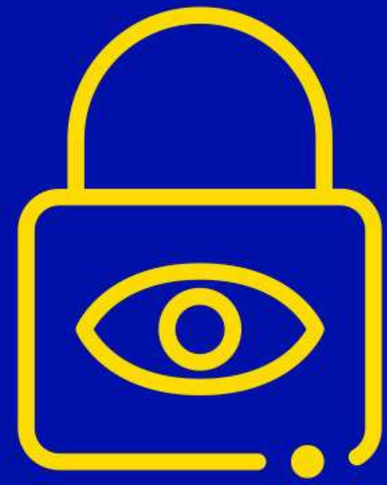
NIS2

Seminář o nové evropské směrnici



Úvod do problematiky NIS2

Radek Šichtanc, O2

NIS2 a nový ZoKB – základní fakta

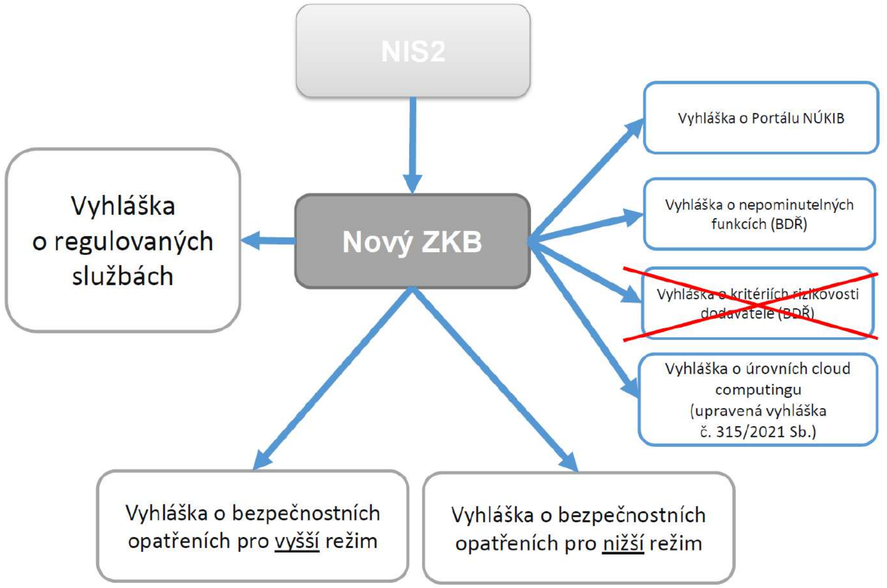
- **Cíl:** zlepšit odolnost veřejných a soukromých subjektů, příslušných orgánů a EU jako celku v oblasti kybernetické bezpečnosti a schopnost reagovat na bezpečnostní incidenty

- Stanovuje **minimální pravidla** týkající se regulačního rámce a mechanismy účinné spolupráce mezi příslušnými orgány v každém členském státě
- Mnohem **širší oblast působnosti** – více společností, ve více odvětvích
- Zpřísňuje a zefektivňuje požadavky na kybernetickou bezpečnost
- Zlepší **sdílení informací** a spolupráci mezi orgány členských států
- Posílení řízení bezpečnosti a **odpovědnosti vedoucích pracovníků** podniku
- Za nedodržení povinností hrozí **vyšší sankce**

- Základ změn pro nový ZoKB

Zákon o kybernetické bezpečnosti

- Nový zákon
- Cca 70 paragrafů
- 6 nových vyhlášek
- Jedna jediná povinná osoba*
- Dva režimy povinností



Poskytovatel regulované služby

Provozovatelé základní služby
Kritická (nejen informační) infrastruktura
Významné informační systémy
Všechny subjekty z NIS2

Regulovaná služba

- naplňující alespoň jedno kritérium pro identifikaci regulované služby podle vyhlášky o regulovaných službách (objektivní naplnění kritérií)
nebo
- určená rozhodnutím NÚKIBu na základě kritéria pro určení regulované služby

** Pro primární sadu povinností spojených s prevencí – zavádění bezpečnostních opatření, hlášení incidentů apod.*

Sebeidentifikace – kritéria

odvětví / činnost

+

velikost subjektu

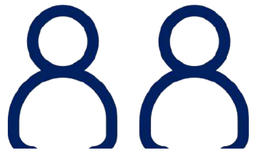
=

vyšší režim

nebo

nižší režim

Sebeidentifikace – velikost

Počet zaměstnanců		Obrat v mil. EUR		
	nebo		=	**velký podnik**
250+		50+		
	nebo		=	**střední podnik**
50+		10+		

Sebeidentifikace – odvětví

Služby uvedené v příloze 1 - Essential

- Energetika
- Zdravotnictví
- Veřejná správa
- Doprava
- Pitná voda
- Digitální infrastruktura
- Bankovnictví
- Odpadní voda
- Vesmír
- Infrastruktura fin. trhů
- Poskytovatelé řízených ICT služeb

Služby uvedené v příloze 2 - Important

- Poštovní služby
- Potravinářství
- Odpadní hospodářství
- Výroba
- Chemický průmysl
- Poskytovatelé digi služeb
- Výzkum

Subjekty, kterým plynou povinnosti z NIS2, ale nespadají do režimu essentail ani important

- Subjekty, shromažďující a udržující přesnou a úplnou registraci názvu domén.

Povinnosti

Hlavní povinnosti

- hlásit kontaktní a další údaje
- **stanovit rozsah** řízení kybernetické bezpečnosti a definovat rozsah regulace v organizaci
- **zavádět bezpečnostní opatření** podle režimu, v kterém je služba určena (vyšší/nižší)
- **hlásit kybernetické bezpečnostní incidenty** podle režimu, v kterém je služba určena (vyšší/nižší)
- **informovat zákazníky** o incidentech a hrozbách
- **provádět protiopatření**
- **plnit povinnosti z tzv. mechanismu bezpečnosti dodavatelského řetězce** u vybraných (strategicky významných) služeb
- **zajistit dostupnost z České republiky** u vybraných (strategicky významných) služeb

Hlášení kybernetických bezpečnostních incidentů

Kybernetickým bezpečnostním incidentem se rozumí narušení bezpečnosti informací v rámci aktiv (související s regulovanou službou).

Hlášení kybernetického bezpečnostního incidentu na NÚKIB

= jen ty, které mají původ v kybernetickém prostoru.

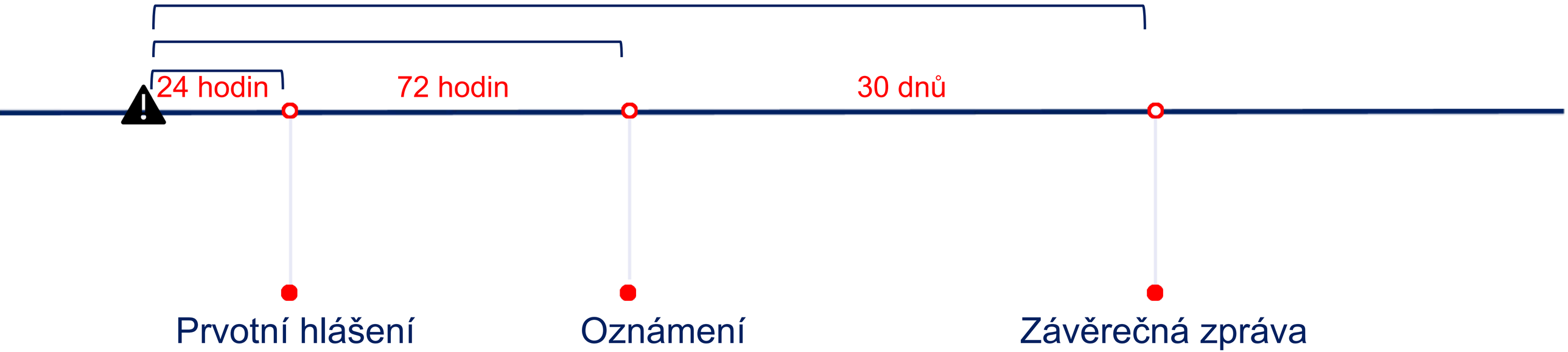
Pro hlášení je třeba posoudit dvě situace:

- **významný dopad na poskytování regulované služby**
- **úmyslné zavinění kybernetického bezpečnostního incidentu**

Hlášení kybernetických bezpečnostních incidentů

Vyšší režim	**hlásí vše**	**NÚKIB** Pozn.: Portál NÚKIB
Nižší režim	**hlásí vše, co je úmyslné,** nebo to, **co je významné**	**Národnímu CERT**

Hlášení kybernetických bezpečnostních incidentů



Sankce – výše pokuty

Subjekt v režimu vyšších povinností

250 mil. CZK

nebo

2 % obratu

Subjekt v režimu nižších povinností

175 mil. CZK

nebo

1,4 % obratu

Lhůty

- Registrovat regulovanou službu – **do 30 dní**
- Hlásit kontaktní a další údaje – **do 30 dní** (15 dní změny)
- Stanovit rozsah řízení kybernetické bezpečnosti – **kdykoliv** (nebo celá organizace)
- Zavádět bezpečnostní opatření – **do 1 roku** (od evidence)
- Hlášení kybernetických bezpečnostních incidentů – **do 1 roku** (od evidence)
- Protiopatření (výstraha, varování, reaktivní opatření) – **ihned**
- Informační povinnost poskytovatele regulované služby – **ihned**

Řízení dodavatelů

Nová oblast, nevyplývá ze směrnice NIS2, ale z **národního rozhodnutí**

- platí **pouze pro vybrané organizace v režimu vyšších povinností** (a to nikoli všech)
- organizace v rámci této povinnosti **musí nahlásit dodavatele**
- budou prověřováni **dodavatelé do kritické části systému**, kteří dodávají bezpečnostně významnou dodávku
- stát prověří to, zda dodavatel není hrozbou pro bezpečnost ČR, zájmy ČR, vnitřní a veřejnou bezpečnost
- NÚKIB může vydat **zákaz dodavatele** použít nebo **upozornění na riziko** (opatření)
- **lze udělit výjimku** (např. pokud to nikdo jiný nevyrábí, ohrozilo by to službu atp.)
- k vyřazení již dodaných technologií nemusí dojít hned, počítá se s přechodnými lhůtami
- hlášení dodavatelů do 1 roku od určení poskytovatele regulované služby

Účinné **do 1 roku** od vyrozumění od označení služby jako **strategické**.

Časová osa nové regulace

Shrnutí

- Sebeidentifikace
  - Odvětví
  - Velikost firmy
  - Nižší a vyšší režim povinností
- Registrace u NÚKIB
- Primární a podpůrná aktiva
- GAP analýza
- Plán nápravy
- Implementace
- Průběžné zlepšování

Jak se připravit na NIS2

Tomáš Svoboda, O2 ITS

Organizační opatření

Role a odpovědnosti vrcholového vedení

Prokazatelná účast na školení

Schvalování bezpečnostních politik

Zajištění dostupnosti zdrojů – interně nebo formou outsourcingu

Jmenování bezpečnostních rolí

Určení výboru pro řízení IKB a účast na jednáních

Minimálně 1x ročně schvalování:

- Výsledků hodnocení rizik
- Auditních zpráv
- Analýzy dopadů – BIA

Bezpečnostní politiky a jejich role v zajištění bezpečnosti

Politika zajišťování minimální úrovně kybernetické bezpečnosti

- Rozsah, SLA

Bezpečnost lidských zdrojů

- Školení, sankce za porušení povinností

Řízení aktiv a rizik

- Identifikace aktiv, odpovědné osoby, přípustné použití aktiv

Řízení dodavatelů

- Pravidla identifikace významného dodavatele, bezpečnostní požadavky do smluv s dodavateli

Bezpečnostní role

Nižší režim:

- Máte to jednodušší ☺
- Osoba odpovědná za kybernetickou bezpečnost

Vyšší režim:

- Manažer kybernetické bezpečnosti,
- Architekt kybernetické bezpečnosti
- Garant aktiva – primární i podpůrná aktiva
- Auditor kybernetické bezpečnosti.

