



Smysluplná ochrana vs finance aneb nemusí to být “za raketu”

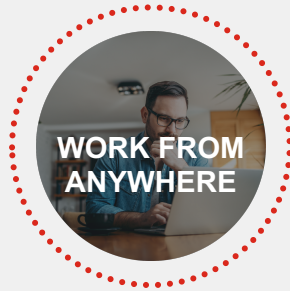
Viktor Pleštil

Major Account Manager



Digital Innovation Impacts Every Business

Many business-critical trends are driving organizations to accelerate digital innovation to transform key growth areas of their business. However, these vital efforts also exponentially grow the organization's digital attack surface and increase cyber risk.



Massive increase in remote worker access



Applications migrate to more compute platforms



Proliferation of vulnerable, network enabled devices



Growing data privacy and regulatory concerns, board level reporting



New, more sophisticated business applications



More edges appearing across the network



Zero day, supply chain, state sponsored, weaponized

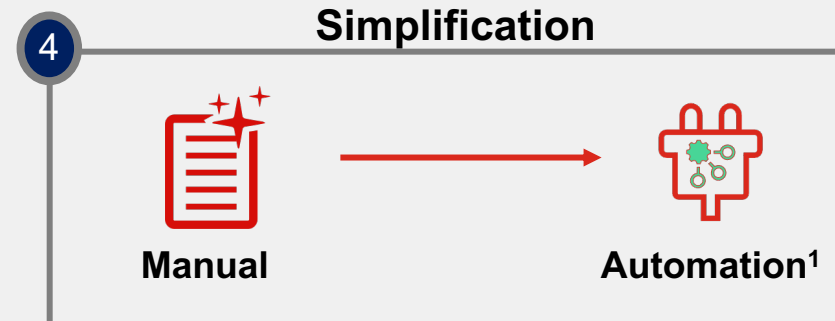
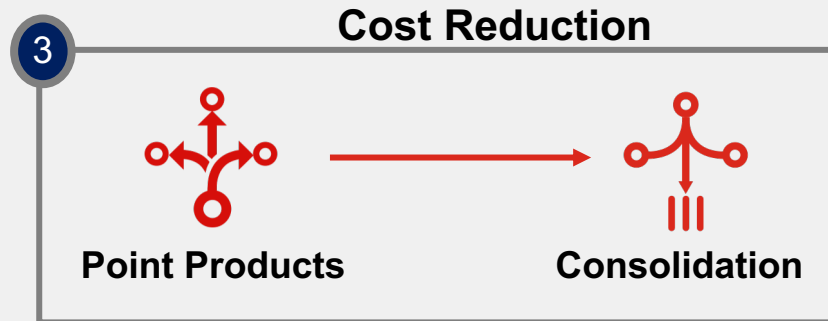
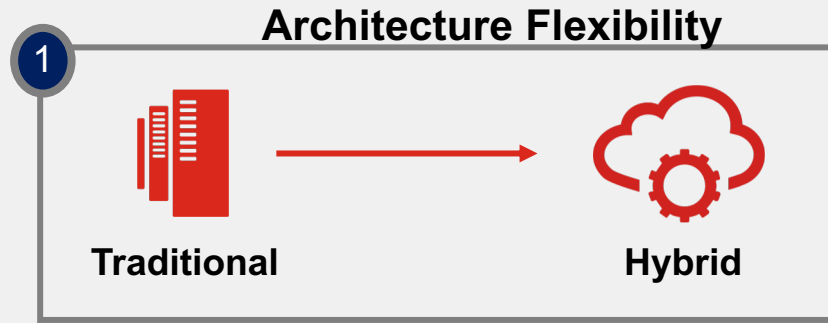


End-to-end performance becoming a critical differentiator



The Ever-Changing State of Network Security

Further Fueled by Innovations Required for New Normal



1. Gartner: Top 10 Trends Impacting Infrastructure and Operations for 2020 Published 14 April 2020 - ID G00464437



Smysluplná ochrana – co je třeba vzít v úvahu?

