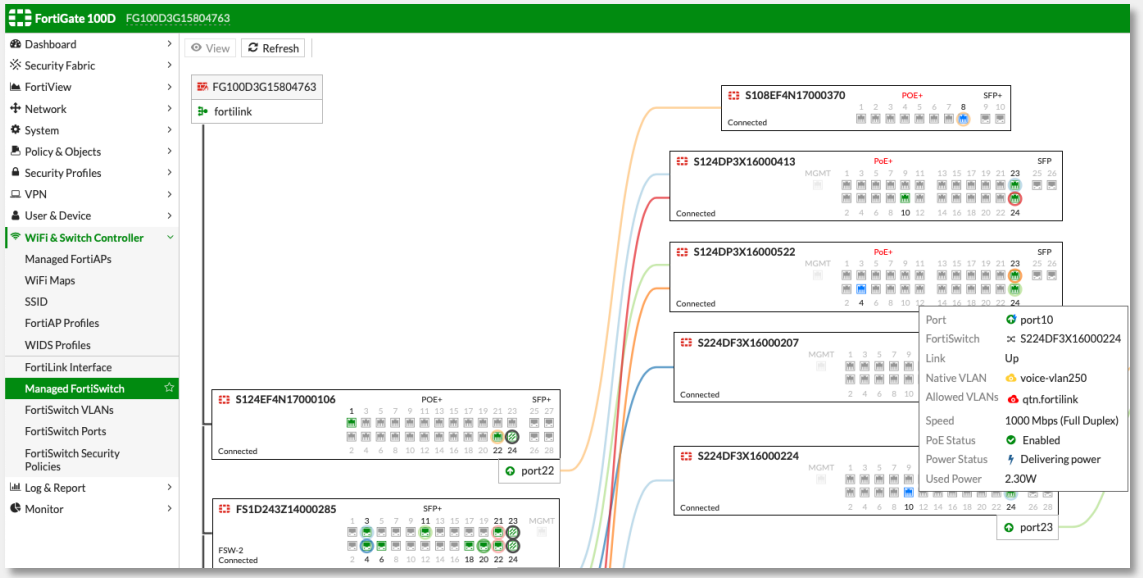
Bezpečnostní desatero
1. část

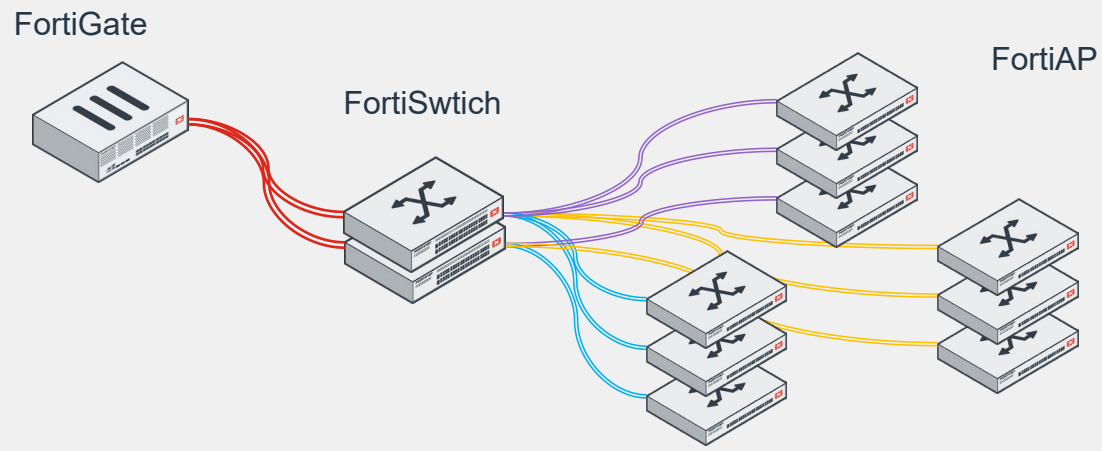
„1. Vnitřní síť segmentovat budeš!“

1. NGFW a bezpečná přístupová vrstva

FortiGate, FortiSwitch, FortiAP, FortiLink NAC, FortiNAC

- Segmentace sítě
- Vhodně nastavená NGFW politiky
  - Antivirus, AntiMalware, AntiBot
  - Web Filter, DNS Filter, Video Filter
  - Application Control
  - Inline CASB
  - Intrusion Protection System
  - Data Loss Prevention, File Filter
  - Web Application Firewall
  - Virtual Patching (např. OT)
- SSL inspekce (podporované šifry)
- Řízení přístupové vrstvy (switche, AP)
  - Centrální správa
  - Network Access Control (Lite verza FortiNAC)
- Device Asset Management
- Automatizace