Zastupitelnost bezpečnostních rolí

Bezpečnostní role nesmí odpovídat za provoz

Řízení aktiv

Je nezbytné vědět, jaká aktiva jsou pro společnost klíčová

- Primární – informace nebo klíčová služba, která je poskytována
- Podpůrná – HW, SW, lidské zdroje, dodavatelé, lokality
- Jak identifikovat aktiva?
- Jak identifikovat garanty aktiv?
- Klíčový vstup do řízení rizik
- **Aktiva nejsou pouze CMDB položky IT infrastruktury!**
- K čemu je to dobré? ☺

Řízení rizik

Je nezbytné vědět, jaká rizika mají vliv na zajištění regulované služby

- Hrozby, zranitelnosti
- Proces řízení rizik – minimálně 1x ročně
- Odpovědnost v procesu řízení rizik
- Bezpečnostní role, vedení
- Analýza rizik aneb hrozby, zranitelnosti a kde je najít? ☺
- Vyhodnocení rizik – prioritizace a kritéria pro řešení
- Zvládání rizik
- Akceptace, přenesení, sdílení, vyhnutí se riziku a jejich význam pro organizaci

Řízení dodavatelů

Nižší režim

- Propsání požadavků do smluv s dodavateli
- CIA, audit, řetězení, řízení změn, NDA, exit strategie, BCM, sankce

Vyšší režim

- Identifikace, informování a evidence dodavatelů
- Pravidelný audit – interní i třetí stranou
- Hodnocení rizik před uzavřením smlouvy
- Požadavky KB ve smlouvách s dodavateli, pravidla chování dodavatele
- Bezpečnostní politiky, incidenty, aktiva, rizika, likvidace dat, odstoupení od smlouvy, předání dat do jiného státu.

Školení

Plán rozvoje bezpečnostního povědomí = periodický plán školení

Prokazatelné:

- Školení vrcholového vedení
- Školení zaměstnanců
- Školení dodavatelů

Vyšší režim

- Školení bezpečnostních rolí
- Co školit – doporučená školení v příloze č. 8
- Sociální inženýrství, VPN, elektronická komunikace, cloudová úložiště, aktuální hrozby, detekce zranitelností, používání zařízení pro soukromé účely

Řízení kontinuity

Kontinuita činností není pouze zálohování a disaster recovery

Kontinuita činností = procesy a činnosti organizace, nejen IT systémů

Nižší režim

- Vazba na primární aktiva – pořadí obnovy primárních aktiv
- Odpovědnosti, pravomoci
- Zálohování

Vyšší režim

- Metodika pro stanovení analýzy dopadů
- Vstup do hodnocení rizik
- Stanovení minimální úrovně poskytovaných služeb
- BC plán per služba
- Testování plánů kontinuity činností

Příklad: Pandemie COVID 19 a vliv na lidské zdroje

Řízení incidentů

Nižší režim

- Jak posuzovat incidenty? Metodický postup – vazba na řízení kontinuity činností
- Hlášení incidentů s významným dopadem
- Závěrečná zpráva o kybernetickém incidentu

Vyšší režim

- Odpovědnosti při detekci a řešení incidentů – IT, vedení, bezpečnostní role
- Hlášení **VŠECH** kyber. bezp. incidentů podle zákona
- Zajištění důkazních materiálů
- Aktualizace analýzy rizik, BCP
- **Prvotní hlášení do 24 hodin**

Řízení změn

Nižší režim

- Řízení změn u dodavatelů

Vyšší režim

- Změny mající vliv na kybernetickou bezpečnost
- Politika řízení změn
- Významné změny – co to je????
  - Dokumentace, role, odpovědnosti
  - Hodnocení rizik, analýza rizik, penetrační testování
  - Testování
  - Navrácení do původního stavu

Technická opatření

Řízení přístupu a identit

Nižší režim

- Každý uživatel jedinečný identifikátor
- Nezapomenout na technické účty!
- Pravidelné přezkoumávání
- Vícefaktorová autentizace jako cíl
- Klíče, certifikáty, hesla
- Jak řídit obálkové účty?

Vyšší režim

- **Centralizovaný nástroj** pro řízení oprávnění
- Evidence aktiv, kde není nasazena vícefaktorová autentizace
- Výchozí hesla generována náhodně

Jak uchopit procesy?

Bezpečnost komunikací

Nižší režim

- **Zejména** oddělení provozního a zálohovacího prostředí
- Evidence povolených komunikací
- Bezpečné síťové protokoly – NÚKIB

Vyšší režim

- Oddělení provozního, zálohovacího, vývojového, testovacího a jiného specifického prostředí
- Vzdálené přístupy a vzdálená správa aktiv
- Kryptografie
- Evidence povolených komunikací
- Firewally, NGFW, aplikační firewally

Aplikační bezpečnost

Nižší režim

- Patch management
- Evidence nepodporovaných systémů, omezení jejich komunikace, náhradní bezpečnostní opatření – best practice?
- Skenování zranitelností relevantních aktiv – vychází z řízení aktiv analýzy rizik

Vyšší režim

- Pravidelné skenování zranitelností 1x ročně a penetrační testy 1x za 2 roky (interní a externí síť)
- Výsledky jako vstup do řízení rizik
- Penetrační testy před uvedením do provozu a při významných změnách
- Retesty
- Penetrační testy celku max. do 5 let

Aplikační bezpečnost

Nižší režim

- Patch management
- Evidence nepodporovaných systémů, omezení jejich komunikace, náhradní bezpečnostní opatření – best practice?
- Skenování zranitelností relevantních aktiv – vychází z řízení aktiv analýzy rizik

Vyšší režim

- Pravidelné skenování zranitelností 1x ročně a penetrační testy 1x za 2 roky (interní a externí síť)
- Výsledky jako vstup do řízení rizik
- Penetrační testy před uvedením do provozu a při významných změnách
- Retesty
- Penetrační testy celku max. do 5 let

Logování a vyhodnocování událostí

Nižší režim

- Ochrana před škodlivým kódem – antiviry, EDR včetně jejich aktualizace – vazba na aplikační bezpečnost
- Kontrola dat na perimetru – FW, NGFW
- Včasné varování osob o incidentu

Vyšší režim

- **Centrální nástroj** pro detekci **–** best practice – log management, SIEM, SOAR
- Časová synchronizace
- **Překlad adres – NAT!**
- Uchování logů nejméně 18 měsíců. Forenzní úložiště?
- Vyhodnocování událostí jako vstup do analýzy rizik a plánu zvládání rizik

Kryptografie

Nižší režim

- Odolné algoritmy a kde je najít?
- Použití tam, kde je to vhodné.
- Hodnocení aktiv a rizik

Vyšší režim

- Kryptografické klíče a certifikáty
- Systém správy klíčů – certifikační autority
- Best practice – procesy generování, změny a zneplatnění klíčů – kompletní dokumentace PKI procesů a infrastruktury

Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

Nižší režim

- Stanovit únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem představující úhrn nejvyšší škody a nemajetkové újmy vzniklé v souvislosti s kybernetickým bezpečnostním incidentem, v jehož důsledku ještě nejsou ohroženy život či zdraví osob ani schopnost poskytovatele regulované služby dostát svým závazkům
- Hodnocení dopadů – využít metodiku NÚKIB – metodika k vodítkům pro hodnocení dopadů
- BCM

Vyšší režim

- Hlásí se všechny incidenty s původem v kyberprostoru

Dostupnost regulované služby

Nižší režim

- Není specifikováno

Vyšší režim

- Zajištění dostupnosti služby podle cílů v BCM
- Redundance aktiv
- Zálohování
  - Testy integrity dostupnosti a obnovitelnosti záloh a dokumentace těchto testů – téměř nikdo dnes neprovádí
  - Šifrování záloh
  - Table-top cvičení jsou nedostatečná

Průmyslová, řídící a jiná specifická aktiva

Nižší režim

- Není specifikováno

Vyšší režim

- Standardní opatření
  - Segmentace sítě
  - Řízení přístupu
  - Omezení vzdálených přístupů
  - Ochrana před zranitelnostmi
  - Fyzická bezpečnost
- **Častý problém – nepodporovaná nebo proprietární zařízení**
  - Evidence zařízení, analýza rizik, ekonomicko-bezpečnostní posouzení

Ukázky a příklady implementace NIS2

Ivo Kubíček, O2

O2 partner pro kyberbezpečnost

Patříme ke špičkám

2021 ESET přes ½ mld, O2 necelou 1/3 mld

Produkty

přímo pro kybez

NGFW, antiDDoS, SOC, MDM, zákaznická řešení

podporující kybez

O2 Hosting/ O2 Cloud v TIII datových centrech, O365, ...

Reference

z B2B, B2C, B2G i B2E

Auto reference

vyhovění ZoKB, ISO 27x, ...

přenos zkušeností do B2x řešení

Snadná cesta NIS2

Při řízení kontinuity činností si organizace stanoví minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby.

Principem zavádění bezpečnostních opatření v ICT je:
zmapovat si své prostředí
identifikovat, co vše je třeba pro zajištění chodu regulované služby
vyhodnocovat rizika, která mohou ohrozit kontinuitu služby
- zavádět přiměřená opatření, která daná rizika sníží na akceptovatelnou úroveň

„Poznat závislost stroje na peníze (regulované služby) na ICT a zavedením přiměřených opatření snížit rizika porušení BC na akceptovatelnou úroveň.“

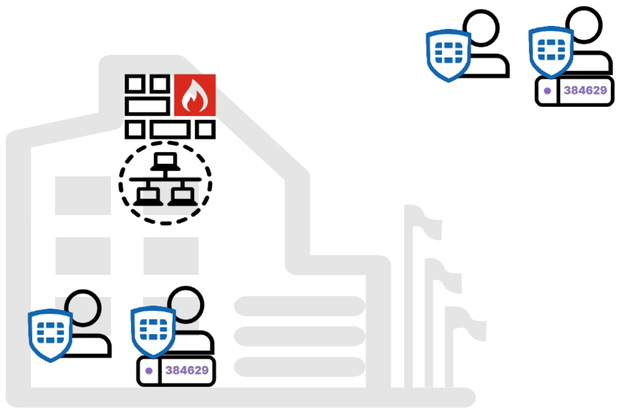
Příklady z praxe

Stuxnet v českých garážích neuspěje
segmentace, ZTNA, …

Peníze ušetřené za AI jsme vrazili do lidí
školicí platforma, MFA, …

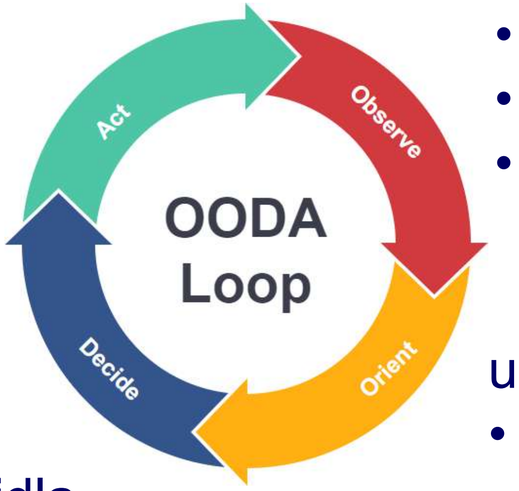
Kontext udělal z DDoSu průmyslovou špionáž
centralizovaný sběr logů s možností analýzy