- Čím více – tím lépe – ne vždy platí – konfigurace je důležitější
- Parametry – co je opravdu potřeba a co je “nice to have”
- Širší portfolio vs jeden předimenzovaný product – větší riziko hrozeb z více směrů
- Hledisko personálních možností – pracnost obsluhy – analýzy, automatizace
- Firewall
- Mailová ochrana
- Sandboxing
- Endpoint protection
- Společný jmenovatel – F Fabric



FortiGuard Labs Overview



VISIBILITY



INNOVATION



ACTIONABLE THREAT INTELLIGENCE

Telemetry
Network
Web
Sandbox
Email
Endpoint

CERTs

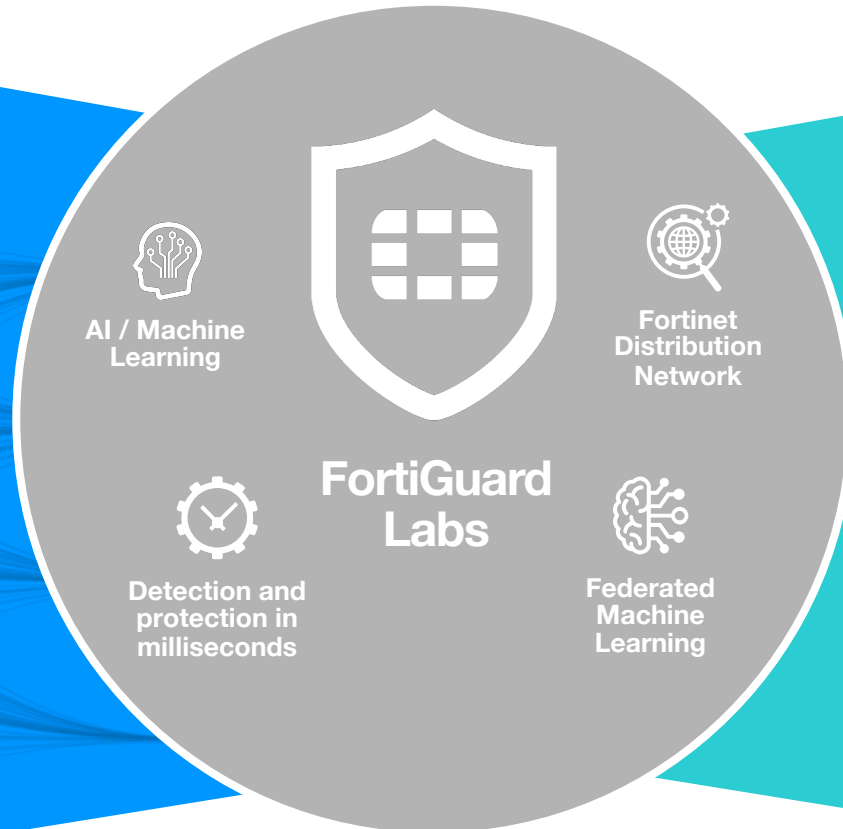
Enforcement Partnerships

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

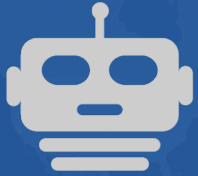
Adversary Playbooks Security Blogs Threat Intel Briefs Threat Signals Virtual Patches

THREAT CONSULTING SERVICES


Penetration Testing Phishing Service Incident Response



FortiGuard Labs Statistics (Q4 2020)



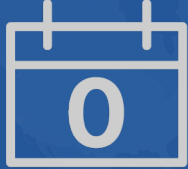
15M
BOTNET C&C
ATTEMPTS
Thwarted Per Minute