„2. Bezpečnou cestou komunikovat budeš!“

2. Bezpečná komunikace

FortiMail, FortiMail Cloud, Workspace Protection

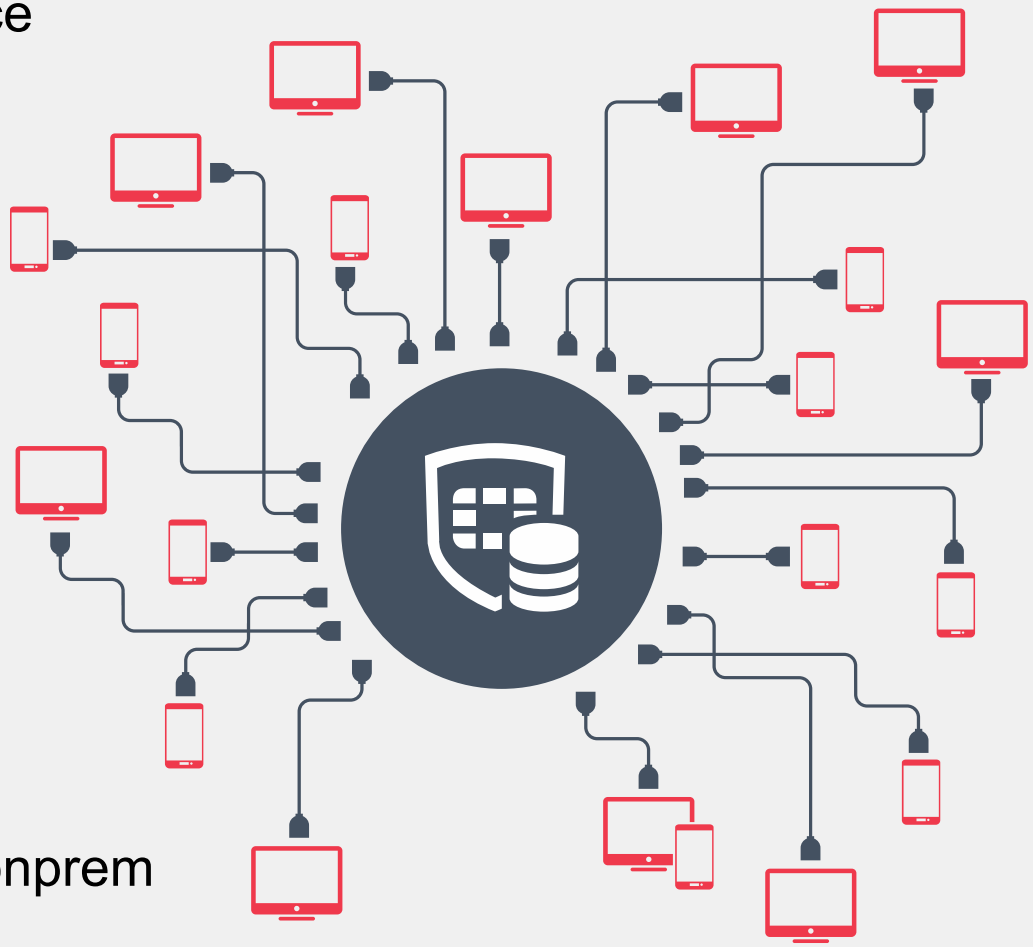
- Email je stále threat vektor číslo 1
- Cloudový poskytovatel mailu není garance bezpečnosti
- Nejde jen o spam a viry ale o další funkce:
  - Integrované DLP
  - Virus Outbreak Service
  - Secure Message Delivery
  - Identity Based Encryption
  - Content Disarm and Reconstruction
  - URL Click Protection
  - Impersonation Analytics
- Nejde jen o email → Workspace Protection

„3. Zabezpečenou pracovní stanici mít budeš, bezpečně na dálku pracovat budeš!“

3. Bezpečná pracovní stanice a bezpečný vzdálený přístup

FortiClient, ZTNA, FortiSASE, FortiCASB, FortiEDR, FortiEndPoint

- Jednotný agent pro telemetrické i bezpečnostní funkce
- ZTNA agent (VPN již odzvonilo)
- SASE agent
- PAM agent
- SW inventory
- Anti-ransomware a anti-malware
- Vulnerability assesment, endpoint posture
- Sandbox agent, CASB agent
- EDR, MDR,…
- Sběr provozních informací, centrální správa, cloud i onprem
- Téma pokryto v dalších prezentacích