Model ZTNA (nulové důvěry) s O2 řešením



pravidla se otiskují do provozu
- LAN
- perimetru
- off-net

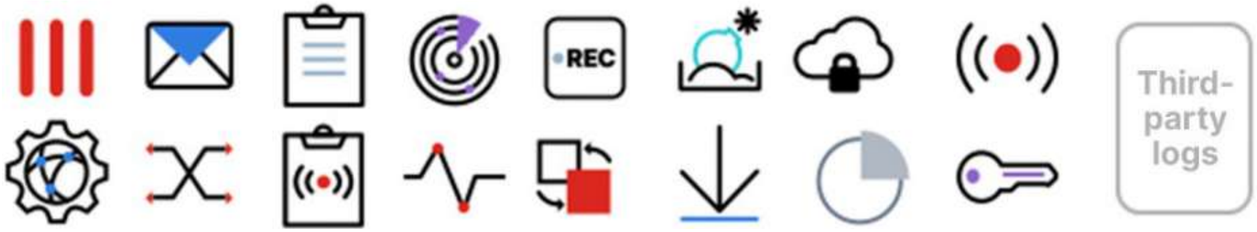
na základě poznání vznikají pravidla



uniCPE vidí
- do vnitřní sítě
- na perimetr
- klienty on-net i off-net

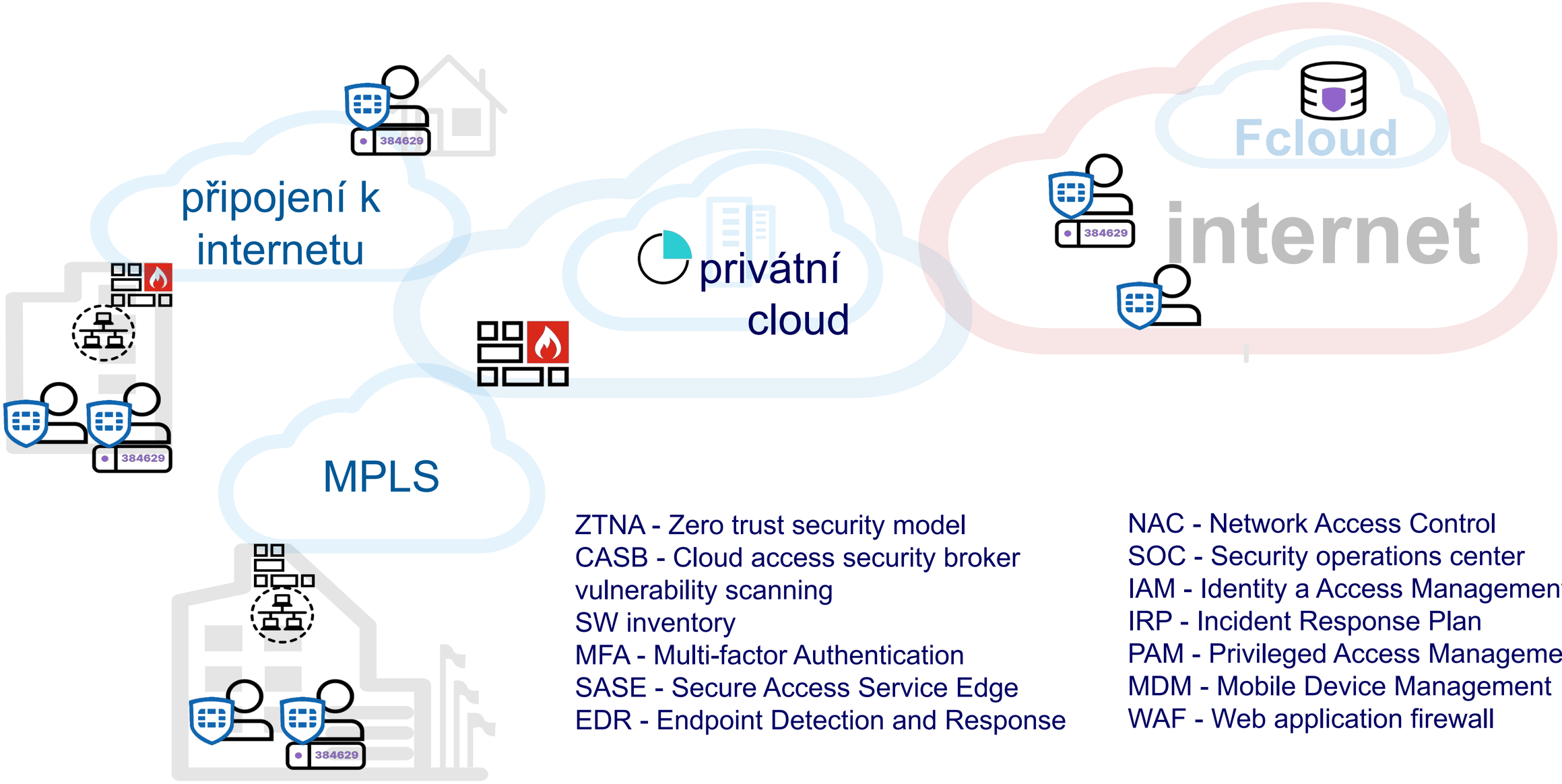
uniCPE a klienti dávají logy
- kam / kdy / kdo přistupuje

informace z platformy
datový provoz, události, DNS, bezpečnostní alerty, ...



sběr a uložení logů
analytika
automatizace

Nasazení s mnoha funkcemi a jednoduchou správou



ZTNA - Zero trust security model
CASB - Cloud access security broker
vulnerability scanning
SW inventory
MFA - Multi-factor Authentication
SASE - Secure Access Service Edge
EDR - Endpoint Detection and Response

NAC - Network Access Control
SOC - Security operations center
IAM - Identity a Access Management
IRP - Incident Response Plan
PAM - Privileged Access Management
MDM - Mobile Device Management
WAF - Web application firewall

Fortinet produkty zasazené do NIS2

Společnost Fortinet v číslech

Founded: **October 2000**

Founded by: **Ken Xie and Michael Xie**

Headquarters: **Sunnyvale, CA**

Fortinet IPO (FTNT): **November 2009**

Listed in both: **NASDAQ 100 and S&P 500**

Member of: **2022 Dow Jones Sustainability World and North America Indices**

Security Investment Grade Rating: **BBB+ Baa1**

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our security solutions are among the most deployed, most patented, and most validated in the industry.

Global Customer Base

705k+

Customers

Broad, Integrated Portfolio of

50+

Enterprise Cybersecurity Products

2022 Billings

$5.59B+

(as of Dec 31, 2022)

Strong Analyst Validation

70+

Enterprise Analyst Report Inclusions

Market Capitalization

$45.5B

(as of Sept 30, 2022)

Vertical Integration

$1B+

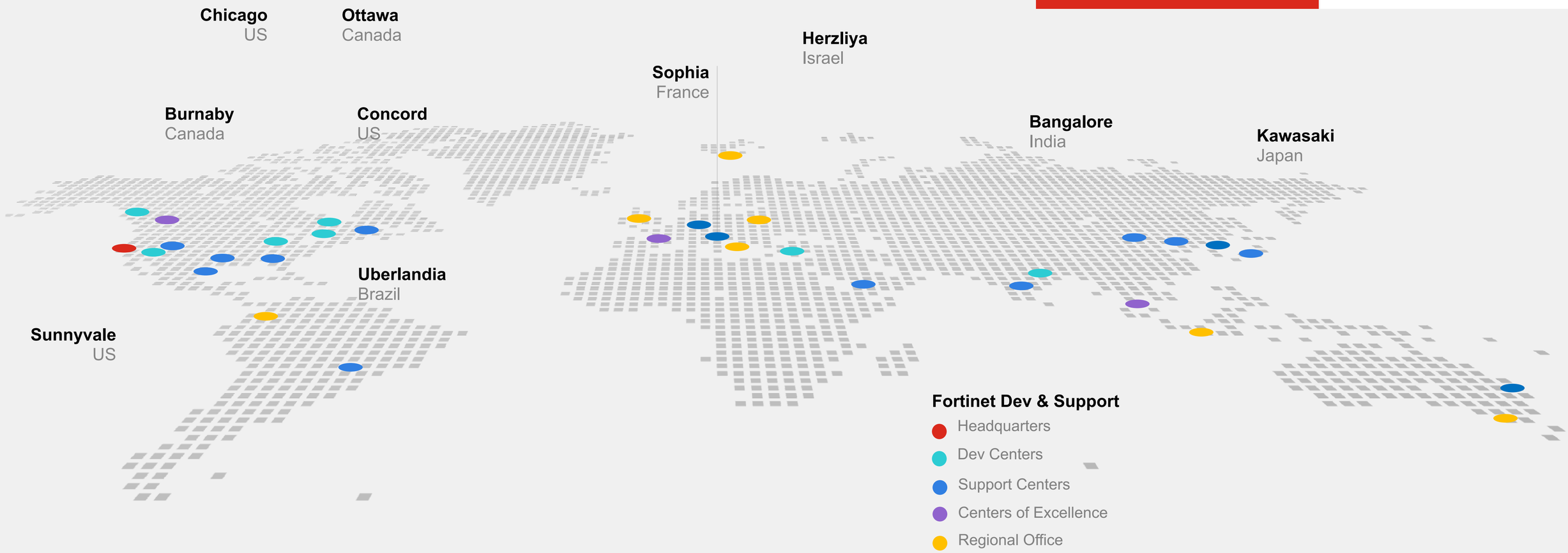
Investment in ASIC Design & Development

Fortinet – světová jednička na poli bezpečnosti

Majority of our R&D is based in North America

13,600+
Employees Worldwide

100+
Global Cloud Locations



FortiGuard Threat Research Lab (AI-Powered)

Broad Coverage
Telemetry across millions of Fortinet endpoints, networks and applications

Early Detection & Response

Broad Protection
across millions of Fortinet endpoints, networks and applications

6M
Firewalls

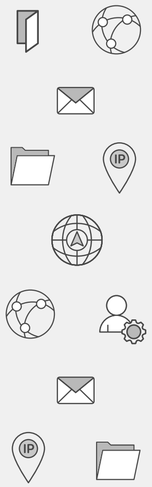
3M
Web Gateways

20M
Emails

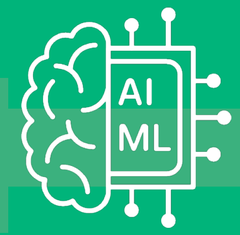
10M
Endpoints

5M
Sandbox

Unknown Query



FortiGuard Labs



AI / Machine Learning

Billions
of Updates Daily

Verdict

Network Security

Web

Emails

Endpoints

Sandbox

1K+
FortiGuard Labs Global Threat Hunters and Researchers

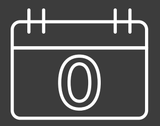
1K+
Threat Intelligence Sources

Pohled na aktuální hrozby (komplexnější než kdy předtím)

SPEAR PHISHING & DEEP FAKES

More targeted, more automated, and more channels

N DAY VULNERABILITIES



24% Growth in Published CVEs in 2022 over 2021

CYBER-PHYSICAL ATTACKS

Removal of Air Gaps is exposing OT

APT THREAT ACTORS

30% of APT groups were detected as active in just the 1H 2023

RANSOMWARE & WIPERS

Ransomware infections times falls from 5 days to 5 hours

CLOUD RISKS

69% of companies use two or more clouds

SUPPLY CHAIN ATTACKS

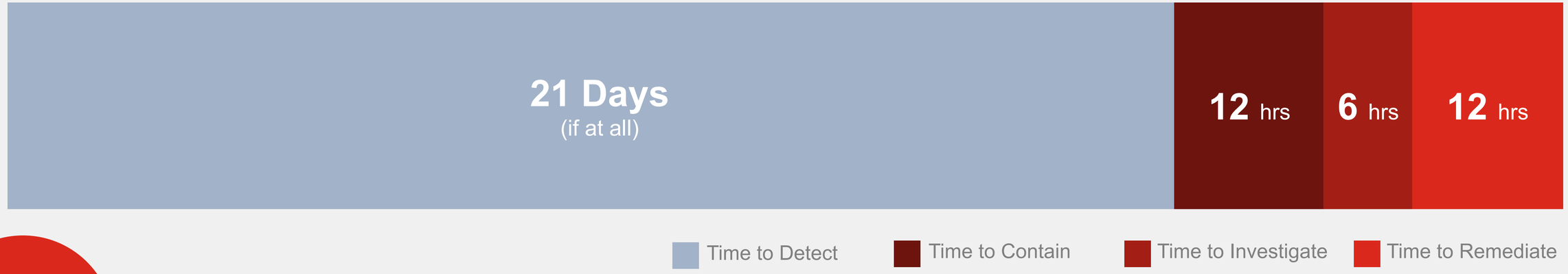
12% of data breaches originated from a software supply chain attack

INSIDER RISK

+32% Year on Year Increase in Insider Risk Incidents

Jak dlouho trvá detekce (a odstranění) útočníka v síti

Average time from detection to remediation



52%

of organizations report SecOps are harder than 2 years ago, cite threats, attack surface, volume/complexity[1]

New SEC Rule

4 Days

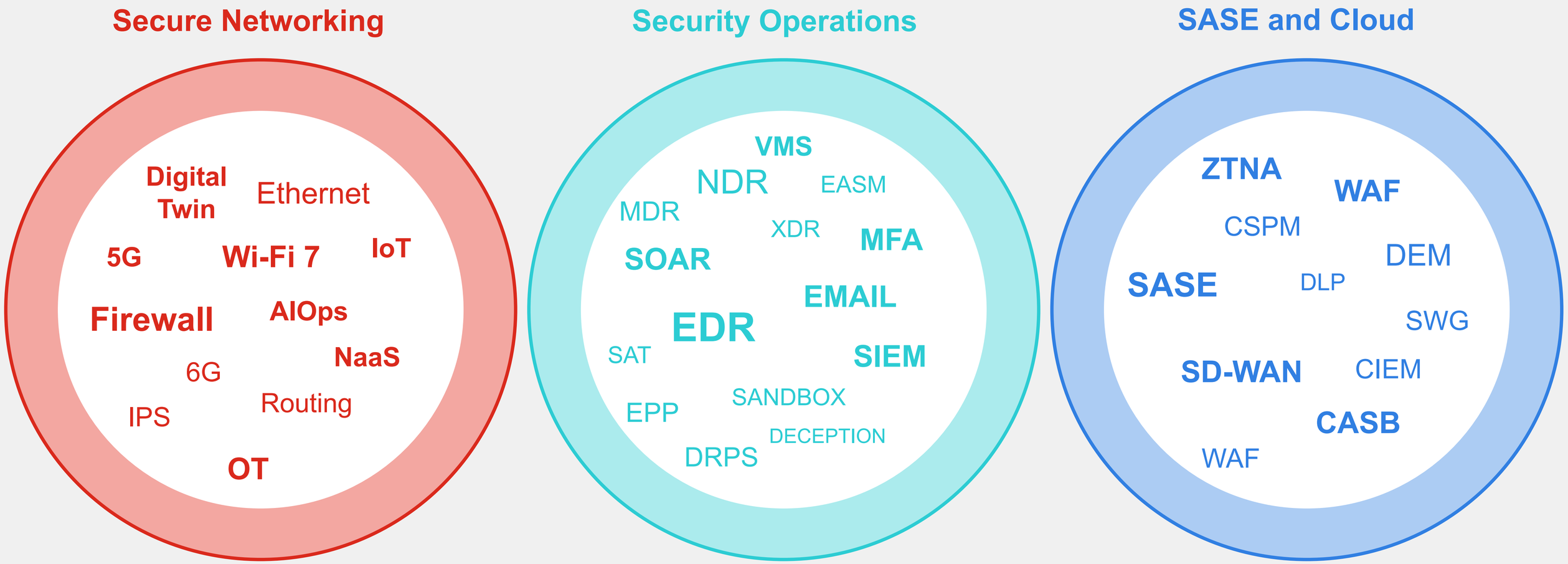
to disclose material cybersecurity incident

