Fortinet Security Fabric – komplexní řešení bezpečnostních hrozeb nejenom ve zdravotnictví

Viktor Pleštil
Major Account Manager

$18B+ Market Cap
Nasdaq: FTNT

S&P 500

$2.6B
FY2019 Billings

Fast Growing, Solid Profitability

660+
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

440,000+
Customers Worldwide

Massive Sensor Network

30+
Cybersecurity Product Lines

Broadest Attack Surface Coverage

Source: Company data, Figures as of December 31, 2019

NSS Labs 3rd-Party Certifications

Most recent test results

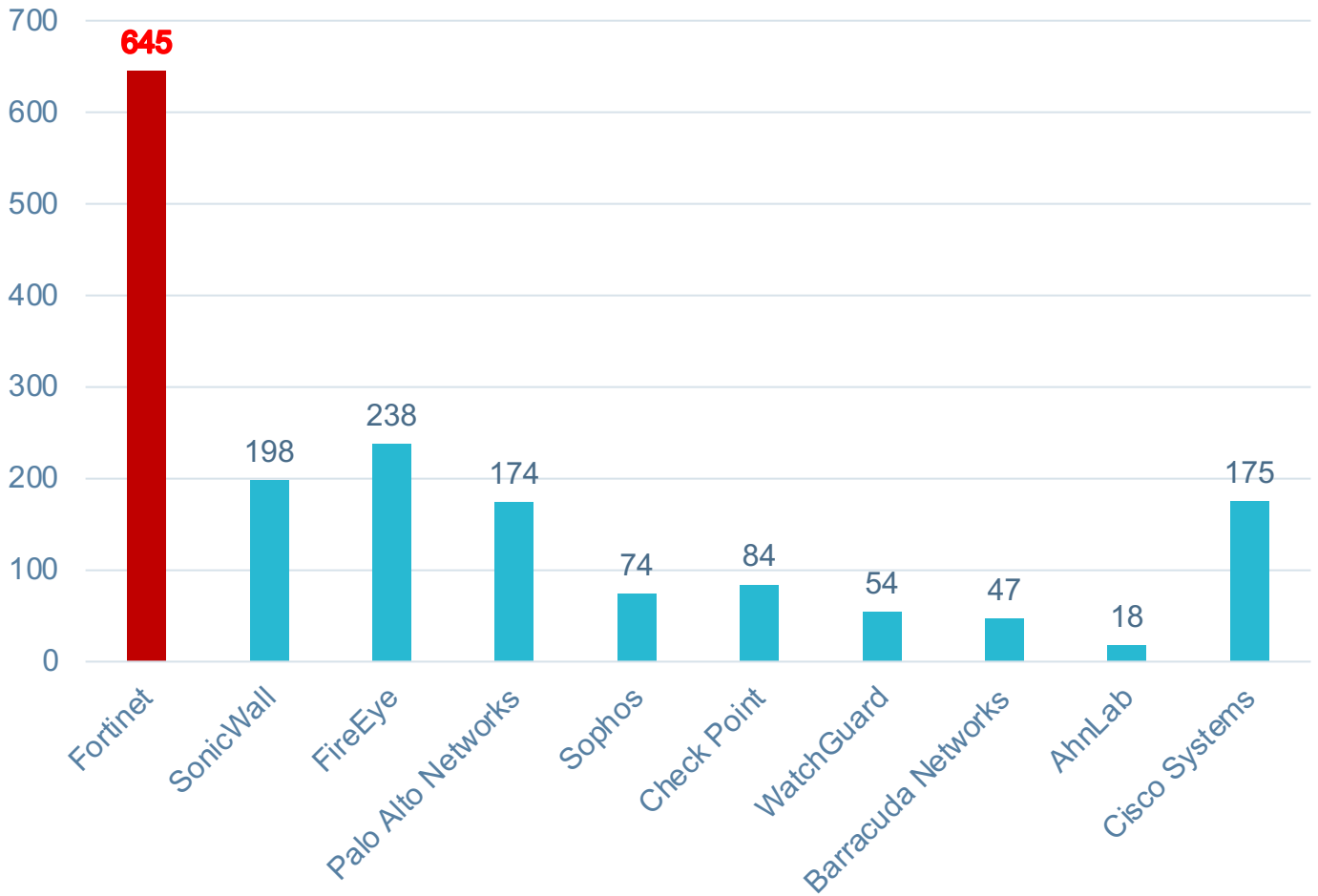
9 **NSS Labs** Recommendations

NGFW 6th year in a row!
NGIPS
DCIPS
DCSG
BPS
BDS
AEP
WAF
SD-WAN

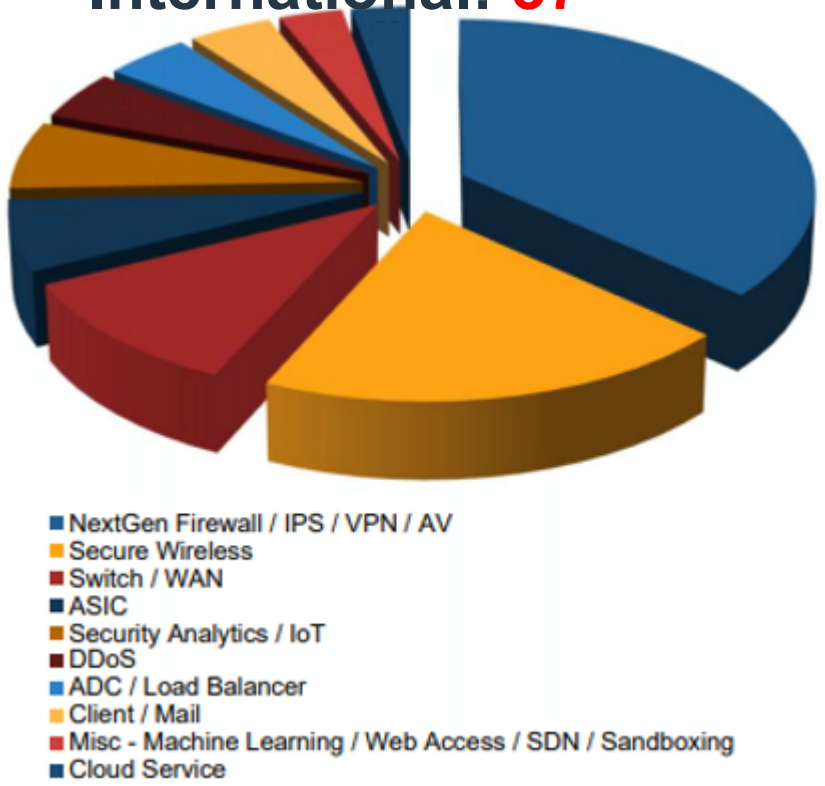
Figures as of April 2020

FORTINET

INDUSTRY LEADING INNOVATION



Issued: 645 - USA
International: 37



Based on patents issued as listed by the US Patent and Trademark Office

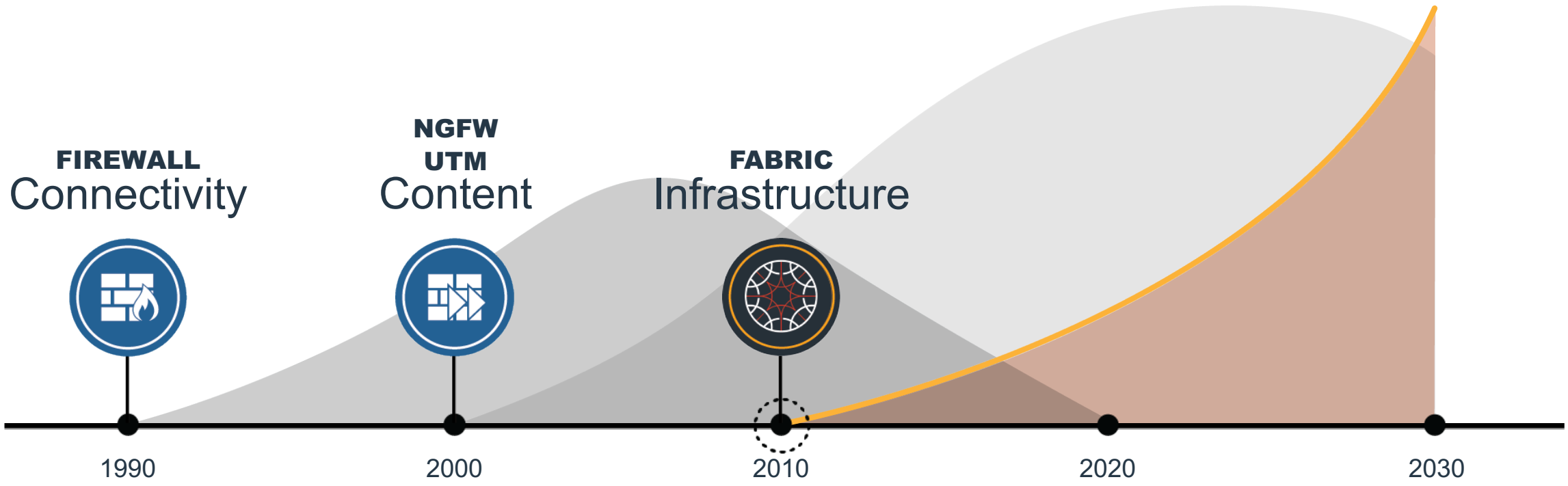
Based on information on USPTO website as of June 2020