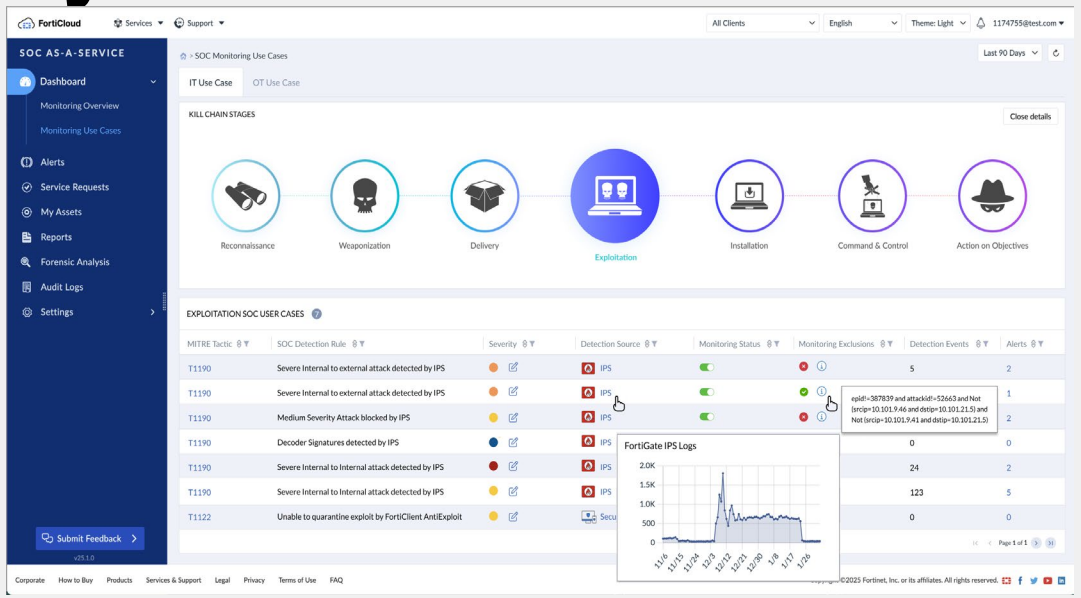


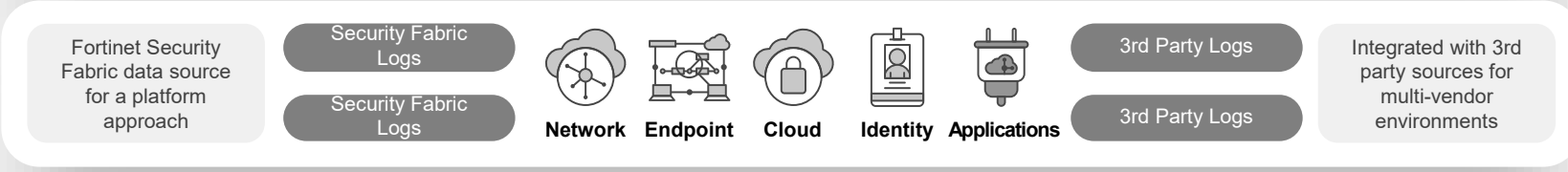
„4. Bezpečnostními incidenty zabývati se budeš!“

4. Práce s bezpečnostními incidenty

FortiSOCaaS, FortiAnalyzer, FortiSIEM, FortiSOAR

- SOCaaS
  - Vše jako služba
- FortiAnalyzer
  - IoC, Outbreak, SOC, Playbook
  - 3rd party log parser
  - FortiAI
- FortiSIEM, FortiSOAR
  - Korelace
  - Automatizace
  - Orchestrace

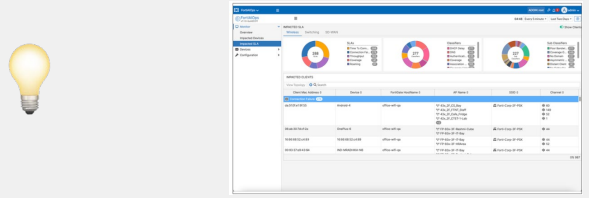


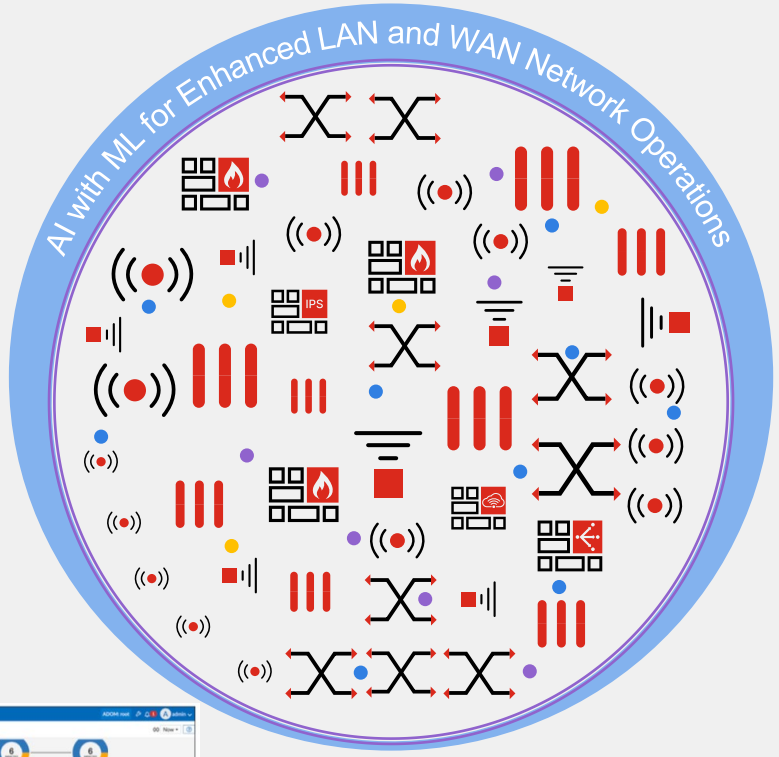


„5. Nejmodernější nástroje pro usnadnění práce používat budeš!“

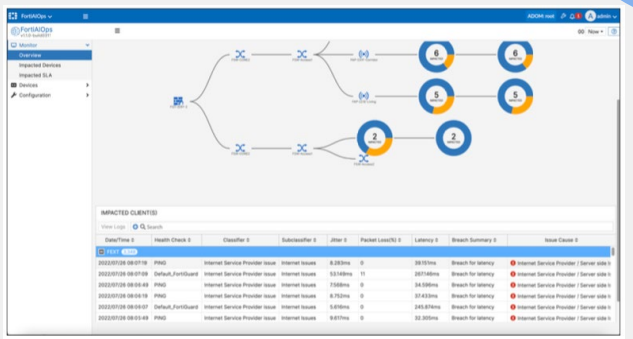
5. Využití automatizace a AI

FortiAI, FortiAIOps





- FortiAI
  - FortiAI Protect - pro detekci hrozeb
  - FortiAI SecureAI - únik citlivých dat do LLM
  - FortiAI Assist - NoC a SoC
- FortiAIOps
  - Autonomní nástroj pro detekci provozních problémů v sítí a jejich řešení
- FortiAIGate
  - Nový produkt určený k zabezpečení LLM