47M
SPAM
Blocked Per Day



462K
MALICIOUS
WEBSITE
ACCESSES
Blocked Per Minute



906
ZERO DAY
Threats Discovered



5.3M
NETWORK
INTRUSION
ATTEMPTS
Resisted per minute




136K
PHISHING
Blocked Per Minute



1.2 PB
OF THREAT
SAMPLES



609K
HOURS
of Threat Research
Globally Per Week



904K
MALWARE
PROGRAMS
Neutralized Per Minute

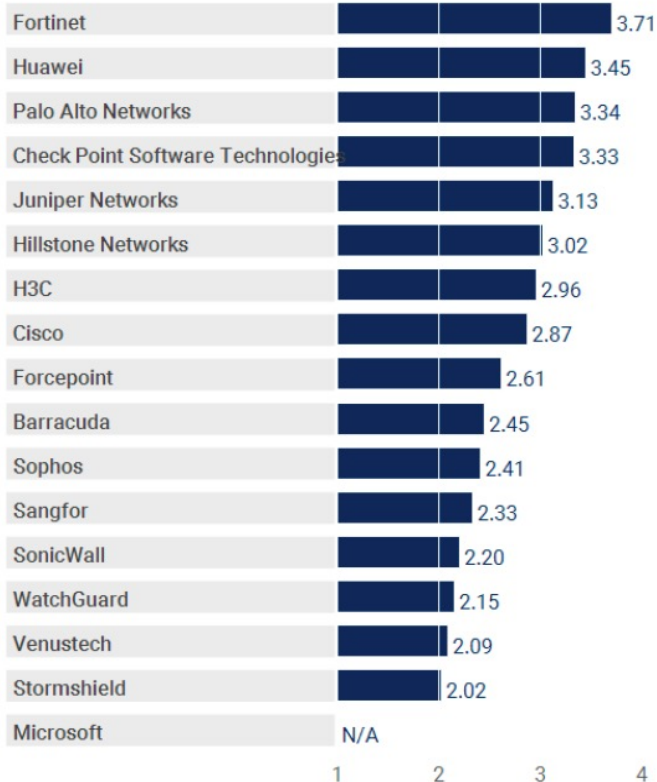


Gartner 2020 Critical Capabilities for Network Firewalls

Enterprise Data Center

Figure 5. Vendors' Product Scores for the Enterprise Data Center Use Case

Product or Service Scores for Enterprise Data Center



As of 6 November 2020

© Gartner, Inc

Source: Gartner (November 2020)

Fortinet is ranked **Highest** for the Enterprise Data Center Use Case

This marks two years in a row for scoring the highest in the Enterprise Data Center Use Case

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 of merchantability or fitness for a particular purpose.