$9.4M

Avg Breach Cost

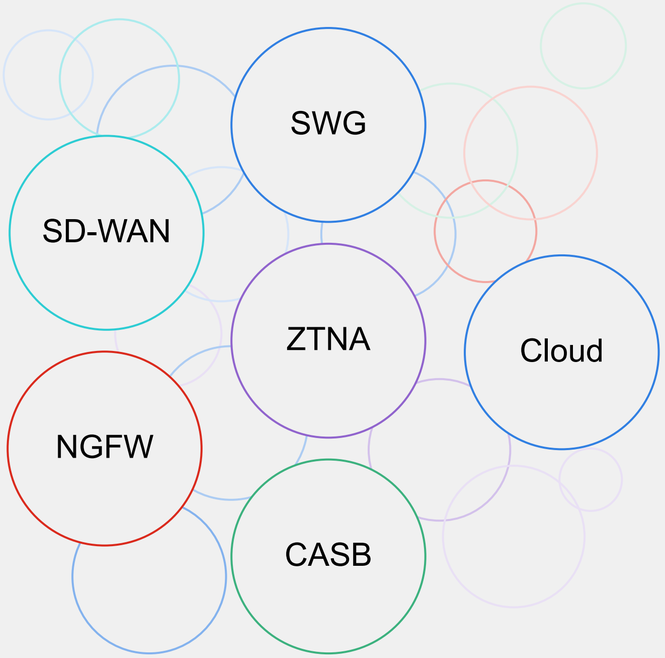
Source: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, October 2022.

„Řešení“



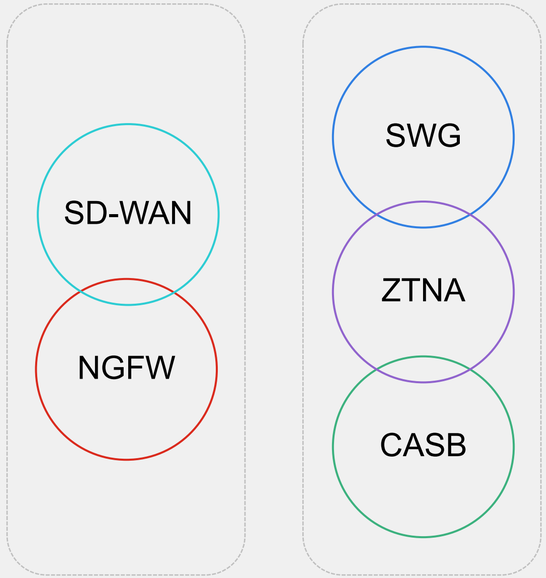
Opravdové řešení směřuje k „SASE“

Point Product Vendors



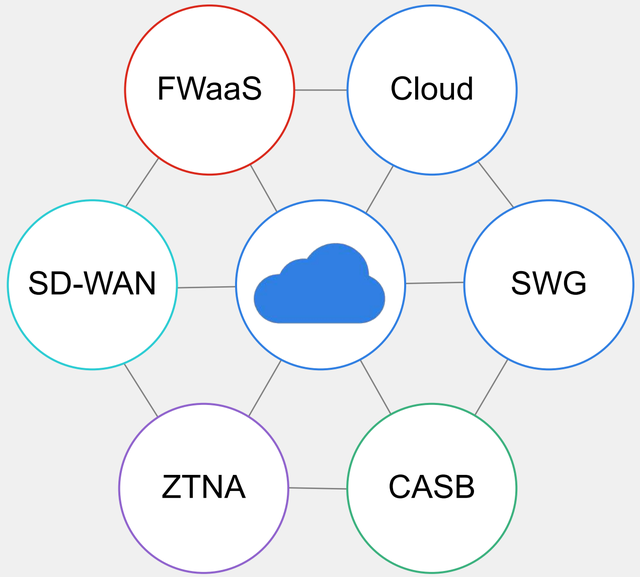
50 Vendors

Dual-Vendor SASE



20 Vendors

Universal SASE



FORTINET

Fortinet Security Fabric

Secure Networking

CONVERGE

Security and networking convergence across all edges, users, and devices

Security Operations

CONSOLIDATE

Consolidated security operations platform to accelerate time to detect and respond

Universal SASE

CONSUME

Flexible consumption of security services to secure access & protect networks, applications & data on any cloud

- AI-Driven Technologies
- FortiCloud
- FortiPoints
- FortiGuard Labs
- OT-Compliant
- Ecosystem

Rev 1.0

AIOps

Threat Intelligence

Ecosystem

Secure Networking

Digital Experience

Secure LAN	Firewall
Secure WLAN	SD-WAN
5G	SASE
SWG	ZTNA
Cloud Networking	NAC

Cybersecurity Platform

Digital Risk

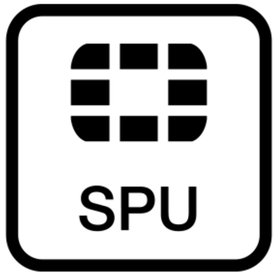
SIEM	SOAR
Analytics	Threat Intelligence
EDR/XDR	Identity
Email	WAF
Cloud Security	NDR

OT Aware Security

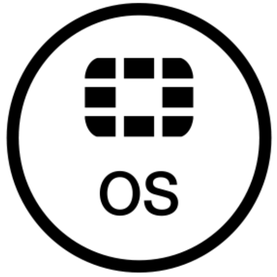
Cyber-Physical Risk

Rugged AP	NAC/PAM
Rugged FW	OT Services
Industrial Switch	OT SIEM/SOAR
SD-WAN/5G	OT EDR

Hlavní výhody společnosti Fortinet



Security Processors



FortiOS

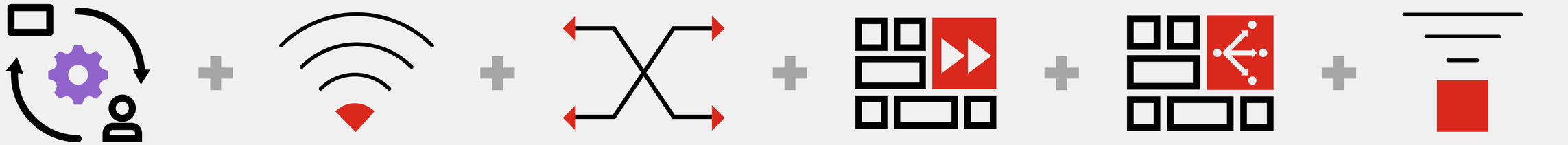
Security Fabric

FortiGuard

Jedno zařízení pro všechno

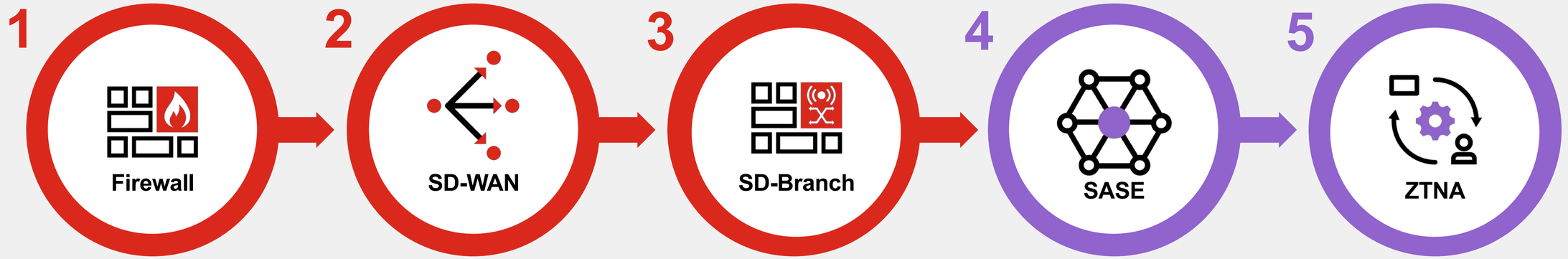
FortiGate jako první uCPE poskytuje:

- SD-WAN
- NGFW
- LAN/WLAN
- ZTNA



Only Vendor Integrates & Manages All Functions with a **Single** Management

Simplify Architecture and Management	Accelerate Troubleshooting	Enhance Operations and Lower TCO	Accelerate Transition to Zero Trust Edge & SD-Branch



Control points across the infrastructure

Optimize application experience

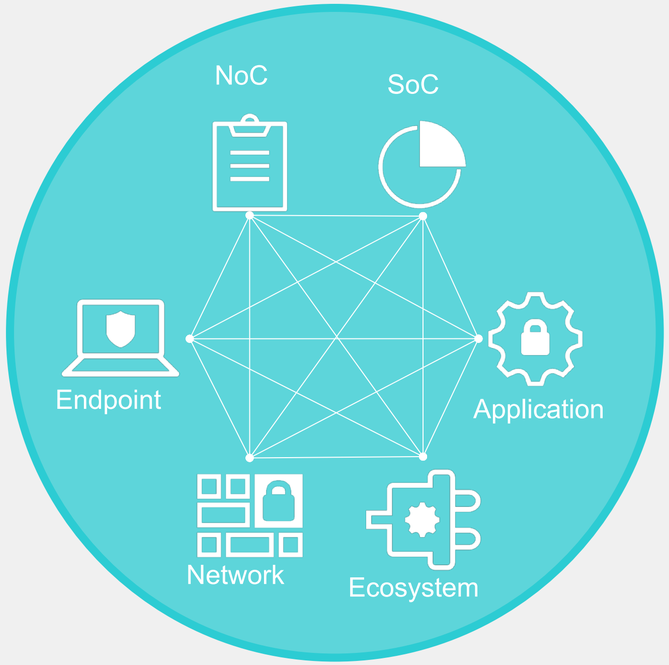
Secure your premise

Secure remote users

Apply zero trust to all applications

97% of organizations plan to have an active vendor consolidation strategy within the next three years.

Consolidate point products and vendors into a cybersecurity platform



Primary Reasons Organizations are Pursuing Security Vendor Consolidation:

55%
Increase efficacy by integrating multiple components

55%
Increase effectiveness by allowing broader reach and visibility

43%
Easier management by reducing the number of separate tools

35%
Cost/budgeting/to save money

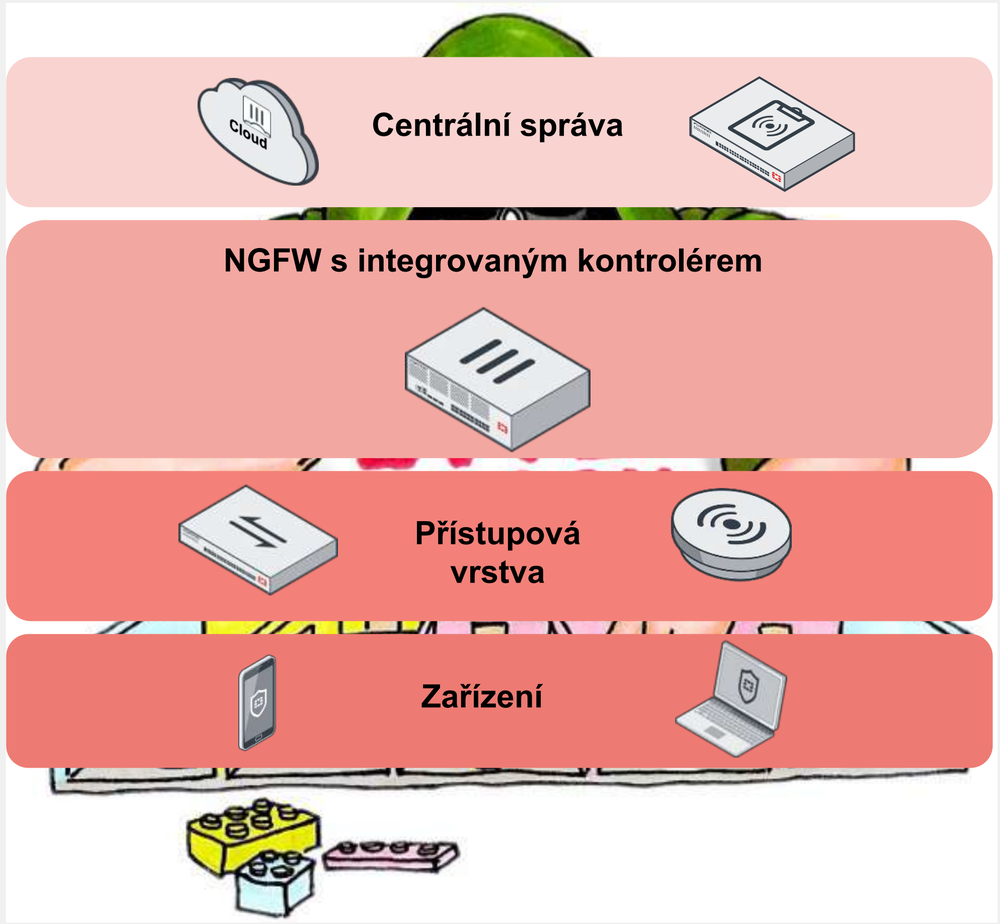
Gartner

Gartner, Accelerate SASE Adoption by Leveraging the Security Vendor Consolidation Wave, Published 5 May 2023 - ID G00785334 - By Analyst(s): Evan Zeng, Naresh Singh