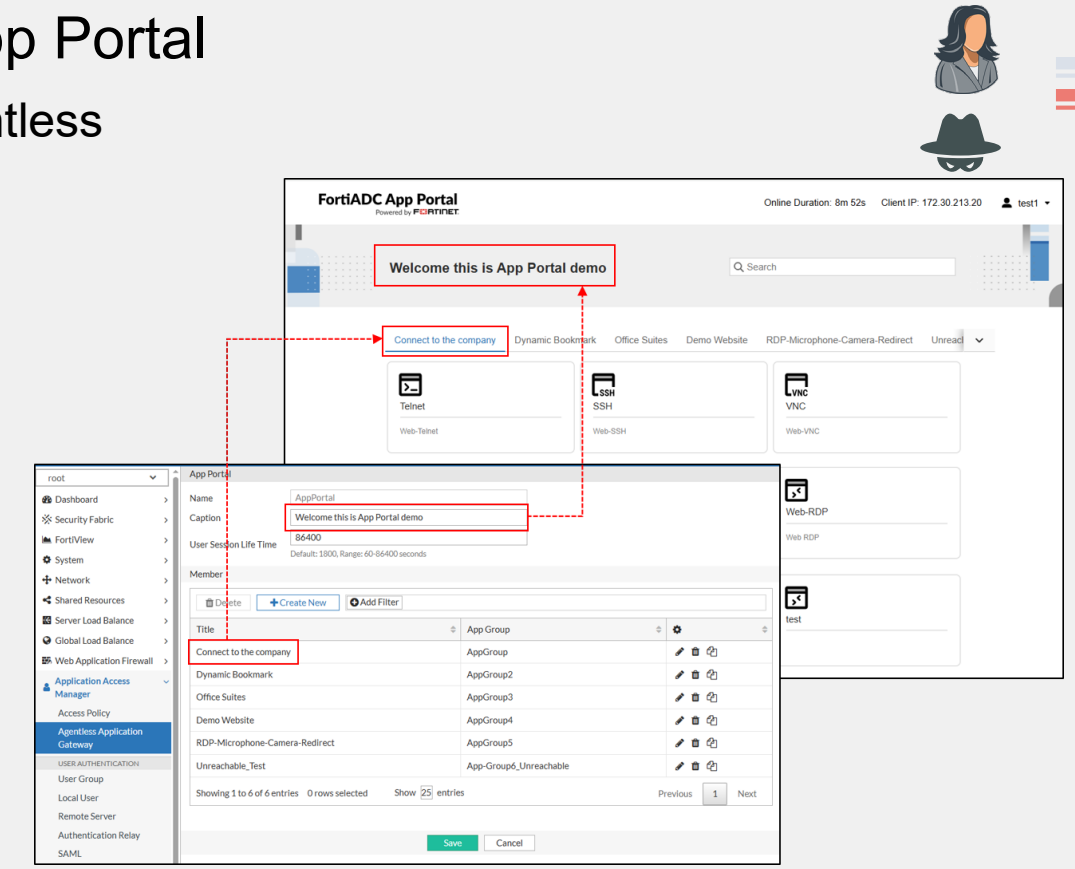
Bezpečnostní desatero
2. část

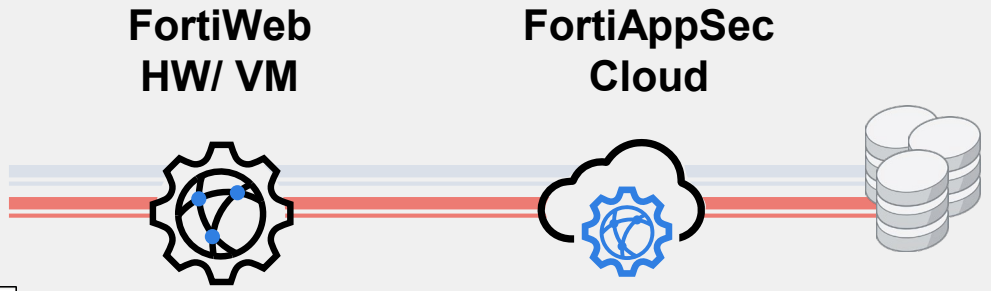
„6. Služby do internetu bezpečně vystavovat budeš!“

6. Zabezpečení vystavených služeb

FortiWeb, FortiWeb Cloud, FortiADC, FortiRECON, FortiAppSecCloud

- Web aplikační firewall (WAF)
  - Cloud i onprem
  - Jako služba
- FortiADC App Portal
  - ZTNA agentless





