpoint Protection Platforms (August 2019), Magic Quadrant for WAN Edge Infrastructure (November 2019)

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (September 2019)

Consistent, Proven Performance

More Third-Party Validation Than Any Other Network Security Vendor



- Recommended in 9 out of 9 tests, nearly 2X the nearest competitor
- All 8 security tests, plus SD-WAN



- Passed last 19 consecutive Advanced Threat Detection (ATD) test cycles



VBSpam, and VBWeb certifications

- 15 VBWeb certifications consecutively
- Highest "VBSpam+" rating



- 100% Effectiveness in latest Real World Protection Test

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

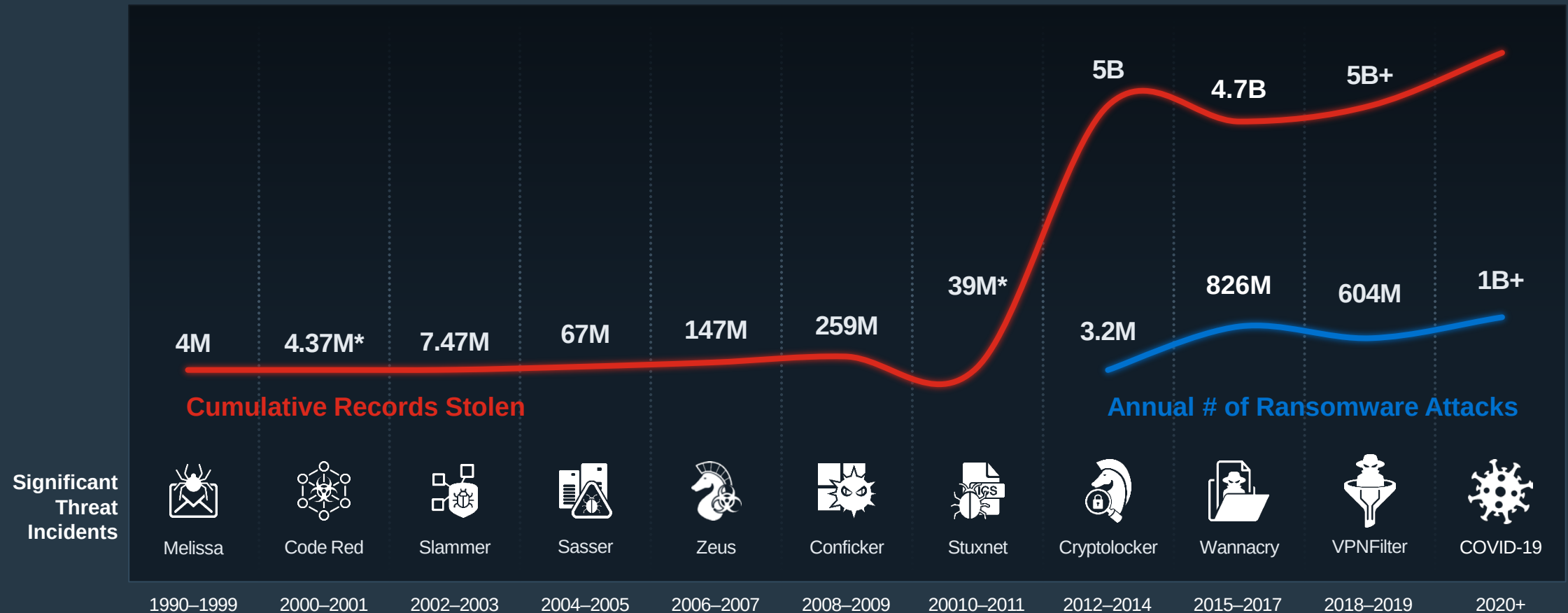


Compliance

Global, country, province, industry, and government regulation

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

ISO 27 00x

ISO/IEC 27000: 2018

*Information technology -- Security techniques -- Information security management systems -- **Overview and vocabulary***

ISO/IEC 27000: 2018 poskytuje prehľad systémov manažérstva informačnej bezpečnosti (SMIB) a základne pojmy a definície bežne používané v štandardoch radu 27000. Je aplikovateľný na všetky typy a veľkosti organizácií (vládne, komerčné, neziskové).