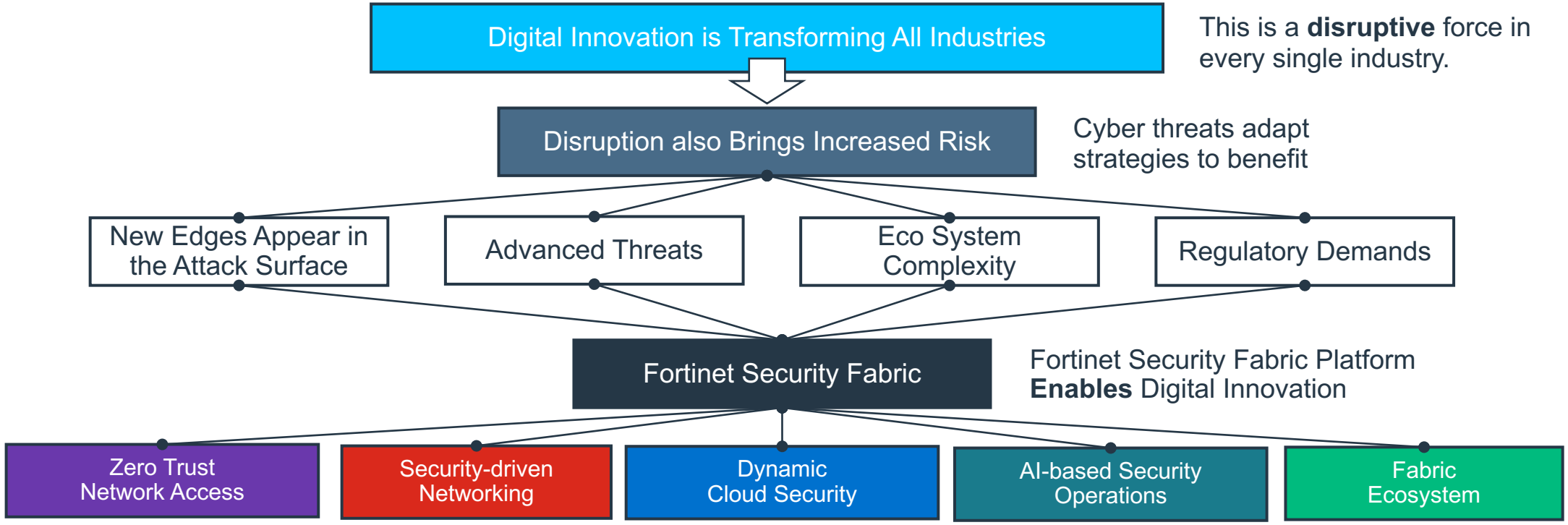
** As of June 2020 Global Patents = 682*