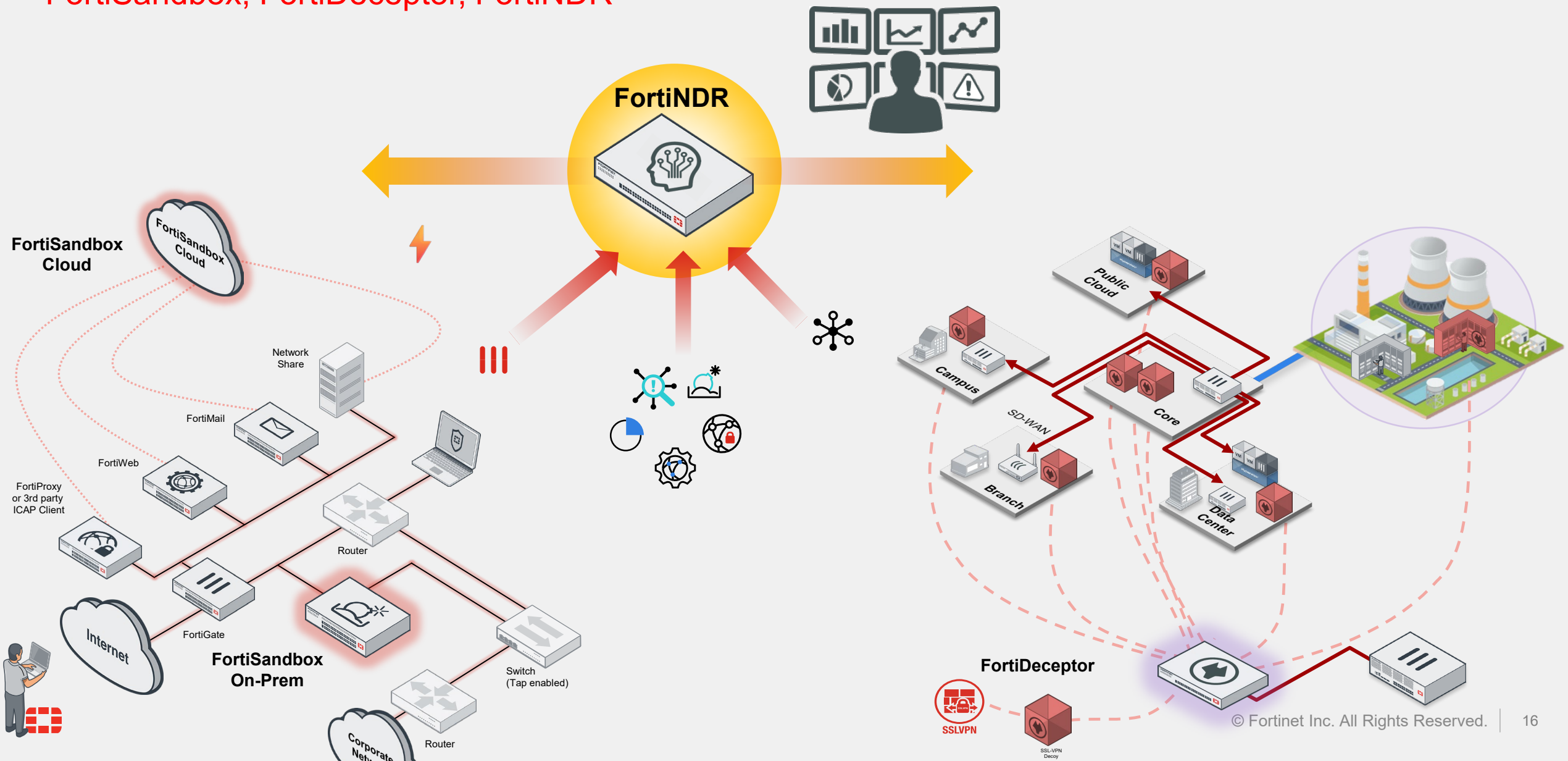
Every WAF deployment modes supported, Reverse Proxy being most common.

Realtime, structured visibility of application usage and web attacks.