Business Value of Adopting Network Firewalls

01 Manage Security Risks



- Trusted Application Access
- Consistent end-to-end security

02 Reduce Costs & Manage Hyperscale



- Eliminating Point products
- Deliver Optimal User Experience

03 Higher Operational Efficiency



- Minimize business disruptions
- Streamline enterprise-wide workflows



Expect More From A Network Firewall

FortiGate Delivers **Unparallel** Enterprise Grade Security

Hybrid IT



**VDOM & HW
accelerated VXLAN**

Cloud On
Ramp



**100G Elephant
Flows**

Latency Sensitive
Applications



**Single Digit
microsecond
latency**

Hosting DMZ



**HW assisted Load
Balancing**

Application
Protection



Integrated WAF

Secure & Superfast
DCI



40+Gbps Per Tunnel

High Performance
Edge



**Full BGP with
multiple ISPs**

Operation
Resiliency

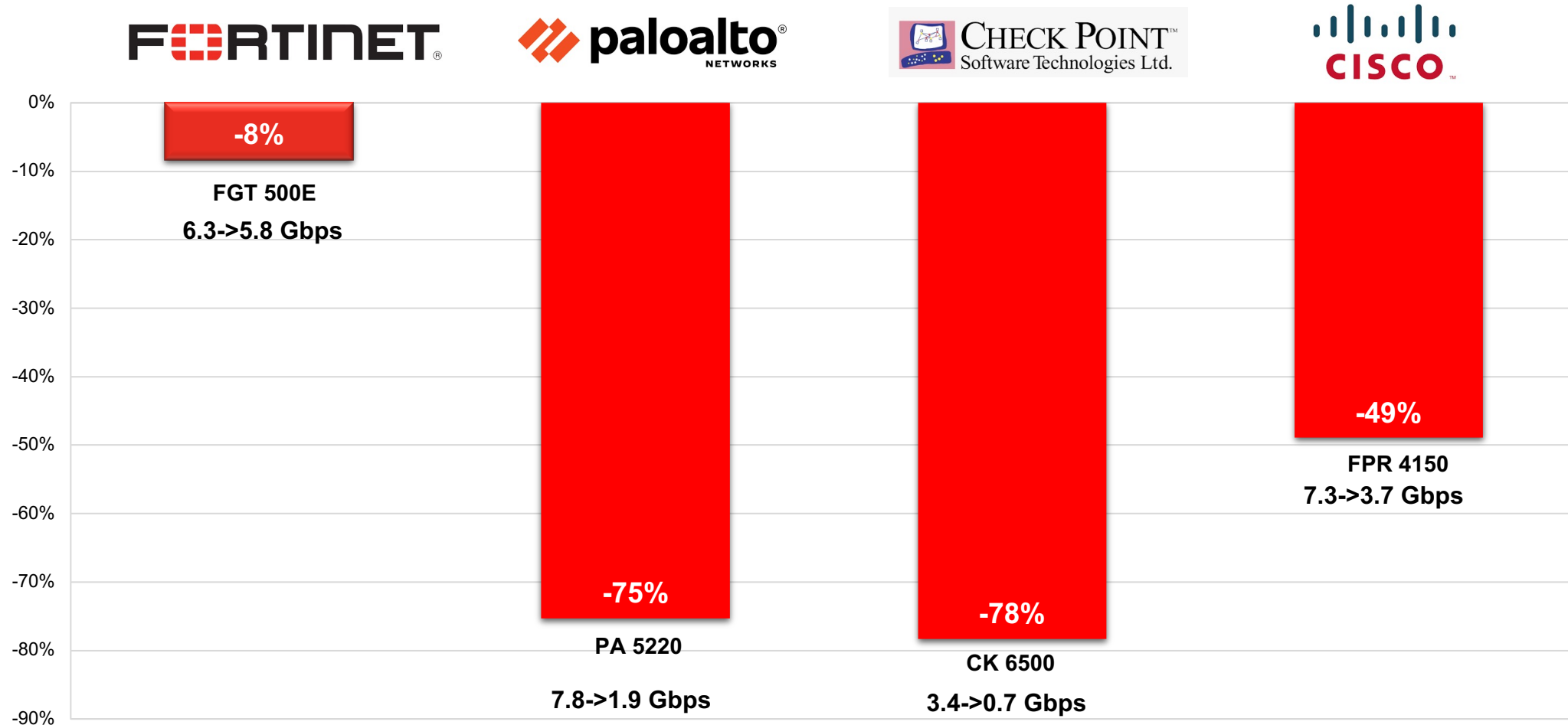


**Hardware Level
DDoS Protection**



SSL Inspection Is the Key to Detect Hidden Threats

NSS Labs NGFW 2019 – New SSL Performance Test

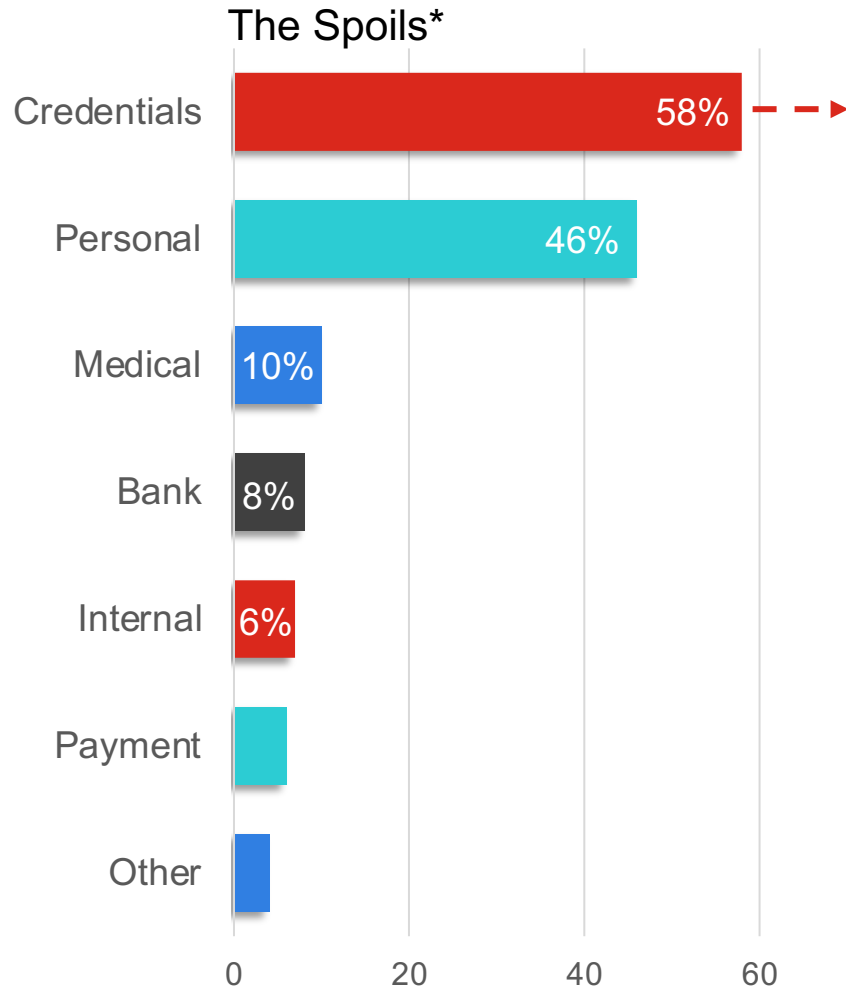


HTTP → HTTPS Performance Decrease

© Fortinet Inc. All Rights Reserved.



Email's use as a primary threat vector...



Percent of breaches involving ransomware, up from ~5% the prior year.*



Average cost of a data breach worldwide.**



*Statistics from Verizon Data Breach Investigations Report 2021.