ISO 27 00x

ISO/IEC 27001:2013

Information technology -- Security techniques -- Information security management systems – Requirements

ISO/IEC 27001:2013 špecifikuje požiadavky na vytvorenie, implementáciu, udržiavanie a zlepšovanie SMIB v kontexte organizácie. Tiež obsahuje požiadavky na posudzovanie a narábanie s rizikami informačnej bezpečnosti. Požiadavky tejto normy sú generické a aplikovateľné na všetky organizácie nezávisle na ich type, veľkosti a charaktere.

ISO 27 00x

ISO/IEC 27002:2013

*Information technology -- Security techniques --
Code of practice for information security controls*

ISO/IEC 27002:2013 poskytuje pokyny pre štandardy informačnej bezpečnosti organizácie a praktiky riadenia informačnej bezpečnosti vrátane výberu, implementácie a riadenia opatrení berúc do úvahy rizikové prostredia informačnej bezpečnosti organizácie. Je navrhnutý pre organizácie, ktoré zamýšľajú:

- výber opatrení v rámci procesu implementácie SMIB založeného na ISO/IEC 27001,
- implementáciu všeobecne akceptovaných opatrení informačnej bezpečnosti,
- vývoj vlastných smerníc pre informačnú bezpečnosť.

ISO 27 00x

ISO/IEC 27003:2017

Information technology -- Security techniques -- Information security management system implementation -- Guidance

ISO/IEC 27003:2017 sa zameriava na kritické aspekty úspešného návrhu a implementácie SMIB v súlade s ISO/IEC 27001:2013. Popisuje proces špecifikácie a návrhu SMIB od počiatku až po vytvorenie plánu implementácie.

ISO 27 00x

ISO/IEC 27004:2016

Information technology -- Security techniques -- Information security management
– *Monitoring, measurement, analysis and evaluation*

ISO/IEC 27004:2016 poskytuje návod pre vývoj a používanie metrík a merania pre posúdenie efektivity implementovaného SMIB a opatrení špecifikovaných v ISO/IEC 27001.

ISO 27 00x

ISO/IEC 27005:2018

Information technology -- Security techniques -- Information security risk management - Guidelines

ISO/IEC 27005:2018 poskytuje návod pre riadenie rizík informačnej bezpečnosti.

Podporuje všeobecné koncepty špecifikované v ISO/IEC 27001 a je navrhnutý tak, aby podporoval implementáciu informačnej bezpečnosti založenej na riadení rizík.

ISO 27 005

... biznis

... dáta a informácie

... **Riziko** > Posúdenie rizika > **Hodnotu rizika** určuje hodnota informačných aktív

identifikácia rizika

analýza rizika

hodnotenie rizika

...hrozby a zraniteľné miesta, ktoré existujú (alebo môžu existovať)

...a určiť si možné následky, konzekvenice

Príklady, kedy to nevyšlo, ...resp. práveže vyšlo ;)

Akvárium

Tesla

Online obchod cestovka

Cenné Informácie – Dáta

Nedozviem sa lebo Botnet

Elektrika

Ransom\$

Verejný zdravotný portal

Espionage

Voľby

Východ vs. Západ

Kali a portály

Nemocnica -19

Metódy hodnotenia technických zraniteľností

Ako hodnotíte efektívnosť Vášho existujúceho bezpečnostného riešenia?

Máte potrebnú vizibilitu robiť tie správne rozhodnutia?

Máte pocit, že máte plnú kontrolu nad Vašou sieťou?

Môže vaše súčasné riešenie držať krok s rýchlosťou vášho biznisu z pohľadu plánovania kapacity?

Máte problémy s pridelením rozpočtu na bezpečnosť?