1. Rozděl a panuj

FortiGate, FortiSwitch, FortiAP

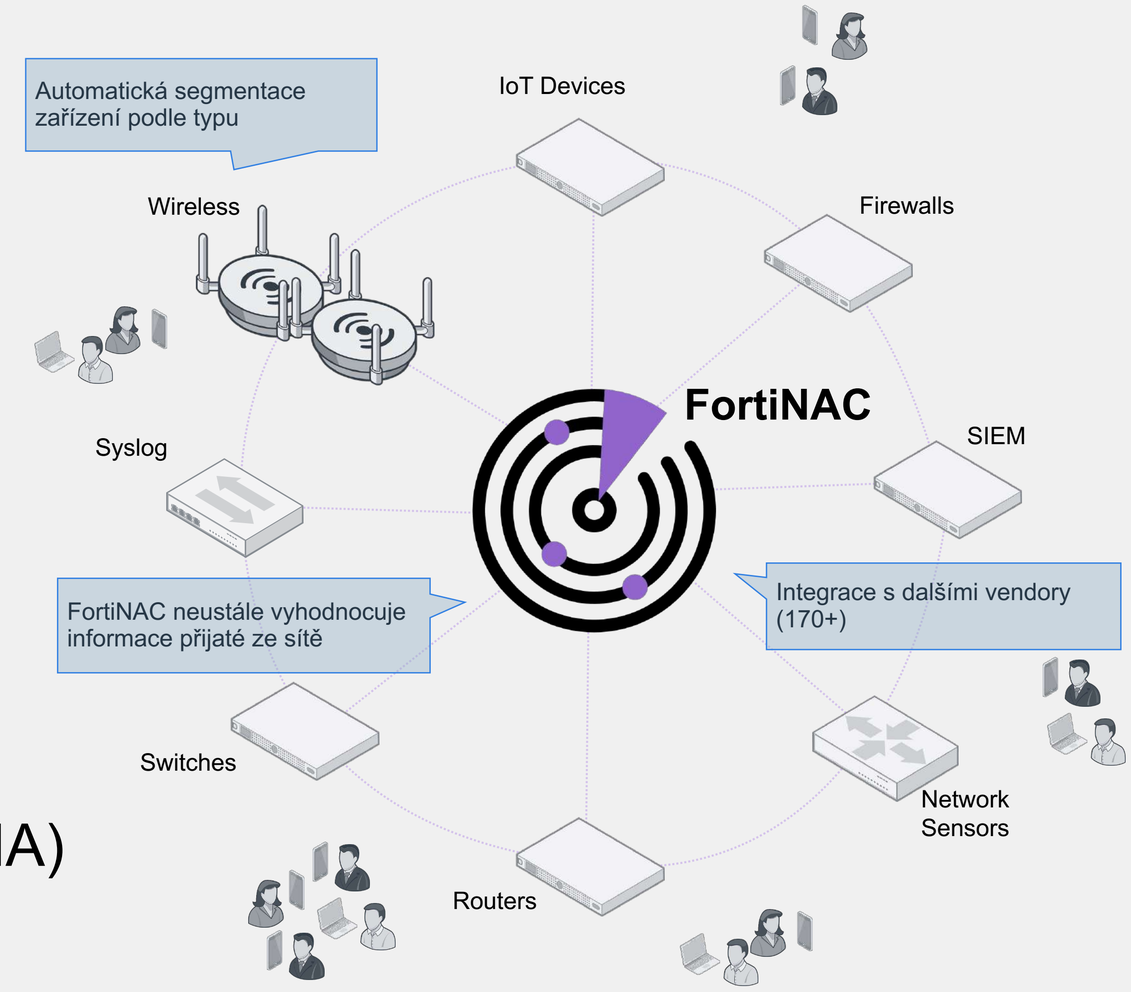
- Segmentace sítě
- NGFW politika (IPS, AppCtrl, WebFilter, AntiMalware)
  - Pro provoz z/do vnitřní sítě
  - Ale také uvnitř sítě
- SSL inspekce
- Řízení přístupu k LAN/WiFi
- Síť pro hosty
- Zabezpečený vzdálený přístup (VPN -> ZTNA)
- Konsolidace bezpečnostních prvků



2. Rozděl a panuj

FortiGate, FortiSwitch, FortiAP, FortiNAC

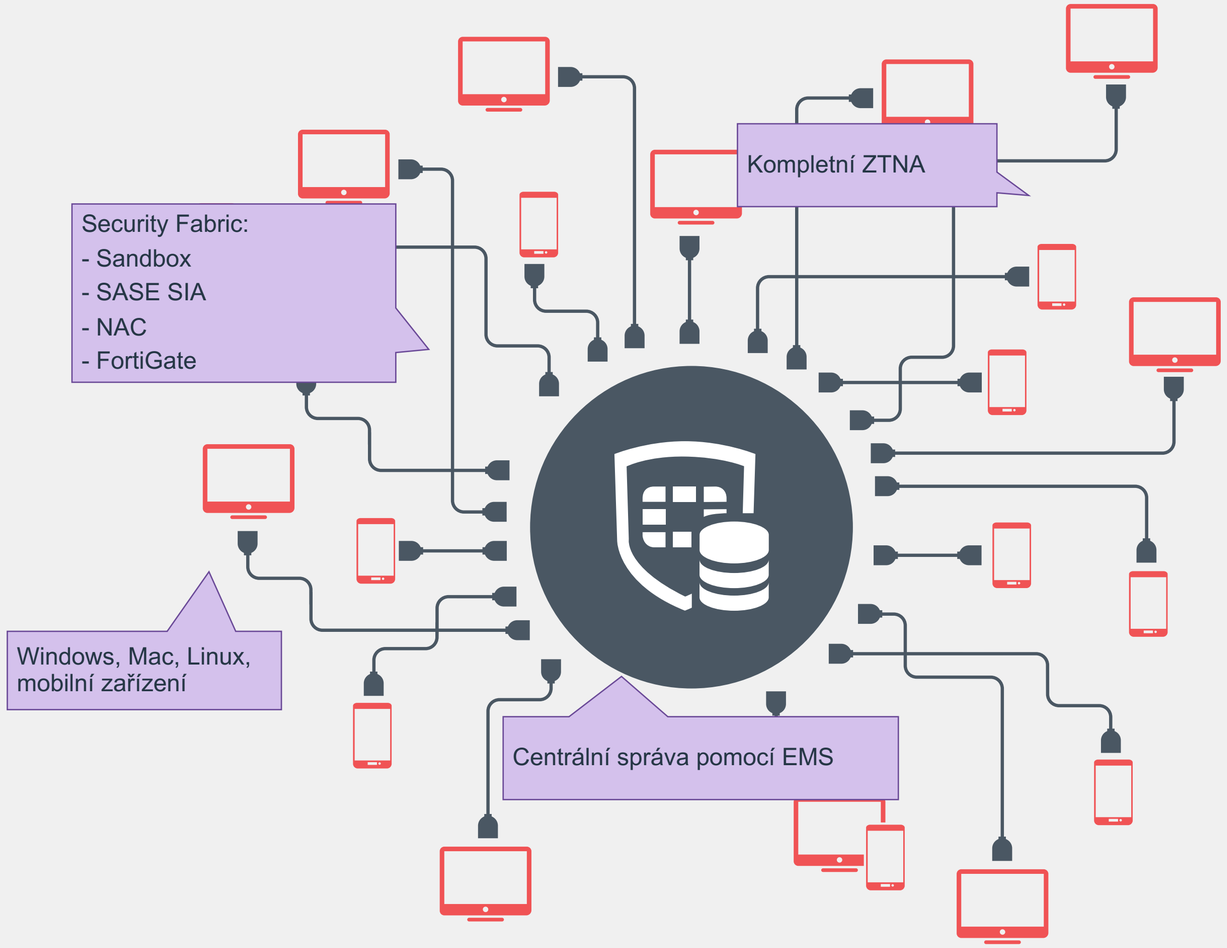
- Segmentace sítě
- NGFW politika (IPS, AppCtrl, WebFilter, AntiMalware)
  - Pro provoz z/do vnitřní sítě
  - Ale také uvnitř sítě
- SSL inspekce
- Řízení přístupu k LAN/WiFi
- Síť pro hosty
- Zabezpečený vzdálený přístup (VPN -> ZTNA)
- Konsolidace bezpečnostních prvků



3. Zabezpečení pracovní stanice

FortiClient EMS (EPP)

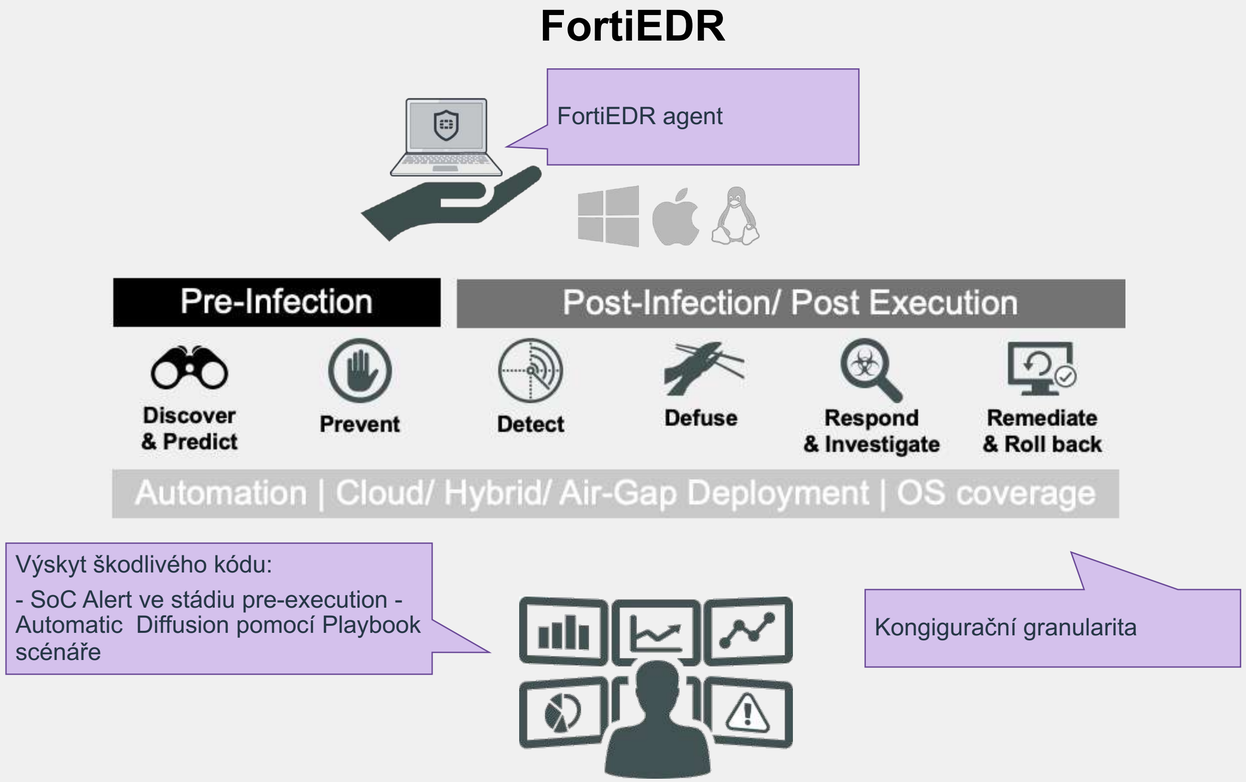
- Konvenční bezpečnostní nástroje
  - AntiVirus/AntiMalware, AntiExploit, napojení na FortiSandbox, WebFilter
- Telemetrické informace z pracovní stanice
  - Stav zařízení, seznam instalovaných aplikací
  - Autopatching zranitelností
  - Monitoring zranitelností (vulnerability)
  - Automatická karanténa
- Vzdálený přístup (VPN -> ZTNA)
- SASE klient
- Identita uživatele (SSO)