**Ponemon Institute Cost of a Data Breach Report 2020.

The trend toward cloud-based email



Percent of companies using cloud or hybrid cloud email today.*



Percent of companies that will use native-built security controls in 2023.*



How **effective** are **native/built-in** email security tools?

*Gartner, "Market Guide for Email Security," authors Mark Harris, Peter Firstbrook, Ravisha Chugh, published September 8, 2020.



Performance results from SE Labs

Great email - Not so great email security

EXECUTIVE SUMMARY				
Product	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)
Perception-Point	2,603	700	3,303	94%
Fortinet FortiMail	2,525	640	3,165	90%
Mimecast Secure Email Gateway	2,412	700	3,112	89%
Kaspersky Security for Office 365	1,681	550	2,231	64%
Google G Suite Enterprise	956	505	1,461	42%
Google G Suite Business	825	535	1,360	39%
Microsoft Office 365	463	550	1,013	29%
Microsoft Office 365 Advanced Threat Protection	426	550	976	28%



Google Workspace
Microsoft 365

More malicious threats, more spam and more risk is getting through to organizations using Microsoft 365.

Source: "EMAIL SECURITY SERVICES PROTECTION: Jan – Mar 2020," SE Labs – April 2020

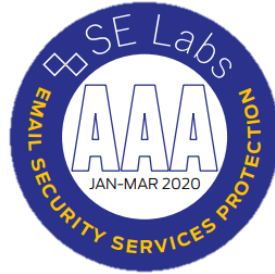


High marks in performance across 3rd party testers



99.9%

Detection of malicious emails across malware types and across malware families.



94%

Overall Detection Rate

91%

Protection and Legitimate Handling Rate

90%

Total Accuracy Rate



99.78%

Spam Catch Rate

94.71%

Malware Catch Rate

93.01%

Phishing Catch Rate



100%

WildList Detection Rate



Options for any organization size and deployment

FortiMail

We want full control.

FortiMail solutions for organizations that prefer full control and management over their email security.

Appliances

- 6 models
- Filter 30K to 2.0M messages per hour*
- Support for 10GE

Virtual Machines

- 6 VM models
- CPU and domain-based
- Perpetual licensing or On-Demand



FortiMail Cloud

Manage it for us.

FortiMail Cloud solutions for organizations that want email security-as-a-service.

SaaS/API*

- Fully-managed by Fortinet
- Gateway or Server mode
- Standard or Premium
- Per user per year



*FortiGuard Enterprise ATP (per hour)

© Fortinet Inc. All Rights Reserved.

Sandbox Borne From **FORTIGUARD LABS**

Since 2000, FortiGuard Labs has provided in-house, industry-leading security intelligence and research, powering Fortinet's platform and delivering a suite of advanced services

Industry Leading Patented Security Technology



Zero-day Research

- 900+ 0-days discovered (2021)

Delivering Advanced Technologies

- FortiSandbox Machine Learning Model
- FortiWeb Machine Learning Model

Delivering Intelligence Services

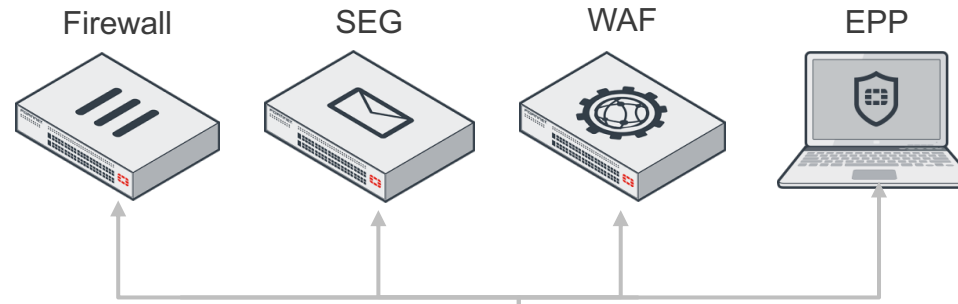
- CPRL AV, IPS, App Control, IP Reputation, Web Filter, Anti-Spam, Web Security App, Vulnerability Management
- Virus Outbreak Service and Content Disarm & Reconstruction (FortiMail and FortiGate)

Published Research

- Quarterly Threat Report
- Bi-weekly Threat Brief
- Blogs



How Should We Address 0-day Threats?