Metódy hodnotenia technických zraniteľností

Fortinet CTAP - Cyber Threat Assessment Program je program na posúdenie kyberhrozieb, ktorý pokrýva 3 hlavné oblasti:

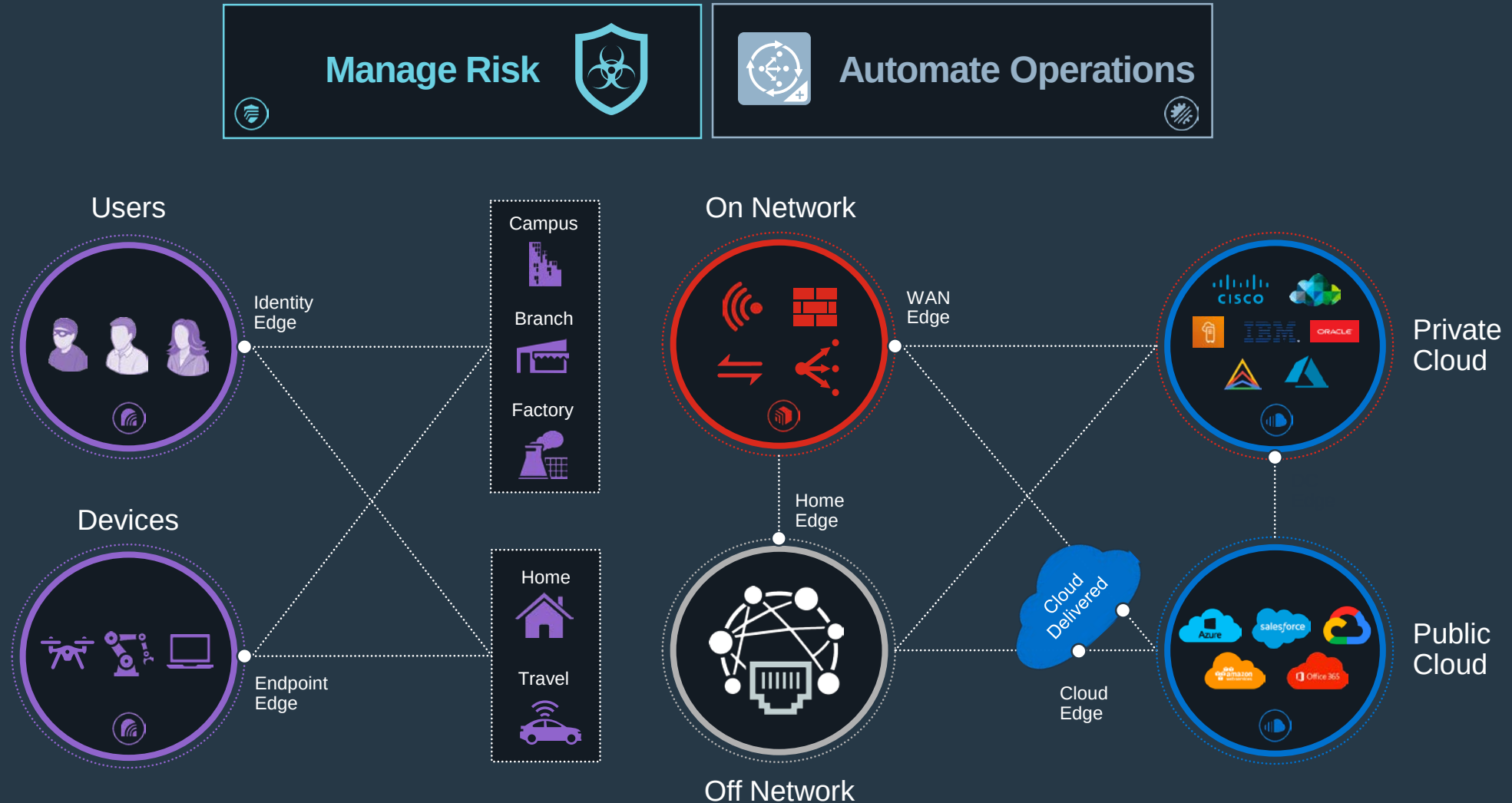
Bezpečnosť/Security - získate prehľad o zraniteľnostiach aplikácií útočiacich na Vašu sieť, o tom, ktorý malware alebo aktívne botnety boli zistené, a dokonca o rizikových zariadeniach, ktoré sú infikované.