„7. Ochranu před pokročilými hrozbami implementovat budeš!“

7. Ochrana před pokročilými hrozbami

FortiSandbox, FortiDeceptor, FortiNDR

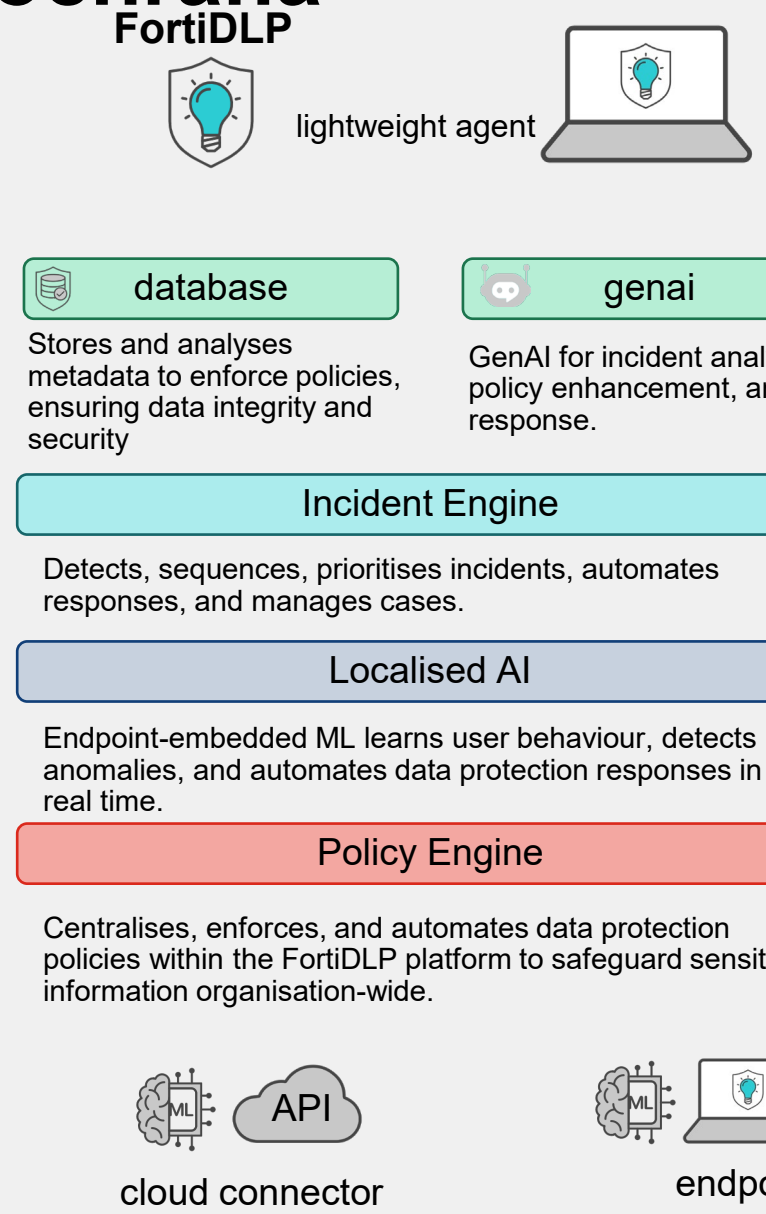


„8. Citlivá data jako oko v hlavě střežit budeš!“

8. Ochrana před únikem citlivých dat, ochrana digitální identity

FortiDLP, FortiDATA, FortiRecon, FortiSAT, FortiDAST

- DLP funkce ve FortiGate, FortiWEB, FortiMail, FortiSASE
  - FortiGuard DLP funkce – 500 datových patternů
- FortiDLP – Endpoint DLP + IRM + SaaS Security
- FortiDATA – Klasifikace dat na úložištích
- FortiRecon – EASM, Brand Protection, Threat Intel
- FortiDAST – testování zranitelností web. Aplikací
- FortiSAT – Security Awareness Training