Network Security Evolution

Second and now third generation Network Security led by Fortinet

1ST GENERATION → 2ND GENERATION → 3RD GENERATION

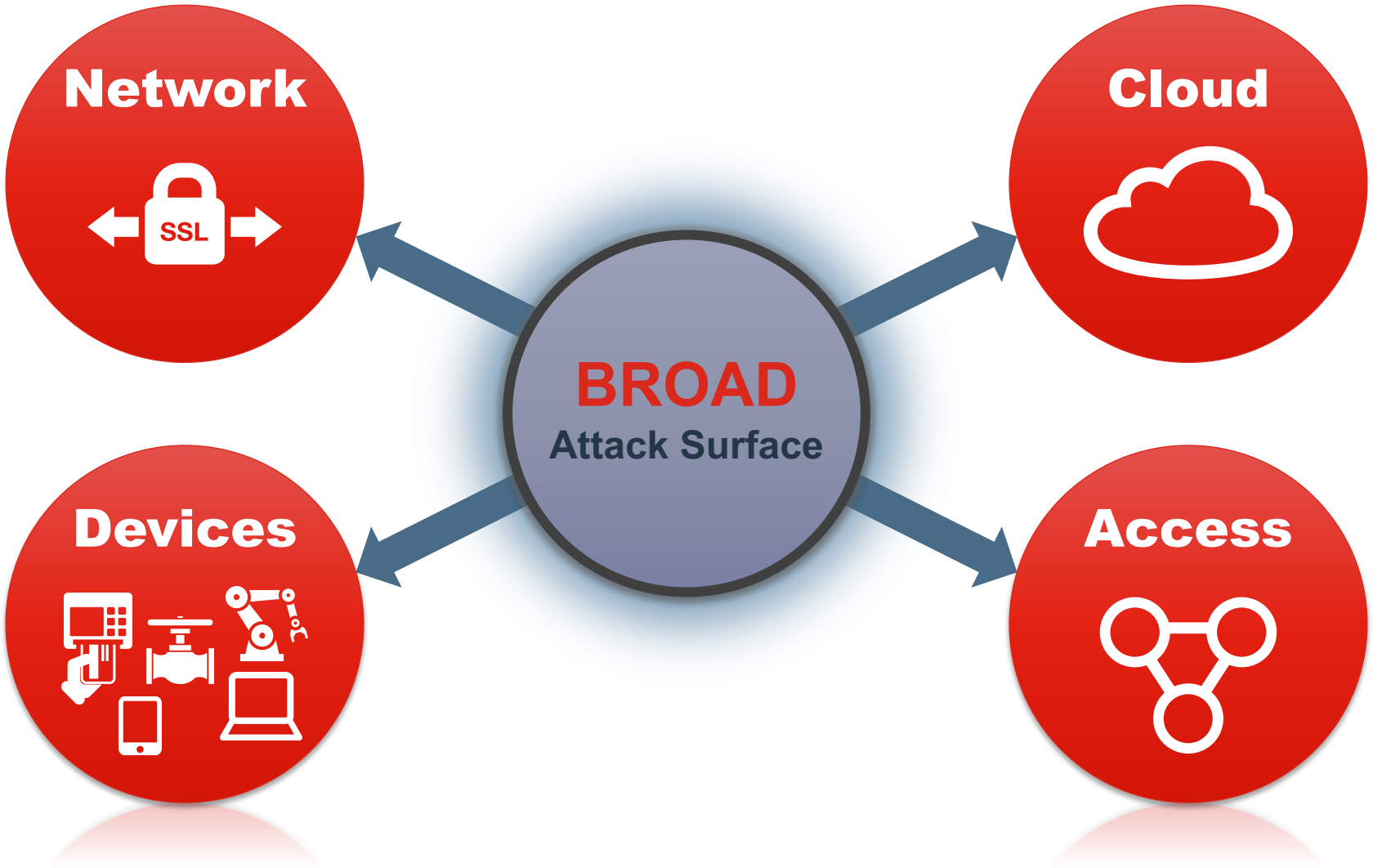




BROAD	INTEGRATED	AUTOMATED
visibility and of the entire digital attack surface to better manage risk	solution that reduces the complexity of supporting multiple point products	workflows to increase speed of operations and response

