Efektívna obrana proti kybernetickým útokom s Fortinet Security Fabric

Zsolt Géczi, CEH, regional manager sales, Slovakia

Who is Fortinet?

Poslaním spoločnosti Fortinet je už viac ako 20 rokov zabezpečovať ľudí, zariadenia a údaje všade na svete.

Sme hybnou silou vývoja kybernetickej bezpečnosti a konvergencie sietí a bezpečnosti. Naše riešenia sieťovej bezpečnosti sú najrozšírenejšie, najpatentovanejšie a patria medzi najviac overené v odvetví.

Nasdaq 100
Nasdaq: FTNT
Publicly Traded

S&P 500
Nasdaq: FTNT
GAAP Profitable

BBB+ Baa1
Security Investment Grade Rating
Financially Stable

$4.18B
FY2021 Billing
Top 3

50+
Integrated Fabric Products
Broadest Attack Surface Coverage

ASIC
Security Processing Unit (SPU)
High Performance

© Fortinet Inc. All Rights Reserved.

Broad Global Footprint

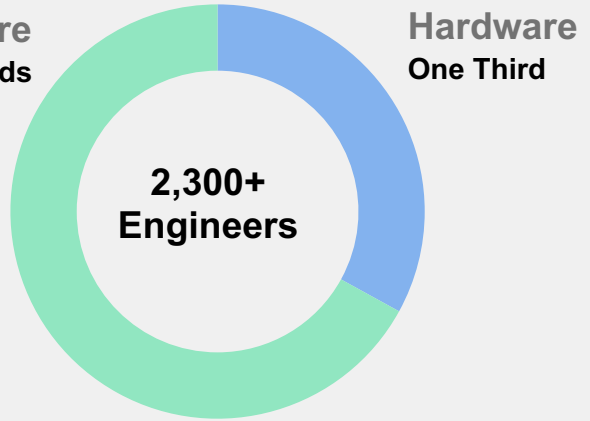
Majority of our R&D is in North America

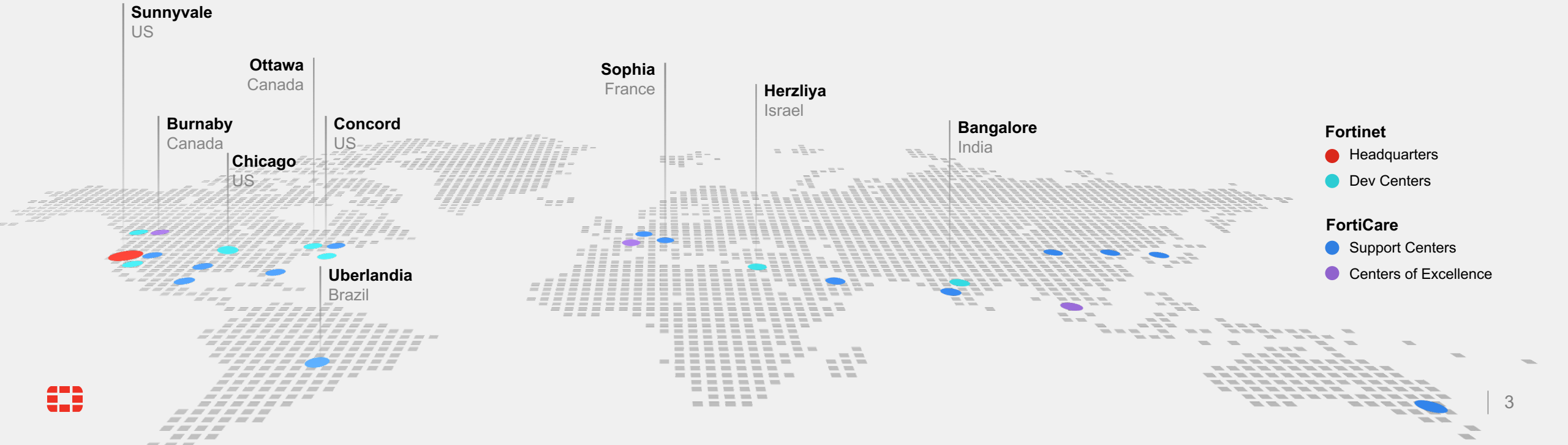
1,269
Patents Globally
Top Innovator

10,800+
Employees
Global Leader

580,000+
Customers Worldwide
Massive Customer Input

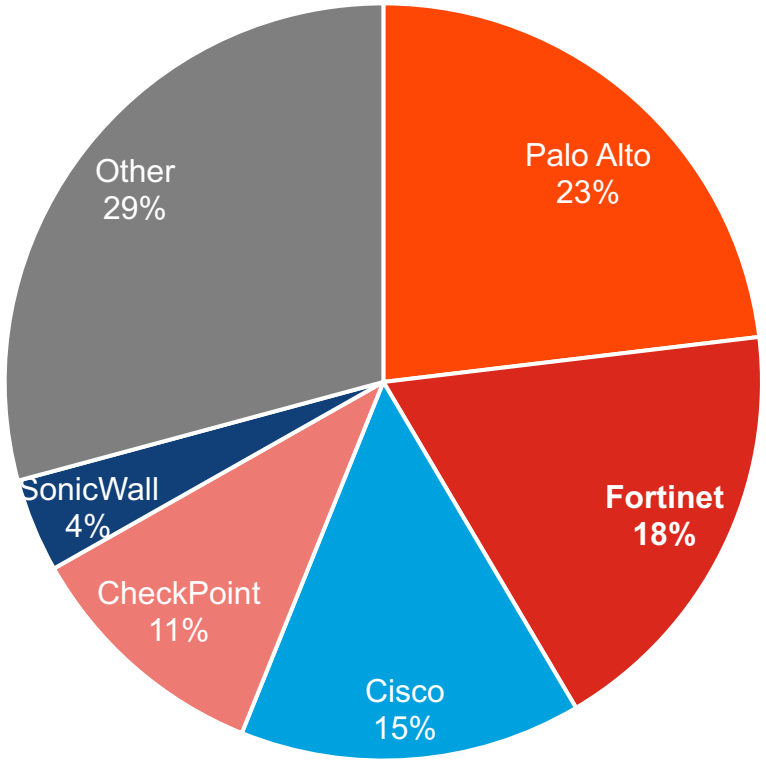
8.4M+
Global Firewall Shipments
Huge Scale