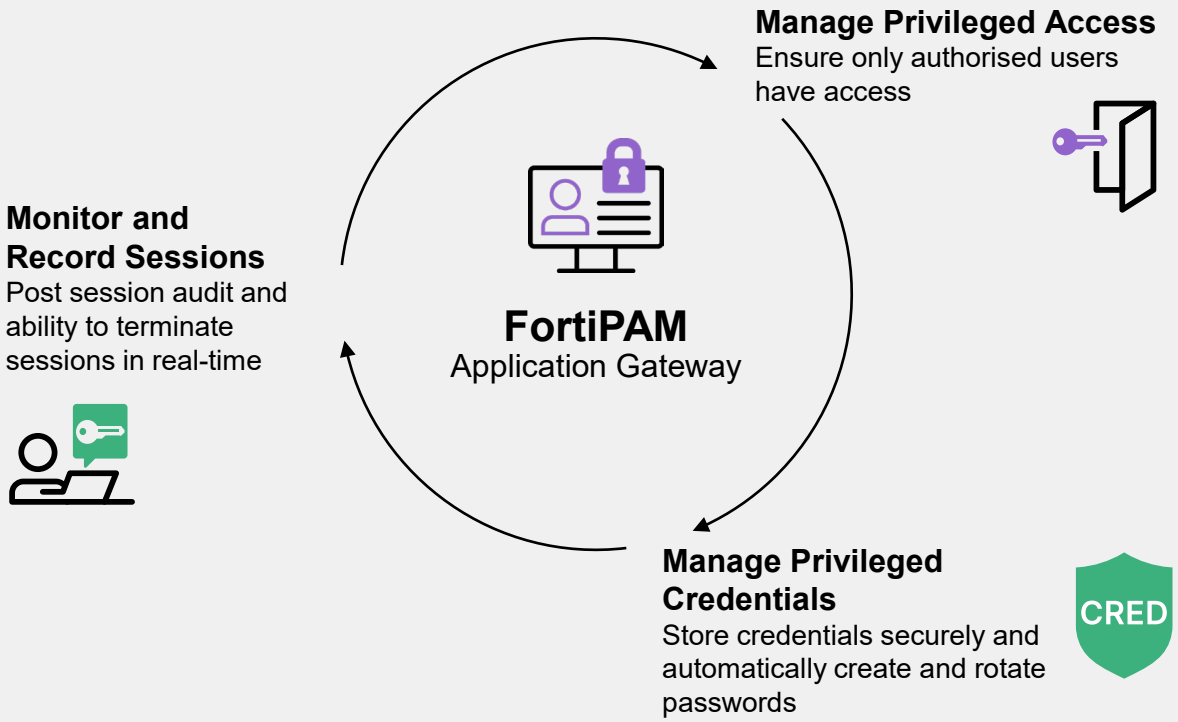


„9. Přístupy ke kritickým systémům pečlivě kontrolovat budeš!“

9. Ochrana přístupu ke klíčovým systémům

FortiPAM

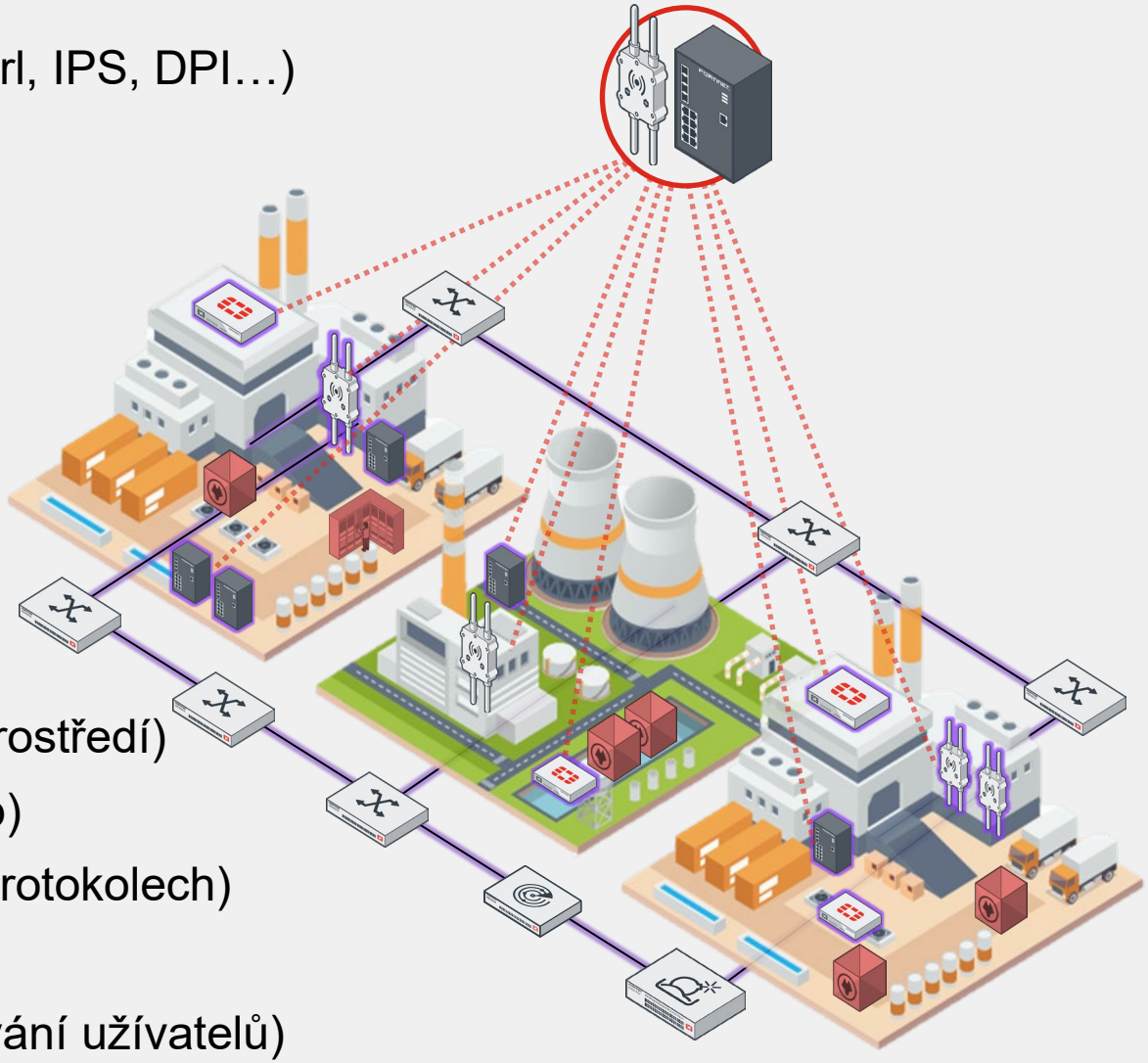
- Centrální správa privilegovaných účtů
- Zabezpečení přístupů k citlivým systémům
- Audit a sledování činnosti
- Integrace s dalšími produkty
  - FortiGate, FortiAuthenticator, FortiClient, ZTNA
- Bezpečná práce s hesly
  - Secrets Management, rotace hesel
- Určeno do IT i OT prostředí
- Bezpečný přenos souborů
- Bezpečný přístup na dálku (zahrnuje FortiSRA)



„10. O bezpečnost OT a IoT zařízení řádně pečovat budeš!“

10. Ochrana světa OT/IoT

- OT funkce v
  - FortiGate (Virtual patching, Device Asset, AppCtrl, IPS, DPI…)
  - FortiSwitch, FortiAP (mikrosegmetace)
  - FortiClient (EPP pro pracovní stanice)
  - FortiEDR/XDR/MDR (pokročilé zabezpečení)
  - FortiExtender (konektivita, sd-wan)
  - FortiAnalyzer (OT Security Service)
  - FortiNAC (OT/IoT headless device)
  - FortiDeceptor (OT Decoy)
  - FortiSandbox (OT Linux)
  - FortiNDR (detekce podezřelého chování v OT prostředí)
  - FortiPAM (+FortiSRA bezpečný vzdálený přístup)
  - FortiSIEM, FortiSOAR (detekce anomálií v OT protokolech)
  - Forinet Security Fabric Partner Ecosystem
  - FortiToken a FortiAutenticator (bezpečné ověřování užívatelů)
  - …