Zero-Day Intelligence Hub

Code Continuum	Known Good	Probably Good	Might be Good	Completely Unknown	Somewhat Suspicious	Very Suspicious	Known Bad
Security Technologies	Whitelists	Reputation: File, IP, App, Email App Signatures, Digitally signed files	Sandboxing			Heuristics Reputation: File, IP, App, Email Generic Signatures	Blacklists Signatures



Integrated and Automated 0-day Protection

Use-case: 0-day Protection for Network, Email and Endpoint (IT/OT)

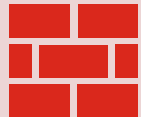


Third Generation **AI-Powered Sandbox**
Accelerates **Detection** and Increases **Efficacy**

Threat Intelligence

NETWORK

Secure SD-WAN and NGFW



- Secure North-South, East-West internet- and internal-based traffic
- Stop malware delivery, callbacks, lateral spread in clear, and encrypted channel

EMAIL

Secure O365



- Secure email attachment and URL phishing
- Disrupts patient-zero by blocking initial email infection

ENDPOINT

Secure IT/OT Devices



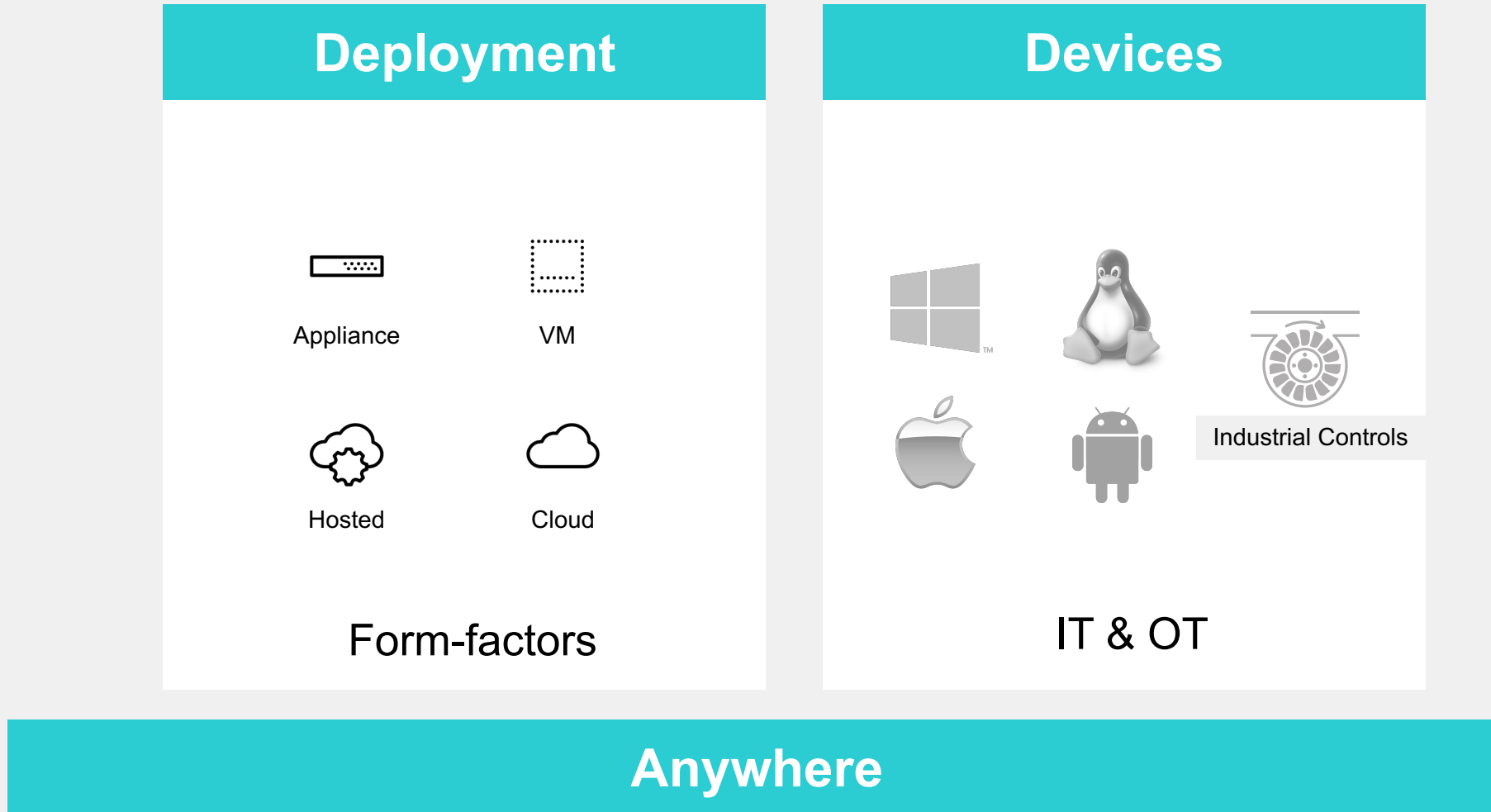
- Secure against execution of malware on IT systems (Win, macOS, Linux, Android) and OT systems (modbus, bacnet, etc)
- Stops endpoint compromise i.e. data exfiltration, destruction, corruption, etc.