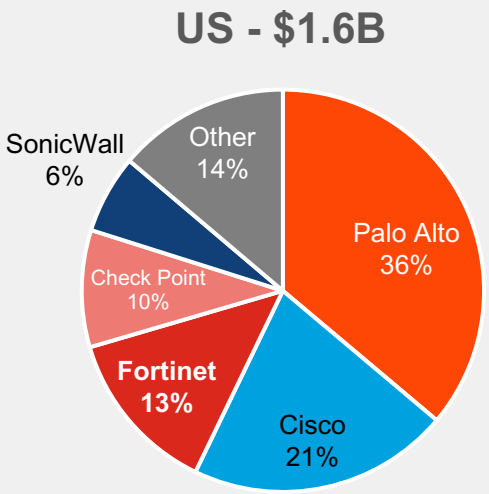


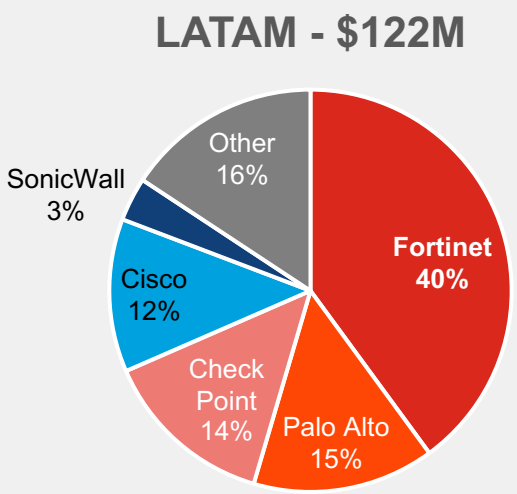


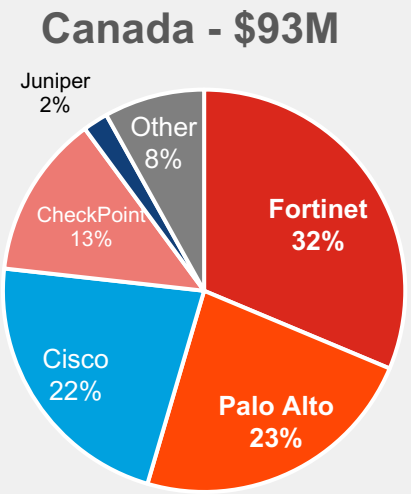
IDC Firewall Appliance Market Share by Revenue

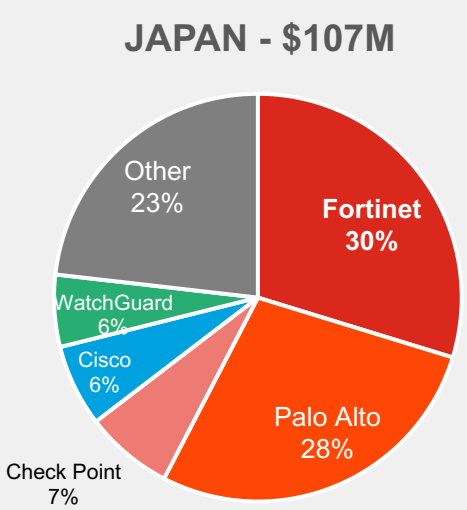
Q3 2021 Data

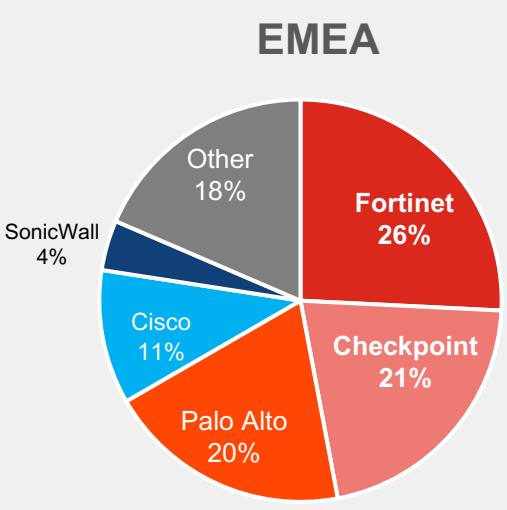


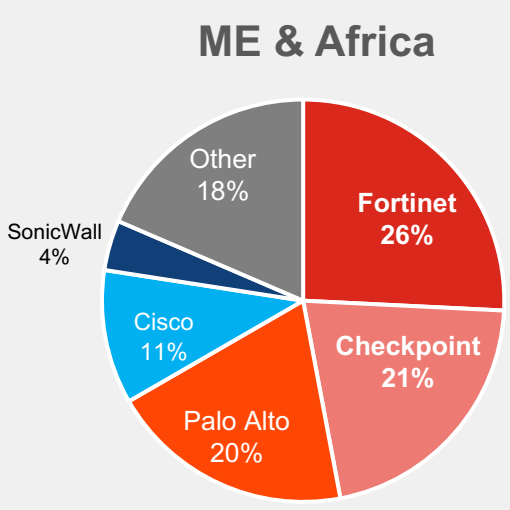












© Fortinet Inc. All Rights Reserved.

Segmenty, horizontály a vertikály

Enterprise

Government
Financial
Healthcare
Retail
Technology
…

Small Business

Consumer
SOHO
Small Business
Medium Business
…

Service Provider

Network
Service
Provider

MSSP

5G
…

Operational Technology

Manufacturing
Oil and Gas
Energy
Transport
…

© Fortinet Inc. All Rights Reserved.

Jeden OS pre Siete aj Bezpečnosť

Jediný výrobca uznávaný ako líder medzi SD-WAN a sieťovým firewallom

Sept. 2021 Magic Quadrant for WAN Edge Infrastructure

Fortinet Recognized as a Leader

Nov. 2021 Magic Quadrant for Wired & Wireless LAN Access Infrastructure

Fortinet Recognized as a Visionary

Nov. 2021 Magic Quadrant for Network Firewalls

Fortinet Recognized as a Leader

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.

© Fortinet Inc. All Rights Reserved.