„11. Bezpečnostní nástroje mezi sebou propojovat budeš!“

The Broadest Platform in Cybersecurity

Secure Networking

FortiGate
NGFW with ASIC acceleration and industry leading Convergence

FortiAP
Protected Wi-Fi connectivity via Secure Networking convergence with FortiGate

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

FortiGate Cloud
SaaS platform offering zero-touch deployment, network management and security analytics

FortiAIOps
AI based insights for rapid analysis and remediation of network issues

FortiVoice
Unified communications with secure voice, chat, conferencing, and fax

FortiRecorder
Secure NVR with smart AI analysis and centralized visibility

FGaaS
Hardware as a service for FortiGate

FortiSwitch
Protected Ethernet connectivity via Secure Networking convergence with FortiGate

FortiManager
Centralized management of your Fortinet security infrastructure

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiEdge Cloud
Cloud management for standalone LAN, WLAN and 5G gateway equipment

FortiFone
Robust IP phones and softclient to stay connected from anywhere

FortiCamera
Physical security with intelligent motion detection in any light condition

FortiConverter
Secure and automated firewall migration from a broad spectrum of vendors

Resources

Product Matrix
Specifications for top selling models

Free Training
Fortinet is committed to training over 1 million people by 2025

FortiOS
The Heart of the Fortinet Security Fabric

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiCare
Support and mitigation services

Unified SASE

SASE

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

FortiClient ZTA Agent
Remote access, application access, and risk reduction

FortiProxy
Enforce internet compliance and granular application control

FortiCASB
Prevent misconfigurations of SaaS apps and meet compliance

FortiClient EPP Agent
Endpoint Protection Agent with AV, URL and Sand-box

FortiSASE
Cloud-delivered Security Services Edge

FortiMonitor
SaaS based DEM platform, performance monitoring

CLOUD

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

FortiWeb
Prevent web application attacks against critical web assets

FortiGSLB
Ensure business continuity during unexpected network downtime

FortiFlex
Flexible daily usage-based consumption licensing for a broad catalog of solution

FortiGate CNF
Hosted cloud-native firewall for simplified cloud network security

FortiADC
Application-aware intelligence for distribution of application traffic

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

FortiPoints
Simplified, flexible licensing for annual contracts, renewals, upgrades, and co-terms

AI-Powered FortiGuard Security

- Web Filtering
- IPS
- AV
- Sandbox
- IL MPS
- Application Control
- Attack Surface
- DLP
- OT Security Services
- IoC
- IL CASB

Security Operations

FortiAnalyzer
Security Fabric log management, monitoring and response

FortiSIEM
Enterprise-wide monitoring, threat detection, and response

FortiEDR/XDR
Automated endpoint protection and correlated incident response

FortiSOAR
Automated security operations, investigation, and response

FortiNDR
AI-driven analysis to detect and respond to threats

SOCaaS
Continuous security monitoring, incident triage, and escalation

IR Services
Rapid detection, containment, and recovery of cyberattacks

FortiDeceptor
Active deception platform for early in-network attack detection and response

FortiTrust Identity
Identity and Access Management as a Service (IDaaS)

FortiGuest
Access management solution for temporary access to guests and visitors

FortiCNAPP
Secure code to cloud with a single, data-driven platform

FortiDLP
Endpoint DLP and Insider Risk management

FortiMail
AI-powered, protection against email-borne threats

FortiSandbox
AI-powered real-time protection against unknown and 0-day threats

FortiToken
Cloud/HW/Mobile MFA provide passwordless adaptive authentication

FortiAuthenticator
Centralized identity and access management solution

FortiGuard MDR Service
Managed threat detection, investigation, and response

FortiRecon
Proactive digital risk protection service and external/internal threat monitoring

FortiPAM
Privileged identity and access management, and session monitoring

FortiTester
Network performance testing and breach attack simulation (BAS)

FortiDevSec
Orchestrated and automated continuous application security testing

FortiDAST
Automated black-box dynamic application security testing

FortiScanner Cloud
Cyber Asset Attack Surface Management Service

FortiAI
Integrated GenAI Assist for SOC and NOC

OT Security Platform

OT Security Service
FortiGuard subscription for FortiGate NGFW enables protection against OT-specific threats

Ruggedized Products
Rugged NGFW, switch, AP, and 5G extenders provide secure connectivity in harsh outdoor environments

FortiSRA
Agentless secure remote access offers robust remote access control, management, session logging, monitoring, and recording

SecOps for OT
Advanced cybersecurity controls bring OT networks into the SOC and incident response plans

Open Ecosystem

FNDN
Advanced tools for Fortinet community to develop custom solutions

Fabric Connectors
Fortinet-developed integrations for automation and security

Fabric API
Partner-developed integrations for end-to-end visibility and protection

DevOps Tools
Community-driven scripts automate network/security tasks

Extended Ecosystem
Integrates with third-party systems and orgs for sharing threat-intel

Fortinet Security Fabric

Broad

Visibility and protection of the entire digital attack surface to better manage risk

Integrated

Solution that reduces management complexity and shares threat intelligence

Automated

Self-healing networks with AI-driven security for fast and efficient operations


FORTINET