4. Pokročilé zabezpečení pracovní stanice

FortiEDR

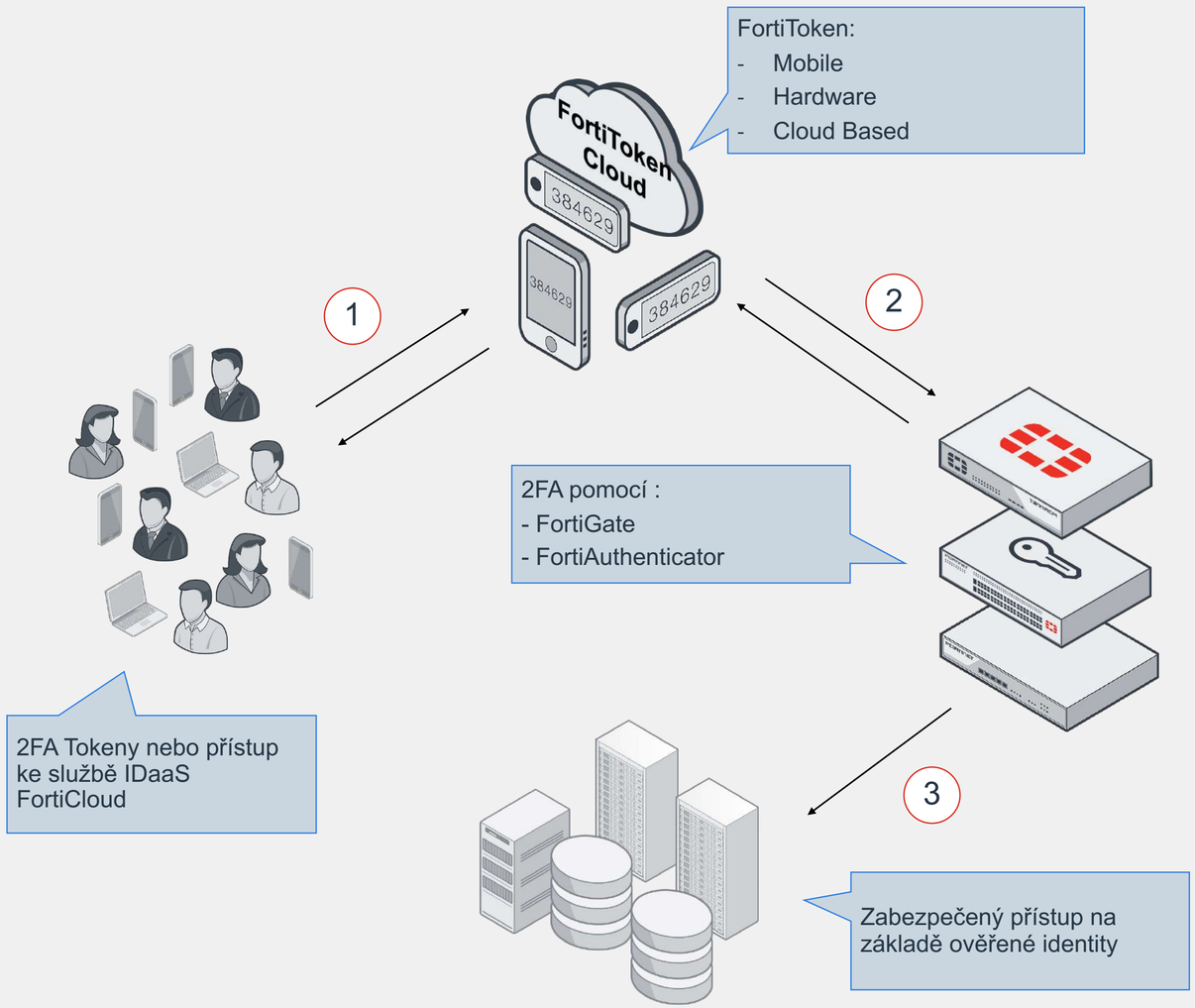
- Nevyužívá statické signatury
- Není založen na reaktivním principu
- Pracuje s ML a proprietárními algoritmy
- Cílem je: „detect & defuse“

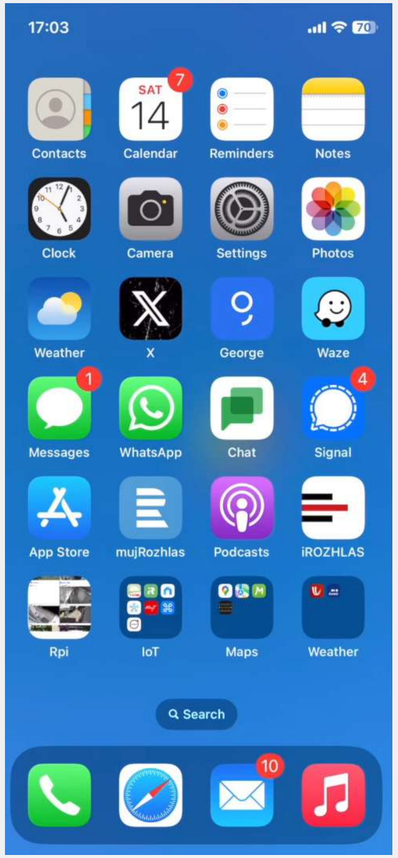


5. Identita uživatele

FortiToken, FortiToken Mobile, FortiAuthenticator

- Multi Factor Authentication
- Několik variant
  - HW přívěsek
  - Aplikace do mobilního telefonu
  - Cloud řešení (IDaaS)
- Push notifikace
- Podpora Apple Watch
- Nativní integrace s FSF

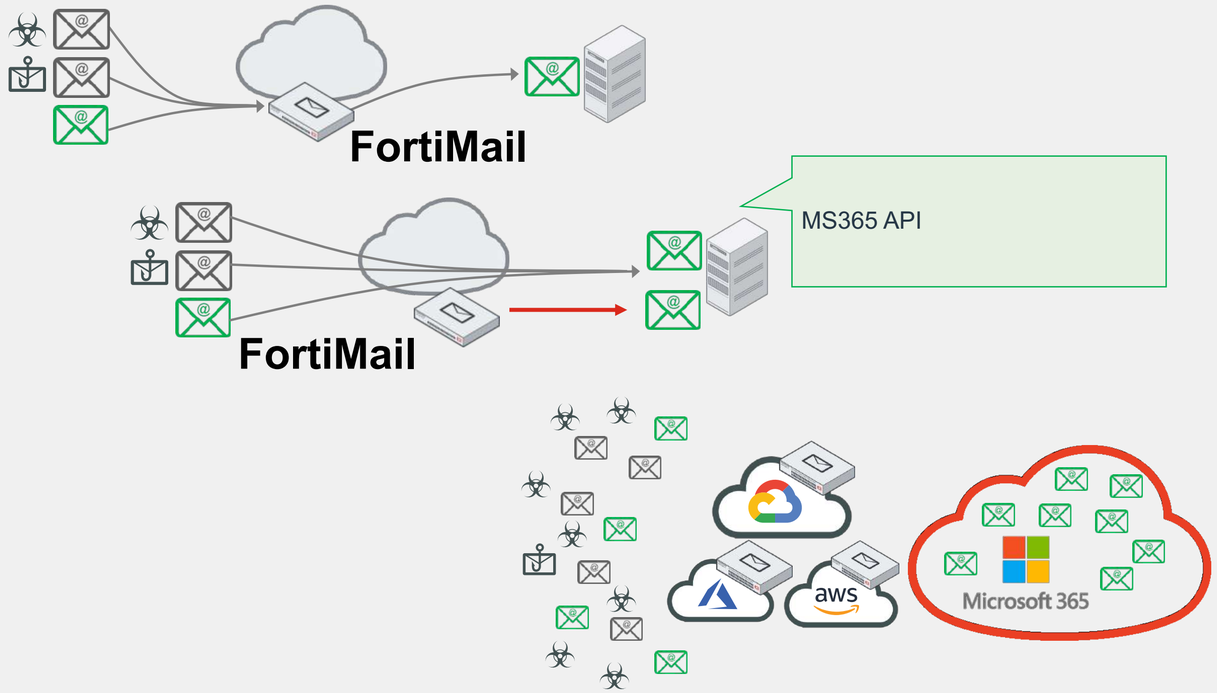




6. Zabezpečení komunikace e-mailem

FortiMail, FortiMail Cloud

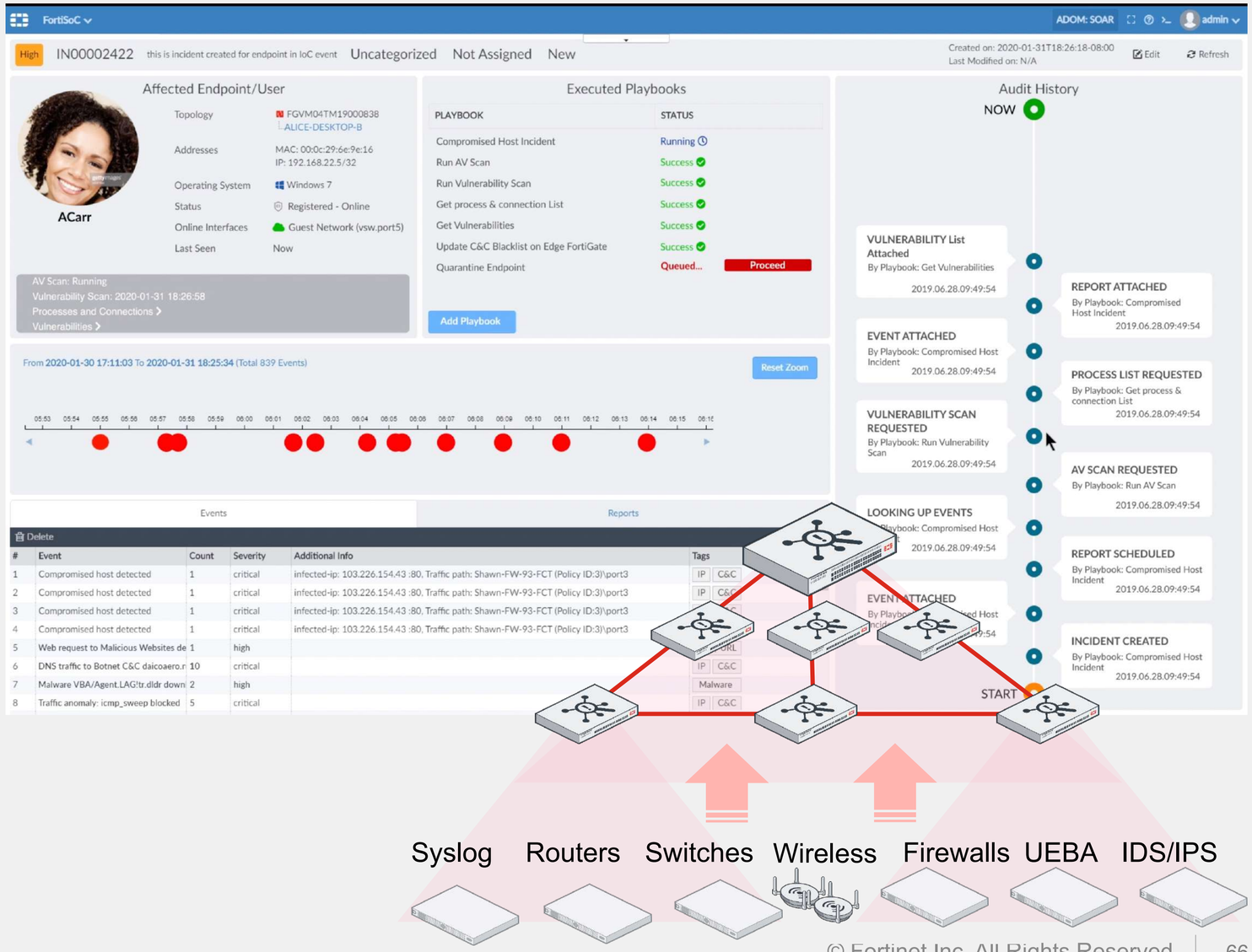
- E-mail je stále #1 threat vector (malware přes e-mail 94 %)
- Podpora SaaS (MS365)
- Podpora MSSP režimu
- Integrace v rámci Fortinet Security Fabric:
  - FortiSandbox
  - FortiIsolator
  - FortiNDR a další
- Otestujte si pomocí CTAP programu