2022 Súhrn Hrozieb

Perforated Attack Surface

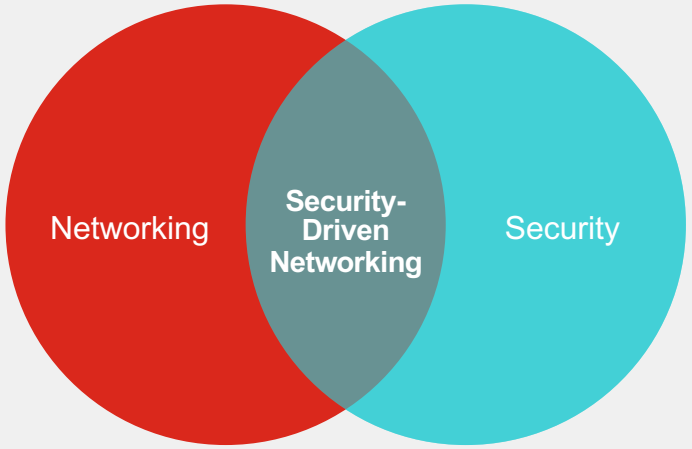
© Fortinet Inc. All Rights Reserved.

Dlhodobé strategické Trendy a Technológie

Reduced Complexity and Rapid Response

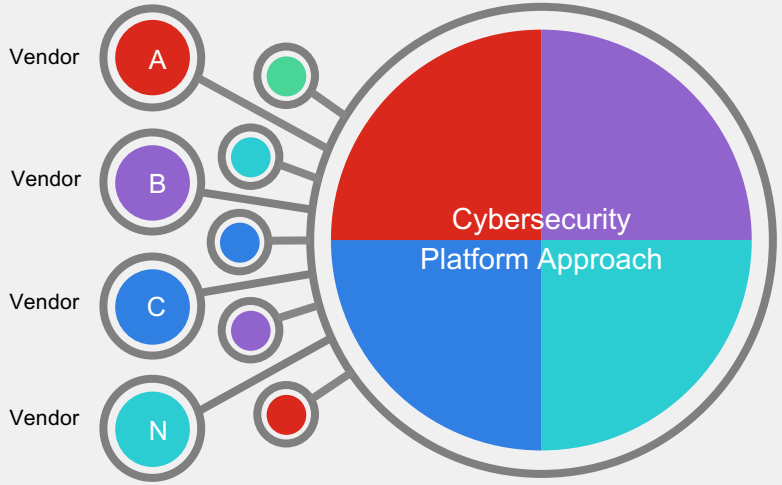
Threat Landscape

Convergence of Networking and Security



Proof points: Gartner Enterprise Networking Market Forecast

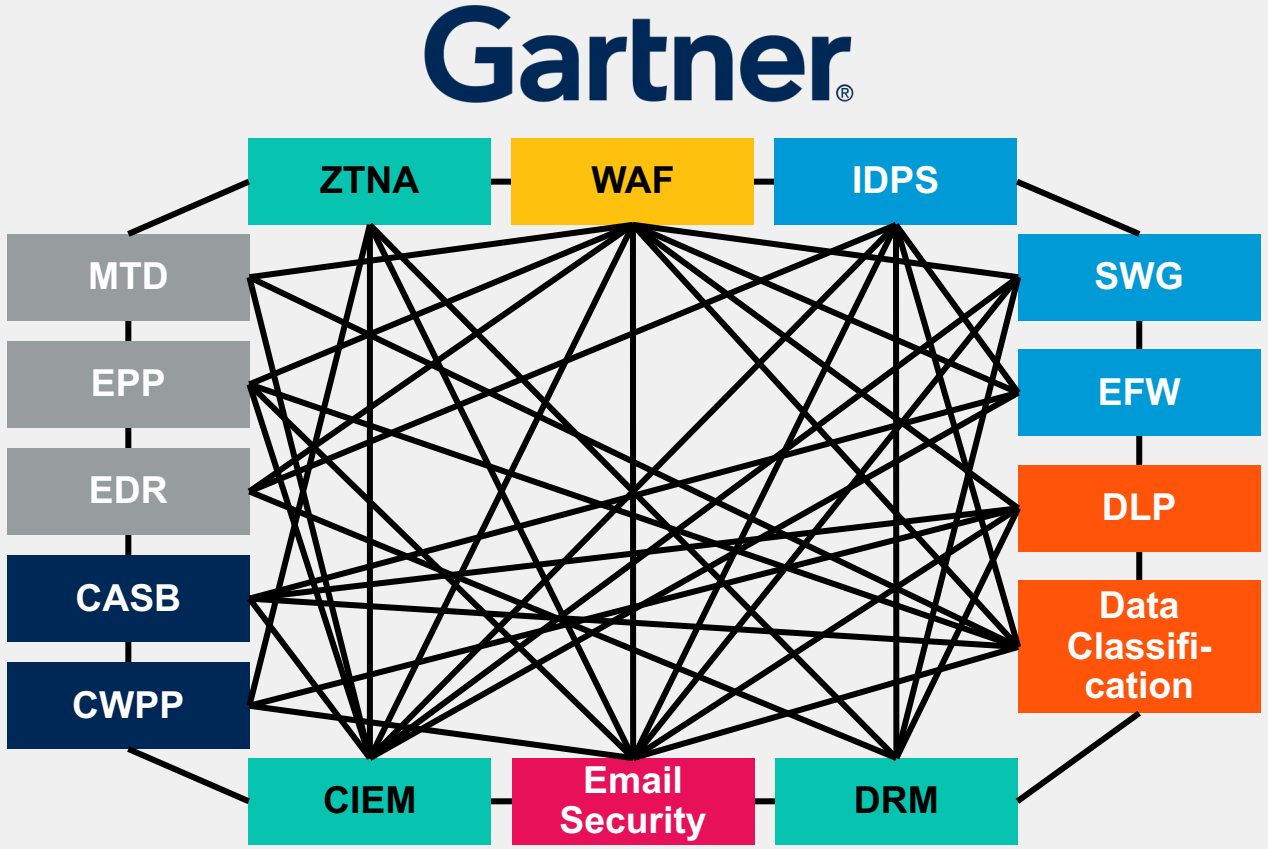
Consolidation of Security Point Product Vendors



Proof point: Gartner Cybersecurity MESH Architecture

© Fortinet Inc. All Rights Reserved.