Produktivita – odhalíte, ako sa vo Vašej sieti využívajú cloudové IaaS / SaaS, peer to peer, hranie hier, video streaming, sociálne médiá a ďalšie podkategórie aplikácií.

Využitie/Utilizácia - zistíte viac o Vašich požiadavkách na priepustnosť a šírku pásma počas špičkových hodín, najnavštevovanejšie stránky, pomer SSL encryptovanej trafiky...

...alebo FortiDeceptor...

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)



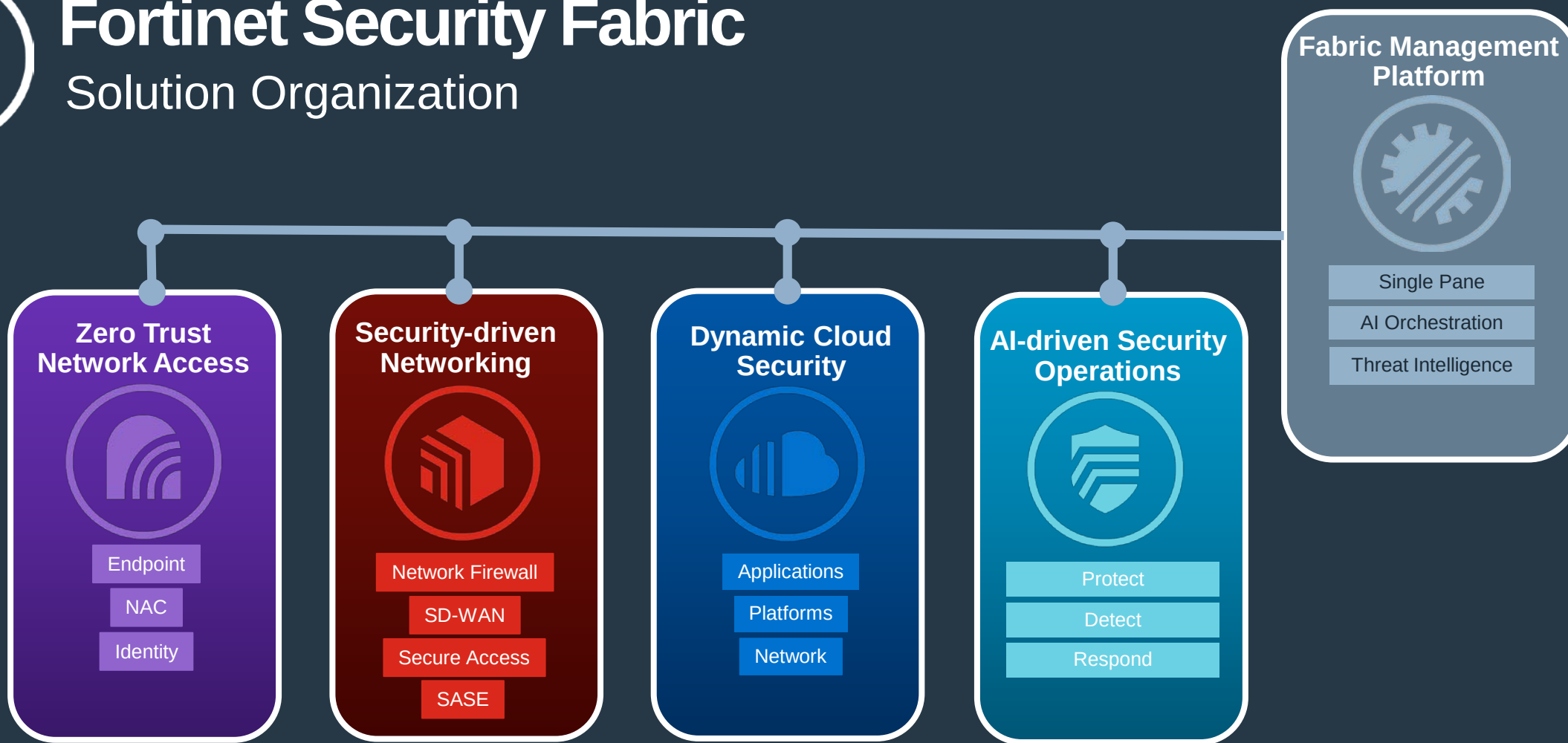
Open
Ecosystem

Predictive Security
Optimized User Experience



Fortinet Security Fabric

Solution Organization



Appliance
SPU



Virtual
Machine