Automated Breach Protection



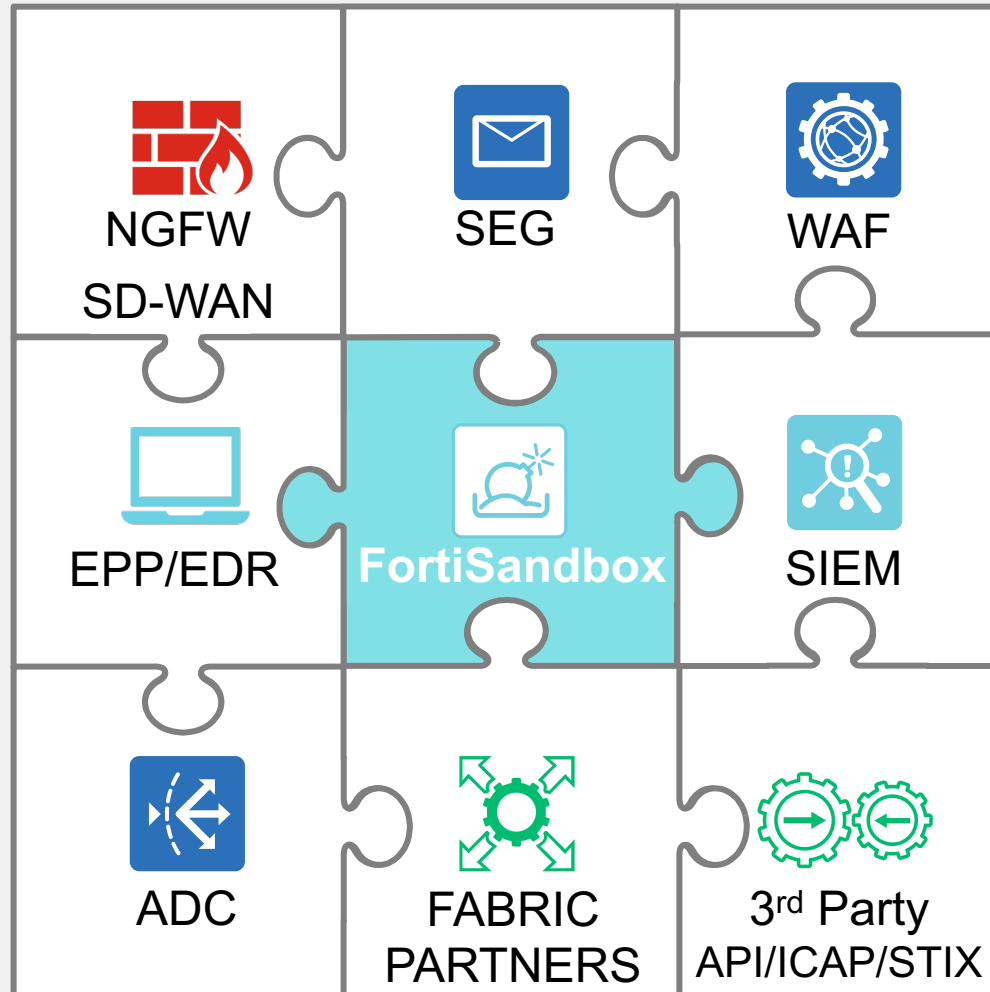
Broad Coverage

Flexible deployment to protect the dynamic attack surface



Integrated Protection

Across Fortinet and Non-Fortinet Products



OS Support



Industrial Controls



Endpoint Security Gaps



63% of companies can not monitor off-network endpoints, over half can't determine endpoint compliance status