Gartner Cybersecurity Mesh Architecture (CSMA)



MESH Benefits

Improved Organizational Risk Posture and sharing of Policy and Threat Intelligence

Increased Speed to respond through automation

Reduced Spending on individual vendor licenses

Reduced staffing and training across many different products

Executive Guide to Cybersecurity Mesh, 2022 Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

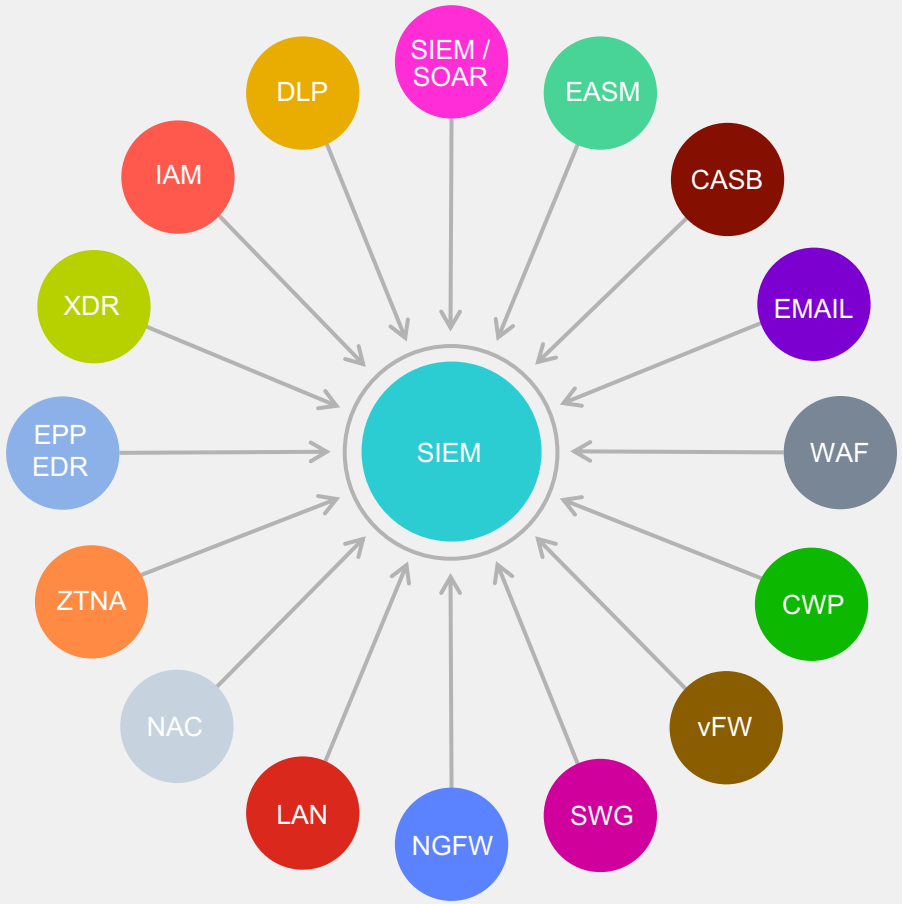
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

© Fortinet Inc. All Rights Reserved.

Konsolidácia bezpečnostných riešení

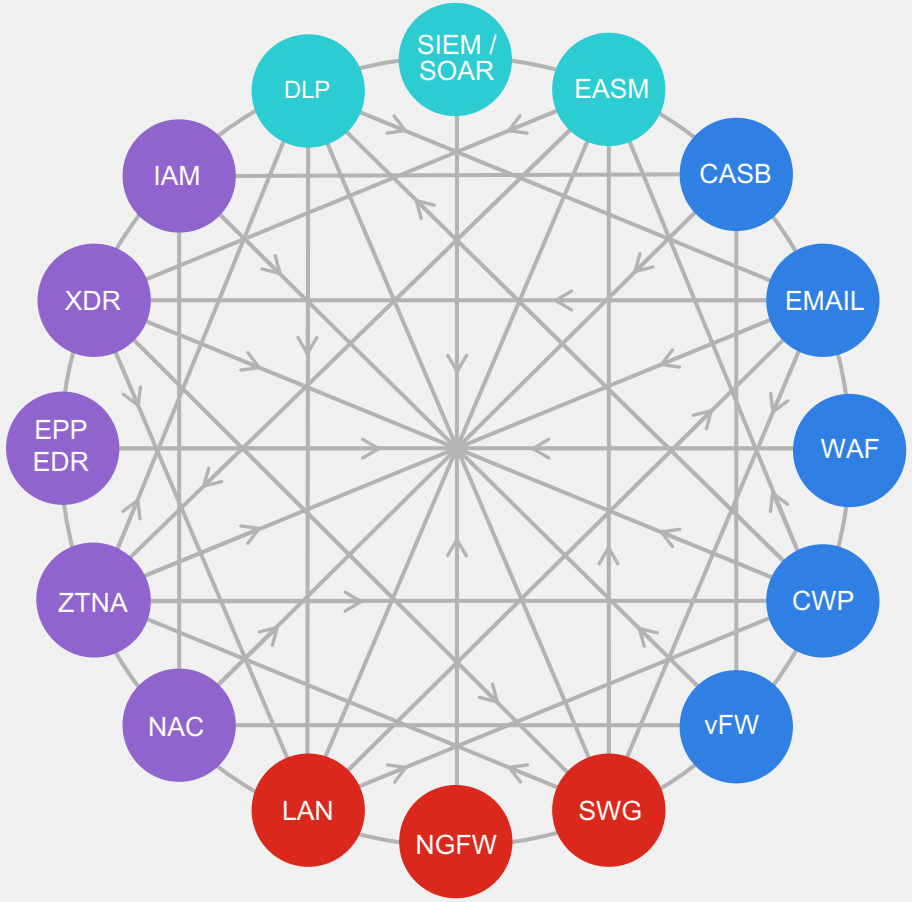
Gartner Cybersecurity MESH Architecture (CMSA)

Cybersecurity Point Products



20 Vendors

Cybersecurity Platform Approach



4-6 Platforms

© Fortinet Inc. All Rights Reserved.