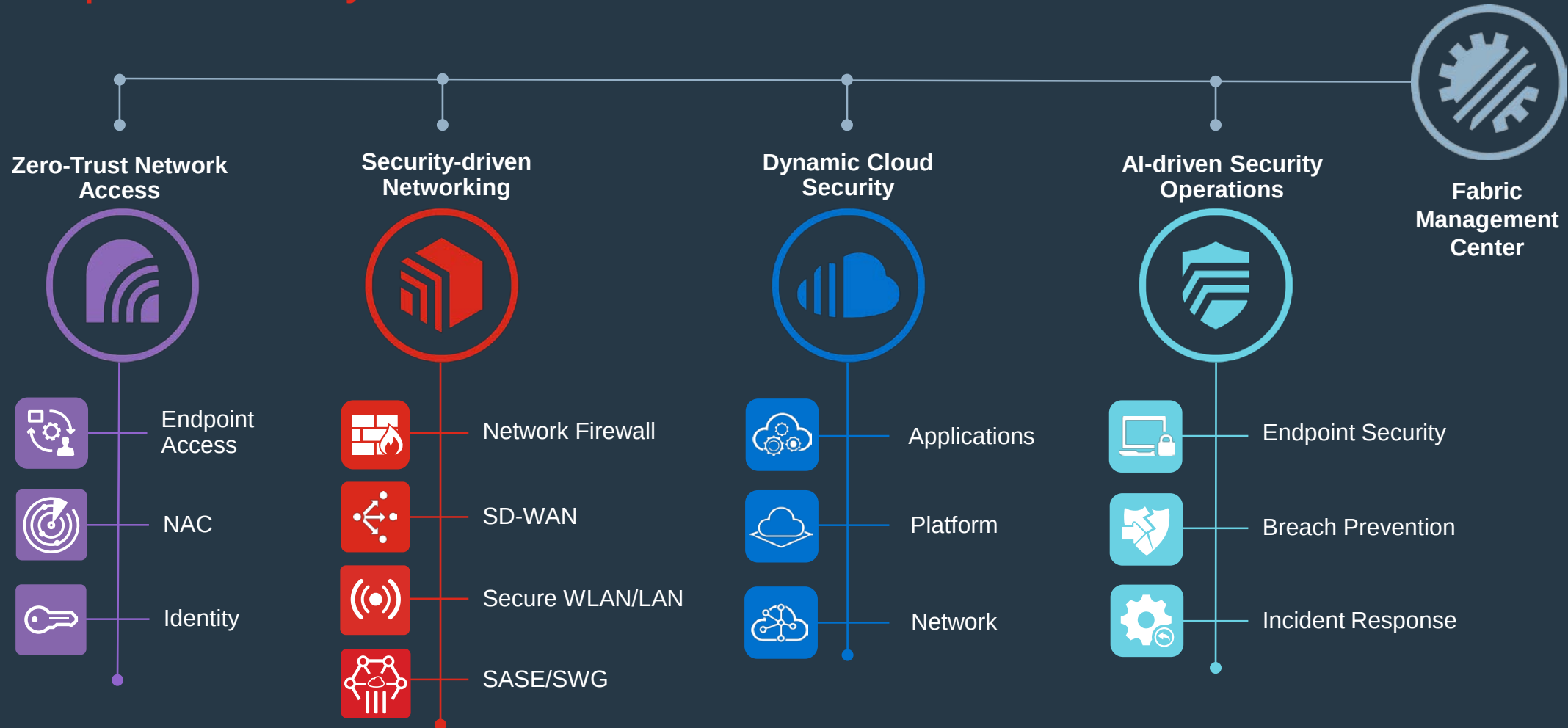
Cloud
Delivery



Flexible
Licensing

Fortinet Cybersecurity Platform

Enterprise Security Fabric

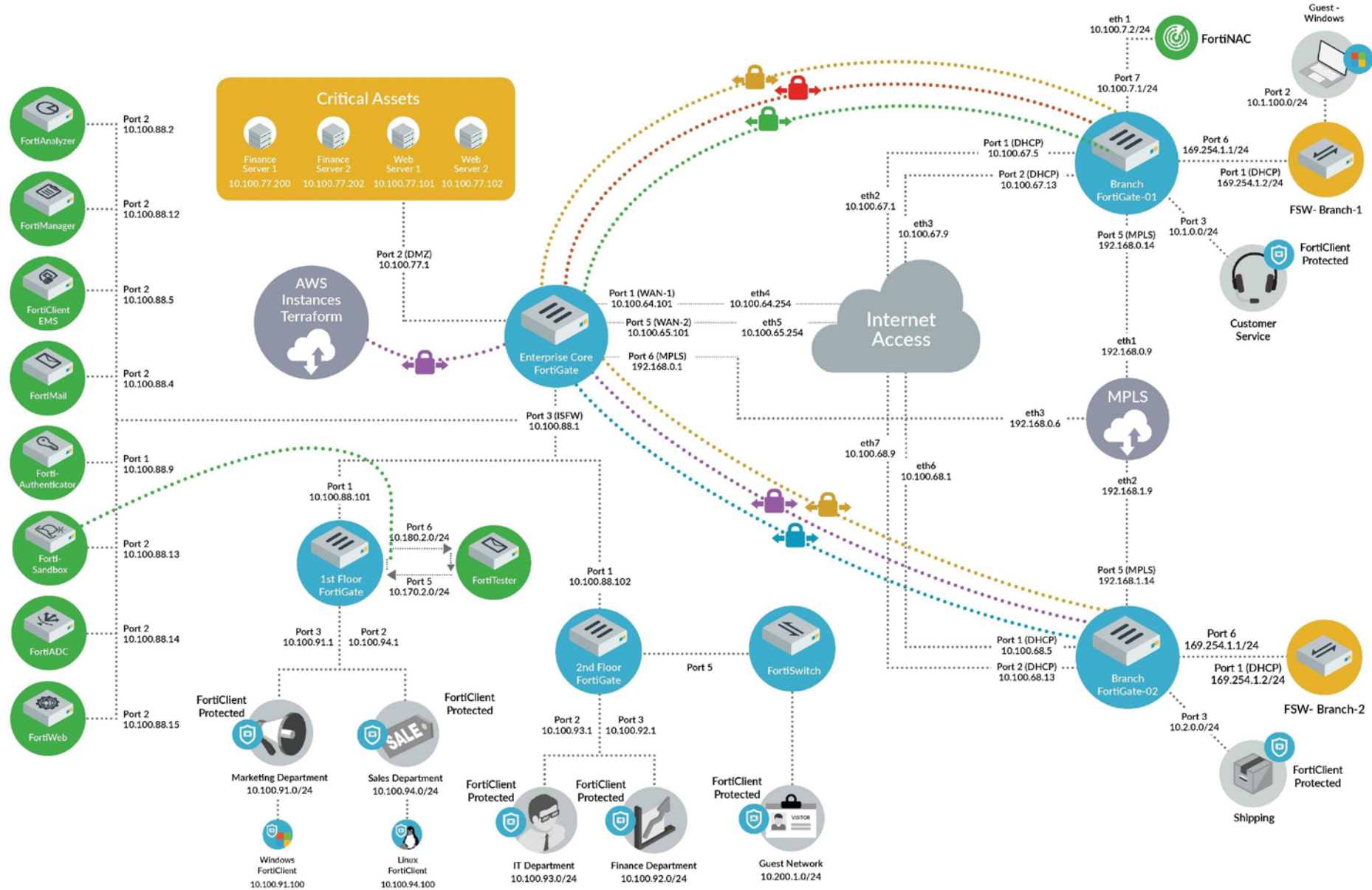


Broadest End-to-End Cybersecurity Platform

Different consumption models available



FortiGuard Services



FORTINET®

BMW i Motorsport
Official Partner