Challenge: Growing Attack Surface

Digital Attack Surface Expanding and Becoming Invisible



Ecosystem Complexity Slows Response and Mitigation

Hard to build automation

Too Many Vendors

Too Many Alerts

Manual & Slow Response

Lack of Trained People

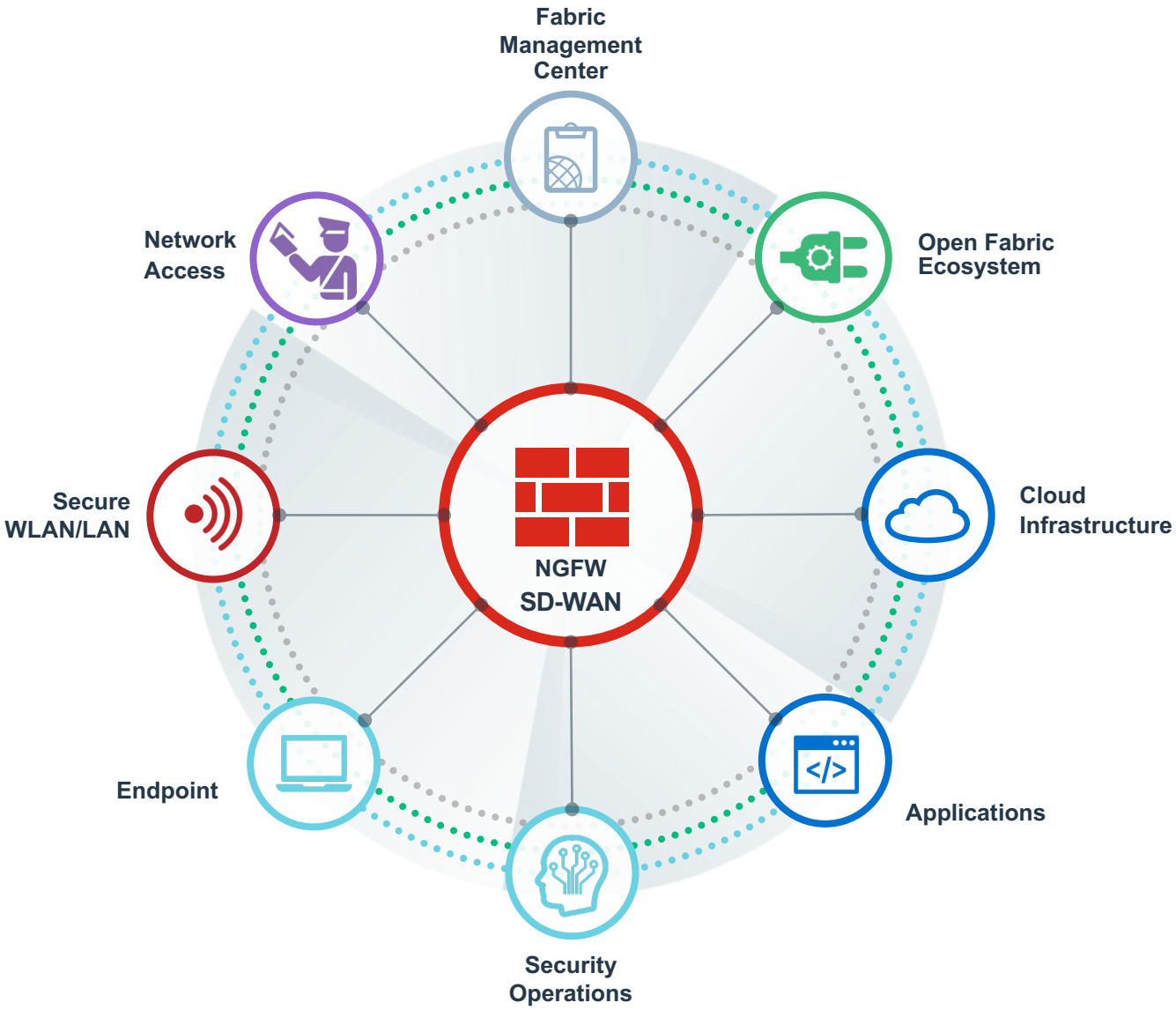
Cost & Complexity

Fortinet Security Fabric

Broad
visibility of the entire digital attack surface to better manage risk

Integrated
solution that reduces the complexity of supporting multiple point products