Lack of Visibility



According to Gartner

Through 2021, **99%** of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

Vulnerabilities



87%

Most compromises took minutes, or less

Attacks are fast moving

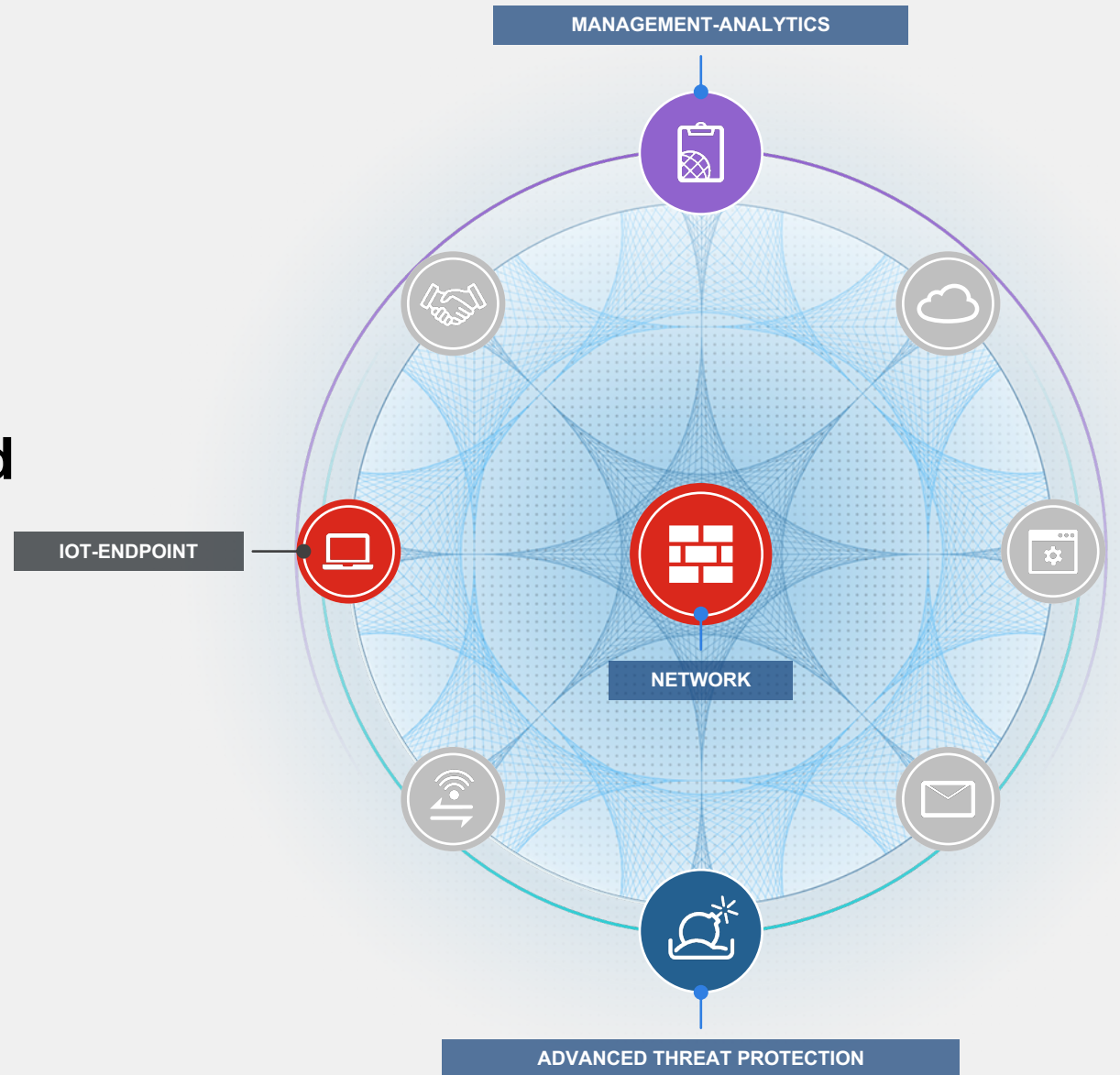
Sources:

1. The Cost Of Insecure Endpoints, Ponemon Institute, 2017
2. Gartner, How to Respond to the 2018 Threat Landscape, Greg Young, 28 November, 2017
3. Breach Investigation Report, Verizon, 2018



Fabric-enabled Endpoint Protection Delivers...

- **Integrated endpoint visibility and compliance control**
- **Proactive endpoint defense**
- **Automated threat containment and outbreak control**
- **Secure remote access**



FortiClient is more than just Endpoint Security



Fabric Agent



Vulnerability Management



Sandbox Agent



Anti-Malware Protection



Remote Access



Software Inventory



Works with other 3rd Party AV as additional layer of protection *



„Případová studie“

- 250 - zaměstnanců
- 3 lokality – centrála a dvě pobočky
- HW – FG v HA, HW - Sandbox, FAZ, Mail – VM, FCL
- 24 měsíců

➤ Zakázka malého rozsahu



Fortinet makes possible a digital world you can always trust

Fortinet's mission is to secure people, devices, and data everywhere.



FORTINET®