Fortinet Security Fabric

Široký

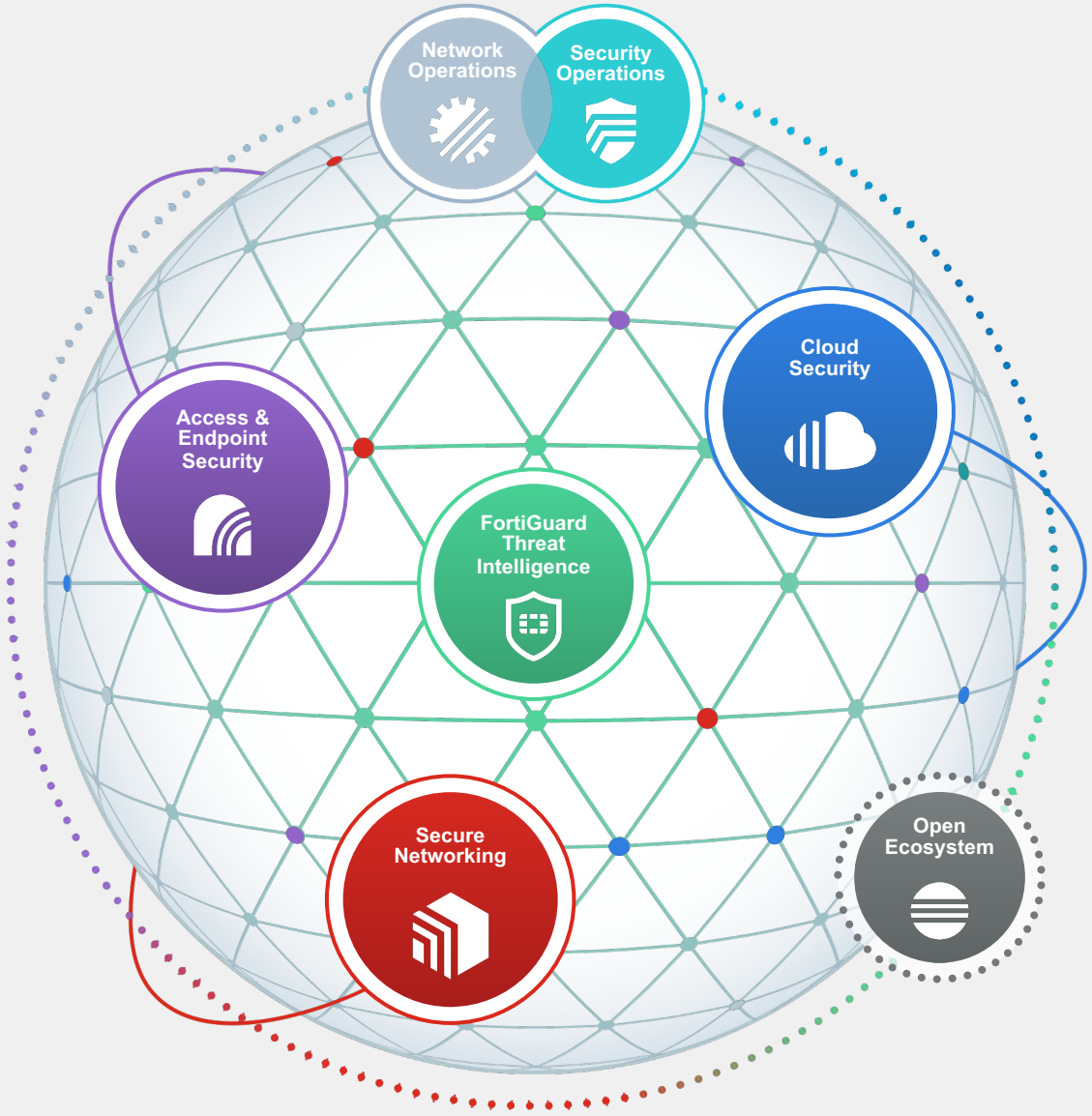
viditeľnosť a ochrana celého digitálneho útočného priestoru s cieľom lepšie riadiť riziká.

Integrovaný

riešenie, ktoré znižuje zložitosť správy a zdieľa informácie o hrozbách

Automatizovaný

samoregeneračné siete so zabezpečením založeným na umelej inteligencii pre rýchlu a efektívnu prevádzku