Automated
workflows to increase speed of operations and response



Broadest End-to-End Cybersecurity Platform

Different consumption models available

FortiGuard Services

FortiGuard Labs AI-Driven Intelligence

Billions of events analyzed every day

Information feeds
200+

CYBER THREAT ALLIANCE · KISA · INTERPOL · EUROPOL · NATO OTAN

450K customer networks
across all major threat vectors

Firewalls · Web · Emails · Endpoints

One of the Largest Security Research Teams

8 dedicated labs

31 countries

609,000 hours of research annually

Prevention
Known attacks

Detection
Unknown attacks

Intelligence
Playbooks, IR

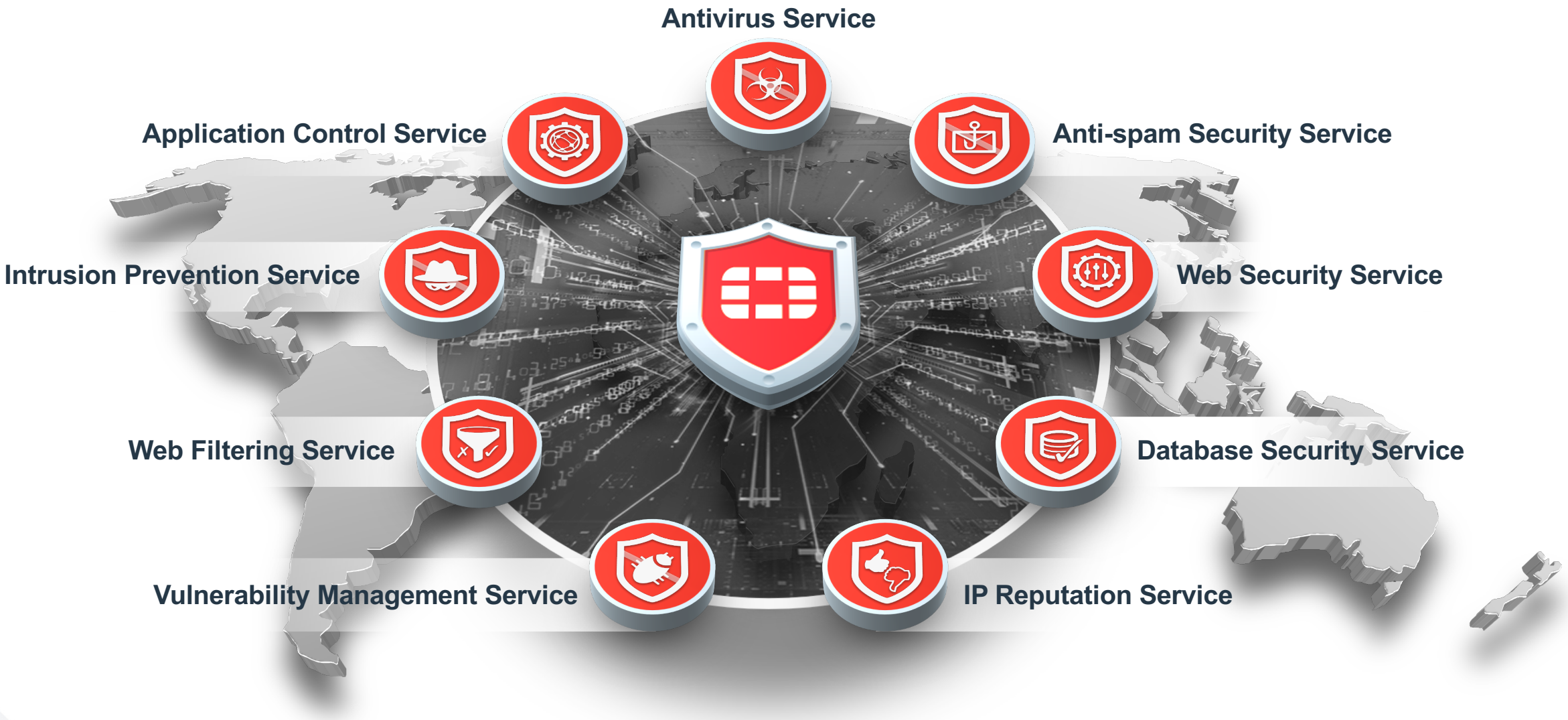
What is FortiGuard?

Fortinet Threat Research
- Malware and URL analysis
- Analysis of current threats
- Zero-day research

Development
- Antivirus Engine
- Intrusion Prevention Engine
- Signature development

Innovation
- Automation of analyst tasks
- Leveraging emerging technologies

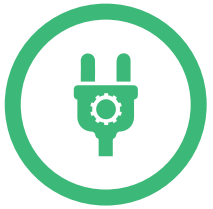
Customer Service
- Signature creation
- URL categorisation
- Premier services



Expansion of the Fabric

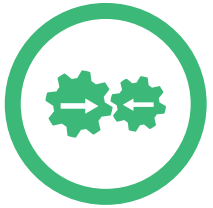
Through integration with the largest industry cybersecurity ecosystem

350+ security fabric ecosystem integrations



Fabric Connector

Fortinet-developed deep integration automating security operations and policies



Fabric API

Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions

Fabric DevOps

Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration

Extended Fabric Ecosystem

Integrations with threat sharing initiatives and other vendor technologies

Závěr - Fabric Management Center (FMC) — FMG 6.4 and FAZ 6.4

- **Way to Simplify Network Operations**
- The events of the past several months, 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.
- The percentage of network activities that will be automated will rise from 30% in early 2020 to 50% by 2023. .
- These data points help explain why 75% of network outages and performance issues are the result of misconfiguration errors.


FORTINET