7. Práce s provozními informacemi (logy)

FortiAnalyzer, FortiSIEM, FortiSOAR, SoCaaS, FortiAIOps

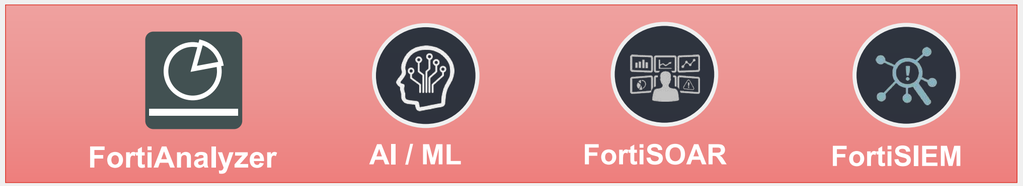
- FortiAnalyzer
  - FortiSoC modul
  - Playbooks (automatizace)
  - Investigace incidentu
- FortiSIEM/FortiSOAR
  - Pro pokročilejší zákazníky
- FortiSOCaaS
  - SOC jako služba poskytovaná společností Fortinet
  - FortiAIOps
  - Diagnostika a troubleshooting NOC pomocí ML/AI engine



7. Práce s provozními informacemi (logy)

Základní požadavky:

- Sběr logů
- Generování realtime informací
- Offline reporting
- Možnost centrální správy



Uvědomělé požadavky s ohledem na současnost:

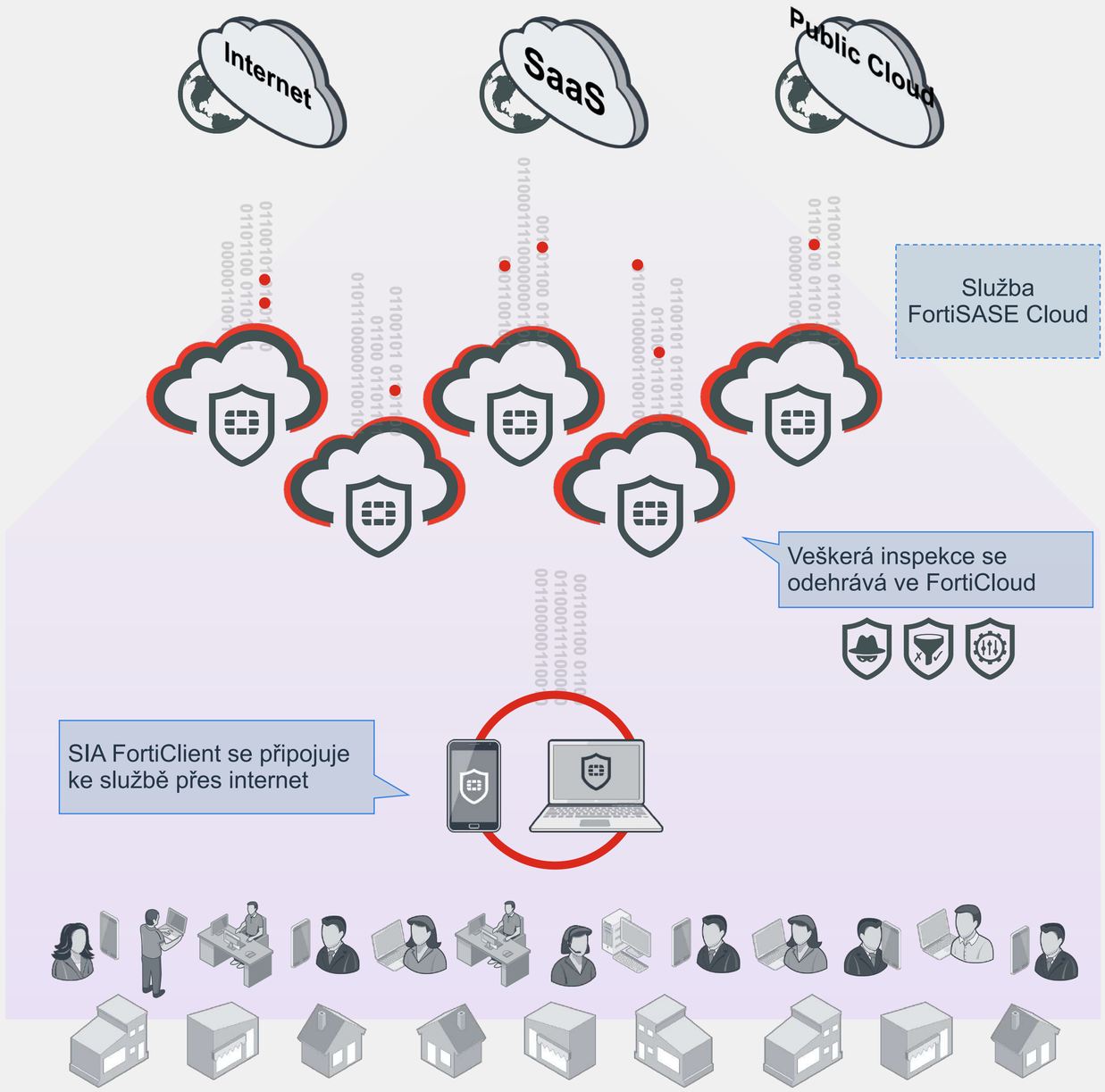
- Automatizace reakcí (playbook)
- Incident response framework
- Pomoc při investigaci incidentu přes celý ekosystém (Fortinet Security Fabric) s podporou AI/ML
- Zero Touch Deployment
- Konfigurační workflow
- Aplikační bezpečnost – best practice
- Optimalizace bezpečnostní politiky

8. Bezpečná práce na dálku

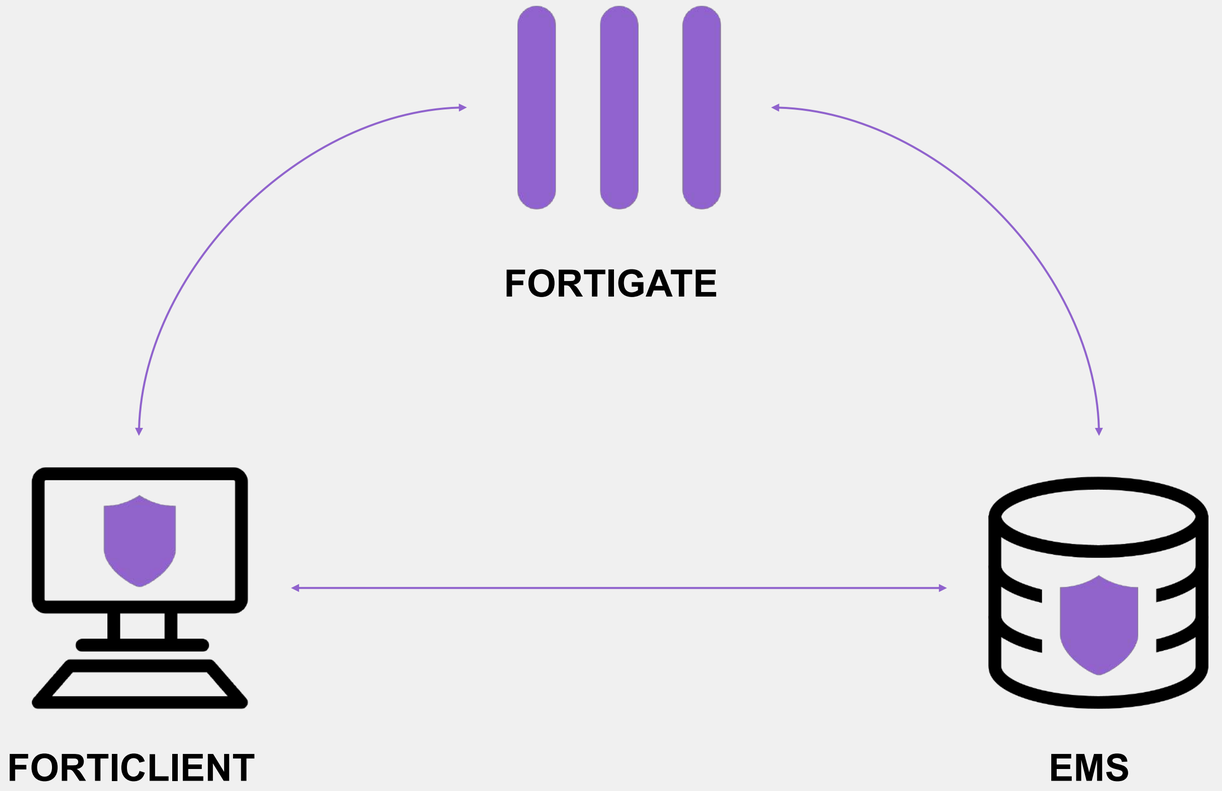
FortiSASE

Jak zabránit tomu, aby se uživatel nenakazil mimo chráněnou síť

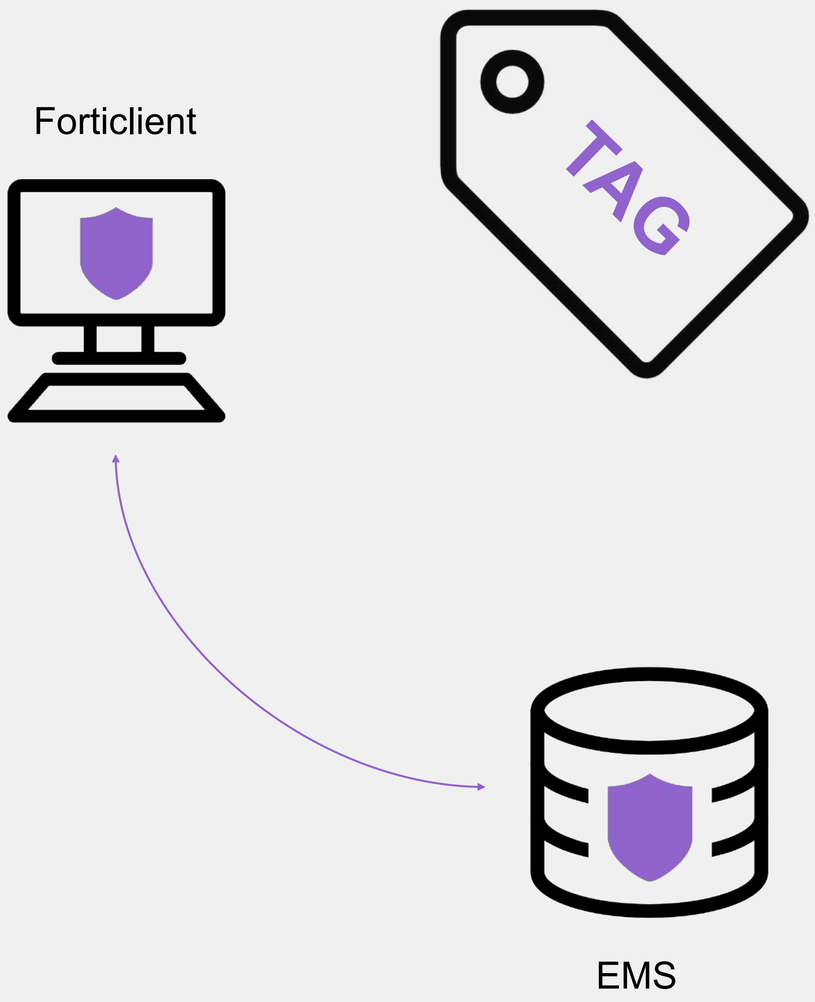
- SASE je obrovské téma (viz Gartner Hype Cycle)
- Bezpečnost pro koncová uživatelská zařízení poskytovaná z cloudu jako služba (FWaaS)
- Uživatel může být kdekoliv
- Pružné licencování