Appliance

Virtual

Hosted

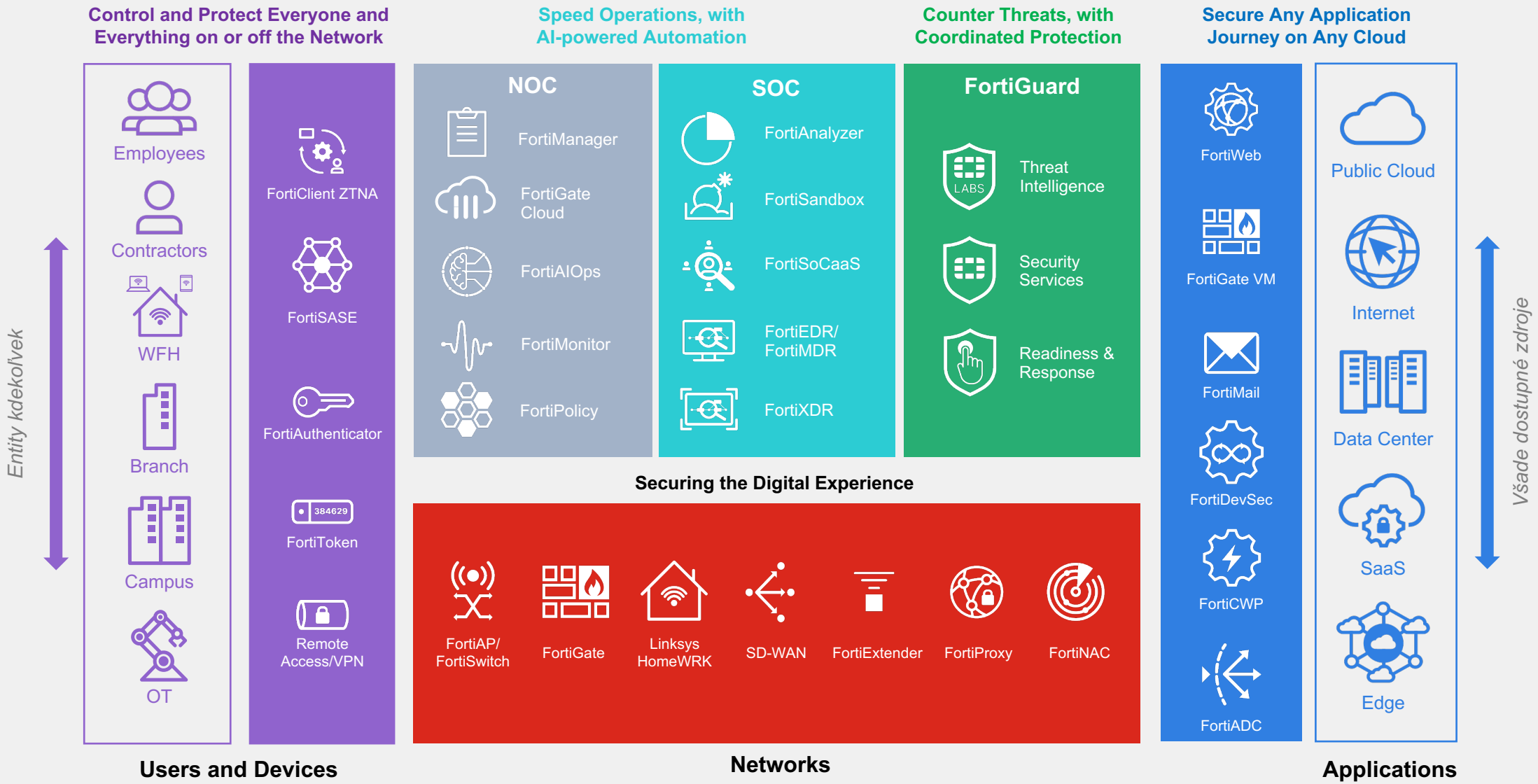
Cloud

Agent

Container

© Fortinet Inc. All Rights Reserved.

Fortinet Technology Vision



© Fortinet Inc. All Rights Reserved.

Fortinet Security Fabric

Cybersecurity Platform to Enable Digital Innovation

FortiOS
The Heart of the Fortinet Security Fabric

Zero Trust Access

FortiNAC
Enforce dynamic network access control and network segmentation

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiClient
Endpoint integration, visibility, and protection across entire network

FortiToken Mobile
One-time password application with push notification

Surveillance & Communications

FortiRecorder
Platform for management of cameras, systems, and storage

FortiCamera
Centrally-managed HDTV-quality security coverage reliability

FortiVoice
Centralized control and simplified management of phone systems

FortiFone
Robust IP Phones w/ HD Audio for versatile deployments

Security-Driven Networking

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiSwitch
Deliver security, performance, and manageable access to data

FortiAP
Protect LAN Edge deployments with wireless connectivity

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiSASE
Secure access service edge to deliver security everywhere

FortiProxy
Enforce internet compliance and granular application control

FortiIsolator
Maintain an "air-gap" between browser and web content

FortiPresence
Real-time location trends, visitor analytics, and heat mapped flows

Fabric Management Center | SOC

FortiXDR
Collect, normalize, and correlate data across security controls

FortiEDR
Automated protection and orchestrated incident response

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSandbox
Secure virtual runtime environment to expose unknown threats

FortiDeceptor
Discover active attackers inside with decoy assets

FortiAI
Accelerate mitigation of evolving threats and threat investigation

FortiGuard MDR Service
Monitor and hunt for threats; analyze events; leverage alerts

Adaptive Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiMail
Secure mail gateway to protect against SPAM and virus attacks

FortiWeb
Prevent web application attacks against critical web assets

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

FortiADC
Application-aware intelligence for distribution of application traffic

FortiCWP
Manage risk and compliance through multi-cloud infrastructures

FortiGSLB
Ensure business continuity during unexpected network downtime

FortiDDoS
Machine-learning quickly inspects all Layer 3, 4, and 7 packets

FortiCloud Networking
Manage network access, assets, and services through single-pane

FortiPhish
Informative simulation to educate internal users of potential threats

Fabric Management Center | NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiCloud
Protect and deliver data and apps in the Cloud and on-premises

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

Open Ecosystem

Extended Fabric Ecosystem

FortiGuard Security Services

Content Security
Web Security | Advanced SOC/NOC
User Security | Device Security

SOC & NOC | User Security

Revised October 1, 2021

Icons on this document link to additional information

© Fortinet Inc. All Rights Reserved.

Boj proti hrozbám v reálnom čase pomocou koordinovanej ochrany s podporou umelej inteligencie

FortiGuard Threat Intelligence

Powered by FortiGuard Labs

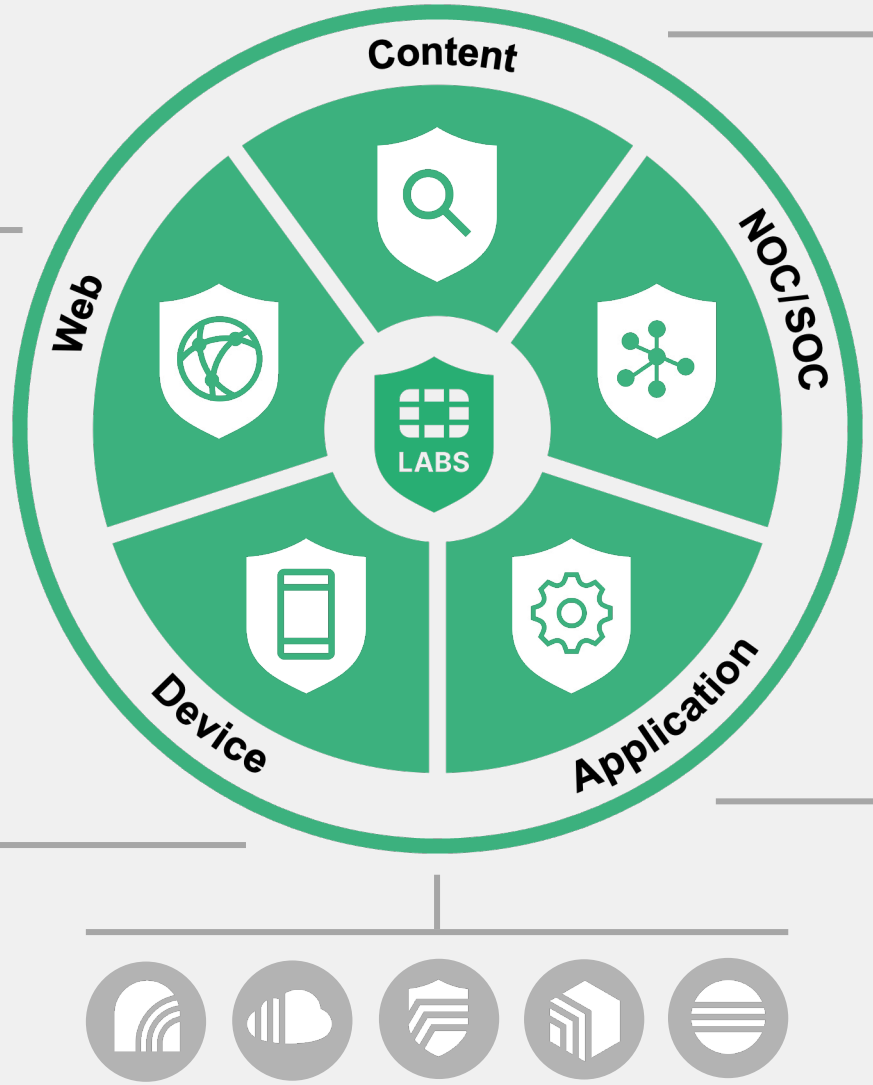
FortiGuard AI-Powered Security

Portfolio

Web
- URL Filtering
- DNS security
- Secure Web Gateway
- Phishing
- Geo-location
- In-line CASB
- Anti-spam

FortiGuard Labs
- Real-Time Security update
- AI & Machine Learning models developments on both local and large-scale Cloud-driven data lakes
- Zero-Day discovery
- Outbreak Alerts
- Threat Monitoring and Communications
- Industry Alliances

Device (IT | OT | IoT)
- Exploit Protection
- Vulnerability Detection & Patching
- IPS Known and Zero-Days
- Botnet & C2



Content
- AI Sandbox & EDR Behavior
- Polymorphic Anti-Malware | Antivirus
- Mobile Malware
- Credential-stuffing defense

NOC/SOC
- Decoys
- IOC Ingestion and Search
- Advanced Forensics & Threat Hunting
- AI-powered investigation & Automated Integrative IR
- Outbreak Detection services (FAZ, FCT, FOS)
- Automated playbooks and remediation
- Fabric Rating Proactive Assessments and Simplified Migration

Application Security
- Secure Email Gateway
- WAF signatures
- DDOS
- CASB – SaaS Security
- ADC

© Fortinet Inc. All Rights Reserved.

Open Ecosystem

500+ Best-in-class integrated solutions for comprehensive protection

Fabric Connectors	Fortinet-developed deep integration automating security operations and policies	aws, aruba (a Hewlett Packard Enterprise company), cisco, Google Cloud, IBM Cloud, Microsoft Azure, ORACLE, servicenow, Symantec.
Fabric APIs	Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions	ARISTA, ASAVIE, DELL, DRAGOS, EQUINIX, intel, SIEMENS (Ingenuity for life), splunk>, TIGERA, tufin
Fabric DevOps	Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration	aws, Google Cloud, HashiCorp, Microsoft Azure, openstack., ORACLE, RED HAT ANSIBLE Automation, refactr, vmware
Extended Ecosystem	Integrations with threat sharing initiatives and other vendor technologies	CYBER THREAT ALLIANCE, MITRE, STIX, INTERPOL, OT CSA, Firewalls, Switching, Wireless, Endpoint Security

Figures as of March 31, 2021
Note: Logos are a representative subset of the Security Fabric Ecosystem

© Fortinet Inc. All Rights Reserved.

Varovanie pred zvýšeným rizikom kybernetických bezpečnostných útokov

21. júna 2022

Národné centrum kybernetickej bezpečnosti SK-CERT **varuje** pred zvýšeným rizikom kybernetických bezpečnostných útokov a to najmä na infraštruktúru **prevádzkovateľov základných služieb a prvkov kritickej infraštruktúry**.

Pokračujúca vojna na Ukrajine je príznačná nie len devastujúcimi fyzickými útokmi Ruska na infraštruktúru a obyvateľstvo Ukrajiny, ale aj **kontinuálnymi kybernetickými útokmi** ako na infraštruktúru Ukrajiny, tak aj na infraštruktúru členských štátov EÚ a NATO. Z dôvodu, že Slovenská republika je členským štátom EÚ a takisto aj NATO, **zvyšuje sa riziko**, že útočníci sa pri svojich aktivitách zamerajú aj na kybernetický priestor Slovenskej republiky. Národné centrum kybernetickej bezpečnosti preto vyhodnocuje **riziko kybernetických bezpečnostných útokov** na infraštruktúru prevádzkovateľov základných služieb a prvkov kritickej infraštruktúry ako **veľmi vysoké**.

V súvislosti so znižovaním tohto rizika je potrebné, aby prevádzkovatelia základných služieb a prvky kritickej infraštruktúry **bezodkladne** vykonali **preventívne bezpečnostné opatrenia**, minimálne v nasledujúcom rozsahu:

https://www.sk-cert.sk/sk/varovanie-pred-zvysenym-rizikom-kybernetickych-bezpecnostnych-utokov/index.html

© Fortinet Inc. All Rights Reserved.