8. Bezpečná práce na dálku



8. Bezpečná práce na dálku



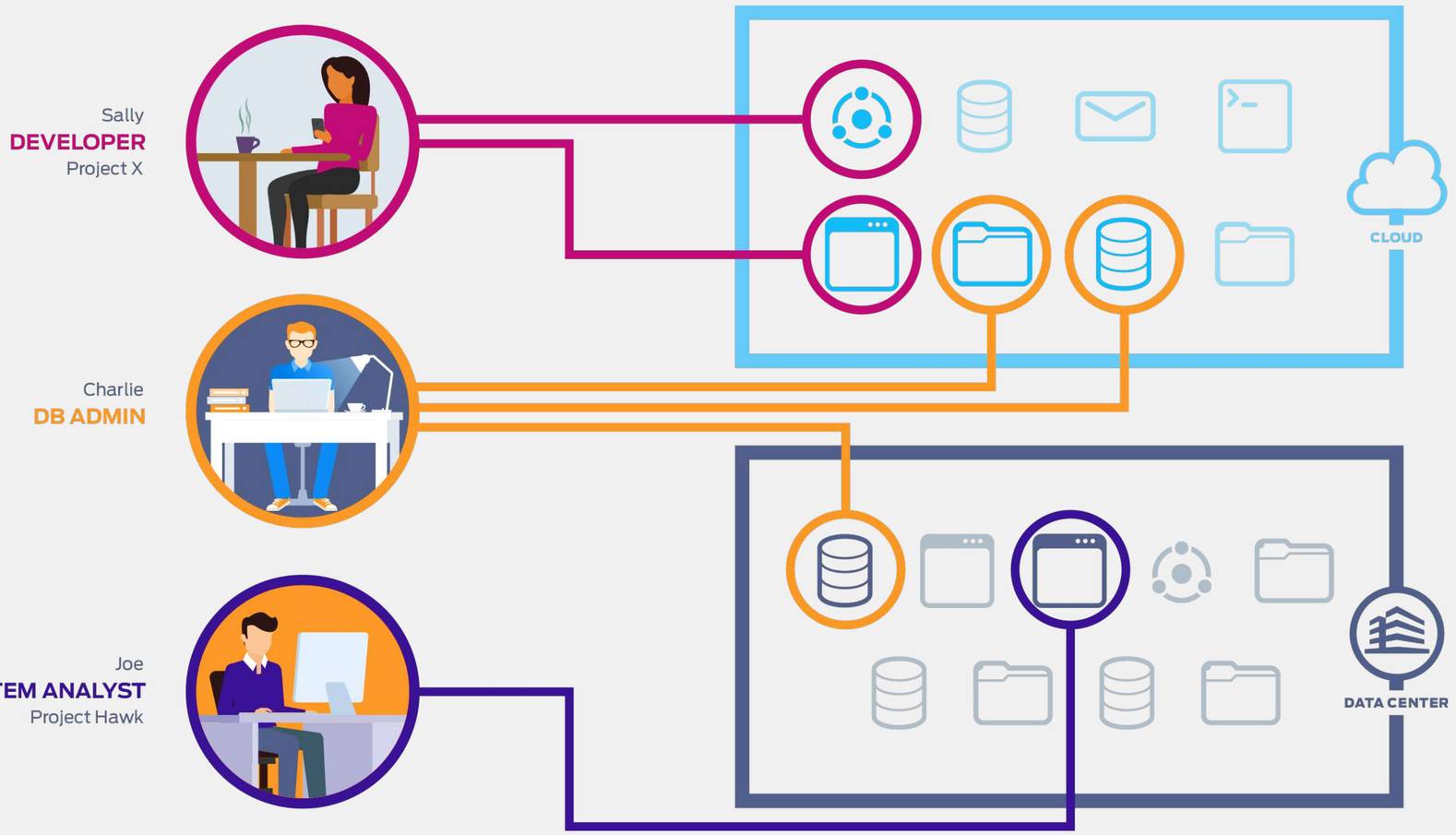
- AD Group
- **Antivirus software**
  - AV Software is installed and running
  - **AV Signatures is up-to-date**
- Certificate
- EMS Management
- File
- IP range
- Logged in Domain
- On-fabric Status
- OS Version
- Registry Key
- Running Process
- Sandbox Detection
- User Identity
- Vulnerable Devices
- Windows Security
  - Windows Defender is enabled
  - Bitlocker Disk Encryption is enabled
  - Exploit Guard is enabled
  - Application Guard is enabled
  - Windows Firewall is enabled

User Specified
- Social Network Login
  - Google
  - LinkedIn
  - Salesforce

8. Bezpečná práce na dálku

Stejné možnosti práce odkudkoliv

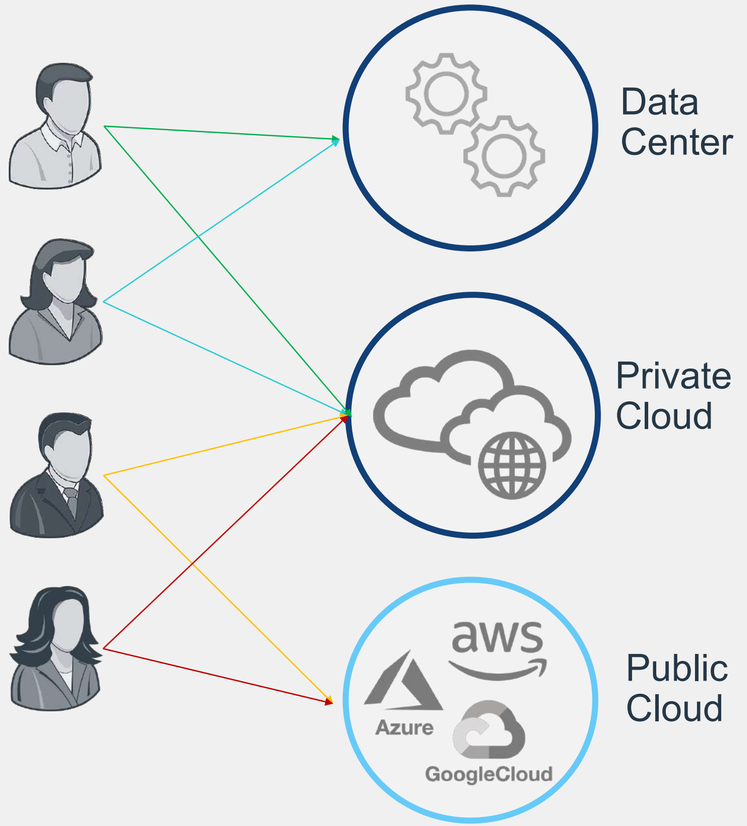
- Stejný přístup v kanceláři nebo mimo ni
- Automaticky zabezpečené aplikace
- Aplikace umístěné kdekoliv
- Možnost multifaktor autentizace



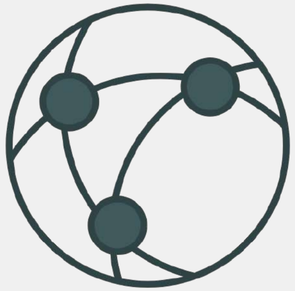
8. Bezpečná práce na dálku

Pro administrátory

- Granulární kontrola
- Centrálně spravované
- Aplikace umístěné kdekoliv
- Uživatelé se dostanou pouze k jim přiděleným aplikacím

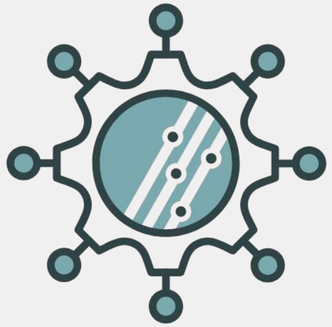


Co nás odlišuje



Attack Surface Coverage

- Users & Devices, Networks & Clouds
- Web & Email Applications
- External Attack Surface & Dark Web



Native Technology Integration

- More than a collection (or consortium) of point products
- Automated containment

Independent Validation

- Virus Bulletin, MITRE
- Gartner, Forrester, IDC, Kuppinger Cole and more
- ESG Research

Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

Secure Networking

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

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

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiProxy
Enforce internet, compliance and granular application control

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

Cloud Security

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

FortiDDOS Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiMail
Secure mail getaway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

FortiCNF Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

FortiSASE
Enforce dynamic network access control and network segmentation

ZTNA Agent Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiGuest Simplified guest access, BYOD, and policy management

FortiPAM
Control & monitoring of elevated & privileged accounts, processes, and critical systems

FortiGuard Threat Intelligence

Powered by FortiGuard Labs

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud Saas
w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage and customize LTE internet access

FNDN Exclusive
developer community for access to advanced tools & scripts

Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOp Tools & Script
Fortinet & community-driven

Fabric API Integration
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiRecon
Digital Risk Protection (DRP) for early, actionable warning and fast response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
15% of hardware

FortiCare Premium*
20% of hardware

FortiCare Elite**
25% of hardware

FortiConverter 25%
of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for ForiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

FortiFone
Robust IP Phones w/ HD Audio with centralized management

FortiVoice
Integrated voice, chat, conferencing management, and fax with centralized

FortiCamera
HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
High-performance NVR with AI-powered video management software

Fortinet Security Fabric

Broad

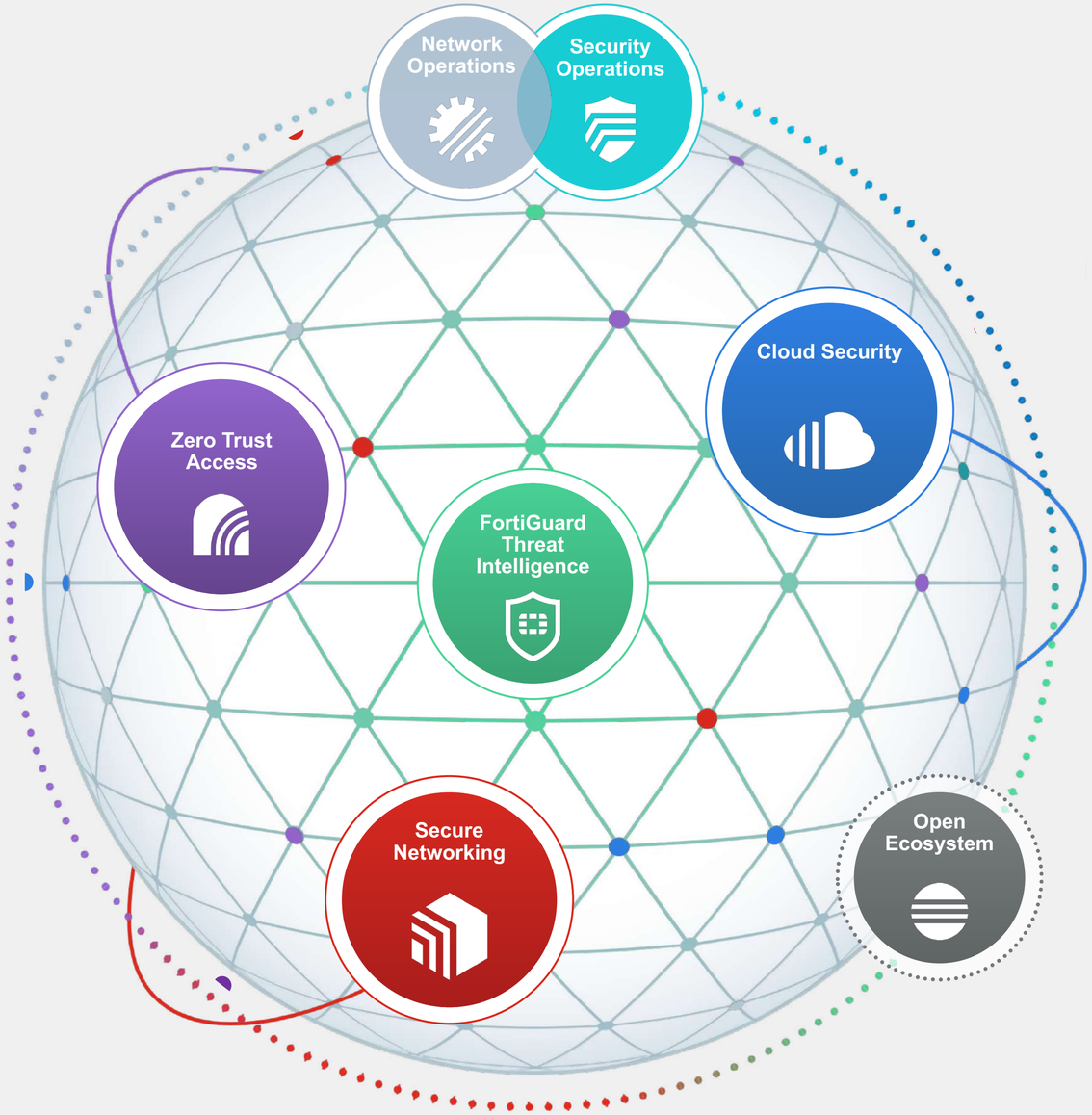
Široké spektrum různých bezpečnostních produktů

Integrated

Konsolidace a vzájemná provázanost

Automated

Rychlá automatizovaná reakce na odhalený incident



Shrnutí na závěr

- Jsme technologicky orientovaná firma
- Vlastní vývoj všech důležitých komponent
  - Operační systém FortiOS
  - HW Akcelerovaná platforma (hodnoty z datasheet odpovídají realitě)
  - Vlastní threat research laboratoř FortiGuard
- Pokrytí od provider prostředí až po SMB (domácí nasazení)
- Všechna zařízení mají stejný set funkcí
- Poskytujeme vlastní SoC formou služby (SoCaaS)

Shrnutí na závěr

- Široké produktové portfolio
- Vzájemná integrace jednotlivých produktových řad mezi sebou
- Integrace s 500+ dalšími vendory v rámci Fortinet Security Fabric
- Centrum technické podpory (Technical Assistance Center) v Praze
- Propracovaný systém školení NSE (8 úrovní)
- Jednoduchá licenční politika (nezávislá na počtu uživatelů)
- Obrovská instalovaná báze v CZ i ve světě
- Silná lokální podpora