Bezpečnosť prevádzky služieb, systémov a sietí

- zaveďte **zvýšený monitoring sietí a systémov** so zameraním sa na neštandardné a neočakávané aktivity, monitoring vzdialených prístupov do siete a zaťaženia sieťovej prevádzky. **Odporúčame**, aby takýto monitoring fungoval **v režime 24/7**,
- monitorujte a na pravidelnej báze kontrolujte **prístup tretích strán** (dodávateľov, management service providerov) a limitujte takýto prístup len na nevyhnutné minimum,
- **obmedzte vzdialený prístup** do vašej siete a systémov a ak sú takéto prístupy nevyhnutné, monitorujte vzdialené prístupy, obmedzte privilégiá vzdialených používateľov, vynucujte viacfaktorovú autentifikáciu a na vzdialený prístup používajte VPN,
- **nesprístupňujte** priamo na internete **služby vzdialeného prístupu** ako sú RDP, SSH, VNC, telnet a podobne,
- **zakážte** všetky **porty a protokoly**, ktoré nie sú potrebné na prevádzku sietí, systémov a služieb,
- **zmapujte všetky verejné služby** vašej organizácie, vystavených do internetu a následne:
  - **úplné vypnite** nepotrebné a nepoužívané systémy
  - **aktualizujte** zastarané systémy
  - preverte účty a heslové politiky na systémoch, prístupných z internetu,
  - **odstráňte staré účty**

© Fortinet Inc. All Rights Reserved.

- Pripravte sa na hrozbu DDoS útokov na L3/L4 úrovni a takisto aj L7 úrovni (odporúčania nižšie sú zamerané práve na ochranu proti takýmto útokom na L7) a to nasledujúcimi spôsobmi:
  - **využite CDN** (Content Delivery Network) na prevádzku webových služieb
  - majte vytvorené **záložné lokality vašich systémov a služieb**, resp. ich redundanciu,
  - do internetu **publikujte statické webové stránky**, ideálne v externej hostingovej spoločnosti (redakčný systém, inštalovaný vo vnútornej sieti neprístupnej z Internetu vygeneruje HTML súbory, obrázky a štýly, ktoré sú následne prenesené na hostingovú službu)
  - striktne **oddeľte citlivé údaje** a **prevádzkovo kritické aktíva** od verejných webových stránok
  - odporúčame zvážiť používanie **služieb na DDoS ochranu** – existujú dokonca aj služby, ktoré základnú ochranu proti DDoS útokom (špecificky proti L7 vrstve) poskytujú zdarma. Typická DDoS ochrana od ISP spravidla nie je ochranou proti DDoS na L7 vrstvu. Preverte si so svojim poskytovateľom internetu, či vám takúto ochranu zabezpečuje a v akom rozsahu.
  - implementujte bezpečnostnú infraštruktúru, **schopnú filtrovať IP adresy** útočníka vo veľkom objeme
  - **implementujte WAF**
- svoje **e-mailové systémy zabezpečte využitím rôznych bezpečnostných metód** (napríklad SPF a DKIM, antispamové filtre). Nakonfigurujte mailový server tak, aby sa škodlivé a podozrivé maily nedostali do schránok používateľov

© Fortinet Inc. All Rights Reserved.

Riadenie bezpečnosti

- preverte účinnosť vášho **zálohovacieho manažmentu**, aktualizujte vaše zálohovacie procedúry s využitím pravidla 3-2-1,
- preverte a aktualizujte váš **manažment prístupov**, odstráňte všetky staré a nepoužívané kontá, obmedzte prístupy jednotlivých používateľov v zmysle pravidla „need to know“,
- **politiku hesiel** aktualizujte tak, aby zakazovala používať rovnaké heslá na rôzne služby a aby vynucovala používanie silných hesliel alebo heslových fráz. Toto opatrenie je potrebné zaviesť **nie len z procesného, ale aj technického hľadiska**,
- **implementujte a vynucujte viacfaktorovú autentifikáciu**, vrátane e-mailových služieb a VPN služieb. **Odporúčame** vyhnúť sa SMS overovaniu. Používajte také autentifikačné spôsoby, ktoré sú odolné voči sociálnemu inžinierstvu (napr. fyzické tokeny),
- **preverte politiku aktualizácií** softvéru a firmvéru a bezodkladne vykonajte aktualizáciu všetkých systémov a služieb, predovšetkým bezpečnostnými záplatami. Pre zistenie rozsahu zraniteľných systémov vykonajte skenovanie zraniteľností dostupnými nástrojmi,
- pri používaní **cloudových služieb** sa uistite, že **spĺňajú bezpečnostné štandardy** minimálne v rozsahu bezpečnosti vašich vlastných systémov – viacfaktorová autentifikácia, politika prístupov, prístup cez VPN a podobne. Cloudové služby **nie je možné využívať** ako úložisko kritických informačných aktív (napr. obchodné tajomstvá, osobné údaje, plány infraštruktúry, klasifikované informácie a podobne),

© Fortinet Inc. All Rights Reserved.

Riadenie incidentov

- preverte a **aktualizujte procesy riadenia kybernetických bezpečnostných incidentov** a uistite sa, že zamestnanci vedia, koho kontaktovať v prípade podozrenia na incident,
- pri zistení kybernetického bezpečnostného incidentu:
  - **bezodkladne riešte incident**,
  - pri riešení incidentu **zaistite všetky potrebné dôkazy** pre ďalšie účely (napríklad trestné konanie),
  - **nahláste incident** Národnému centru kybernetickej bezpečnosti SK-CERT a komunikujte s SK-CERT pri riešení incidentu,
- **zabezpečte dostupnosť kľúčového personálu** v oblasti prevádzky a riadenia kybernetickej bezpečnosti,
- uistite sa, že vaše **BCM plány a plány obnovy po havárii** sú funkčné. V prípade akéhokoľvek negatívneho nálezu alebo neúspešného testu **aktualizujte tieto plány** tak, aby v praxi bolo možné obnoviť prevádzku v čo najkratšej dobe,

© Fortinet Inc. All Rights Reserved.

Bezpečnosť používateľov

- **Poučte svojich zamestnancov** o rizikách kybernetických bezpečnostných incidentov a informujte ich o zvýšenom riziku útokov. Vzdelávacie aktivity robte adresne, podľa rolí a zodpovedností jednotlivých zamestnancov:ň
  - bežní používatelia – princípy sociálneho inžinierstva a ako sa proti nemu brániť,
  - administrátori – pravidlá bezpečnej infraštruktúry
  - kyberbezpečnostní špecialisti – špecializované bezpečnostné vzdelávanie
- Školenia (podľa role jednotlivých používateľov) **opakujte na pravidelnej báze**,
- **Pravidelne** vykonávajte phishingové testy a cvičenia v oblasti kybernetickej bezpečnosti (blue vs. red team, tabletop)

© Fortinet Inc. All Rights Reserved.

Ďakujeme, nech sa Vám darí!