Technická opatření Zákona o kybernetické bezpečnosti

Lze se vyrovnat se všemi?

Viktor Pleštil

Adam Římský

181/2014 Sb., o kybernetické bezpečnosti

- 29. srpna 2014 vstoupil v platnost s účinností od 1. ledna 2015
- **Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti.** Zpracovává příslušné předpisy Evropské unie (jedná se o transpozici směrnice NIS) a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.
- Subjekty, kterých se zákon týká jsou dané nicméně ochrana dat, uživatelů a komunikace se týká všech – Zákon je metodikou a doporučením, jak přistupovat ke KB
- Pokrytí jednotlivých částí konkrétními řešeními různých výrobců může komplikovat integraci řešení do funkčního celku

➢ **Fortinet nabízí snadno integrovatelné řešení pokrývající zásadní kapitoly ZKB**

© Fortinet Inc. All Rights Reserved.

Části kybernetického zákona

Část 1 Kybernetická bezpečnost - Ostatní řeší platnost, účinnost, změny zákonů (6)

- Hlava 1 - základní ustanovení
  - Předmět úpravy, pojmy…
- **Hlava 2 – Systém zajištění kybernetické bezpečnosti**
- Hlava 3 – Stav kybernetického nebezpečí
- Hlava 4 – Výkon státní správy
- Hlava 5 – Kontrola, nápravná opatření a přestupky
- Hlava 6 – Závěrečná ustanovení

© Fortinet Inc. All Rights Reserved.

Hlava 2 – Systém zajištění kybernetické bezpečnosti

Bezpečnostní opatření -

Organizační

- System řízení bezpečnosti informací, rizik
- Bezpečností politika, organizační bezpečnost
- Bezpečností požadavky, řízení aktiv
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací, přístupu osob
- Zvládání kyber. událostí a incident
- Akvizice, vývoj, údržba
- Řízení kontinuity činností, kontrola a audit

Technická

- Fyzická bezpečnost
- Nástroj pro ochranu integrity komunik. sítí
- Nástroj pro ověřování identity uživatelů
- Nástroj pro řízení přístupových oprávnění
- Nástroj pro ochranu před škodlivým kódem
- N. pro zaznamenávání činností systému, už., admin
- Nástroj pro detekci kybernet. bezpečnostnbích událostí (KBU)
- Nástroj pro sběr a vyhodnocení KBU
- Aplikační bezpečnost
- Kryptografické prostředky
- Nástroj pro zajišťování úrovně dostupnosti informací
- Bezpečnost průmyslových a řídících systémů

© Fortinet Inc. All Rights Reserved.

SECURITY/NETWORK OPERATING CENTER

FortiAnalyzer
Central Log & report

FortiNAC
IoT Access Control

FortiSandbox
File Analysis

FortiAI
Virtual Security Analyst ™

FortiSIEM
SIEM / UEBA

FortiXDR
XDR

FortiManager
Central Device Mgmt.

FortiAuthenticator
User Access Mgmt.

FortiTester
Network Tester

FortiDeceptor
Honeypot

FortiSOAR
SOAR

HOSTED SERVICES

Cloud mgmt.
FortiGate Cloud | FortiLAN Cloud | FortiExtender Cloud | FortiManager Cloud | FortiAnalyzer Cloud | FortiClient EMS Cloud | FortiToken Cloud | FortiSOAR Cloud

Cloud services
FortiPresence | FortiMail Cloud | FortiPhish | FortiGSLB | FortiConverter | Fortinet SOCaaS | FortiSASE | FortiPenTest | FortiWeb Cloud | FortiSandbox Cloud | FortiVoice Cloud | FortiMonitor

MOBILE USERS

FortiToken
2 Factor OTP Token

FortiClient / FortiEDR
VPN, ZTNA, EPP, and SASE Client

FortiCASB

FortiCWP

SaaS

Secure SD-WAN

IPsec / SSL VPN

SASE

FortiGate
Security Gateway

ZTNA

FortiDDoS
L7 D/DOS Mitigator

FortiADC
Load Balancer

FortiMail
Mail Sec. Gateway

FortiWeb
Web App. Firewall

Fortilsolator
Browser Isolation

FortiProxy
Secure Web Gateway

BRANCH OFFICE

FortiWiFi
Secure WiFi Access

FortiExtender
3G/4G/5G WAN

LAN

FortiSwitch
Switch

FortiAP
Wireless Access Point

FortiRecorder
Surveillance Manager

FortiVoice
IP PBX

FortiCamera

FortiFone

DATA CENTER

CLICK ON PRODUCT NAME TO JUMP ONTO ITS SECTION

© Fortinet Inc. All Rights Reserved.

Fortinet Security Fabric

Broad

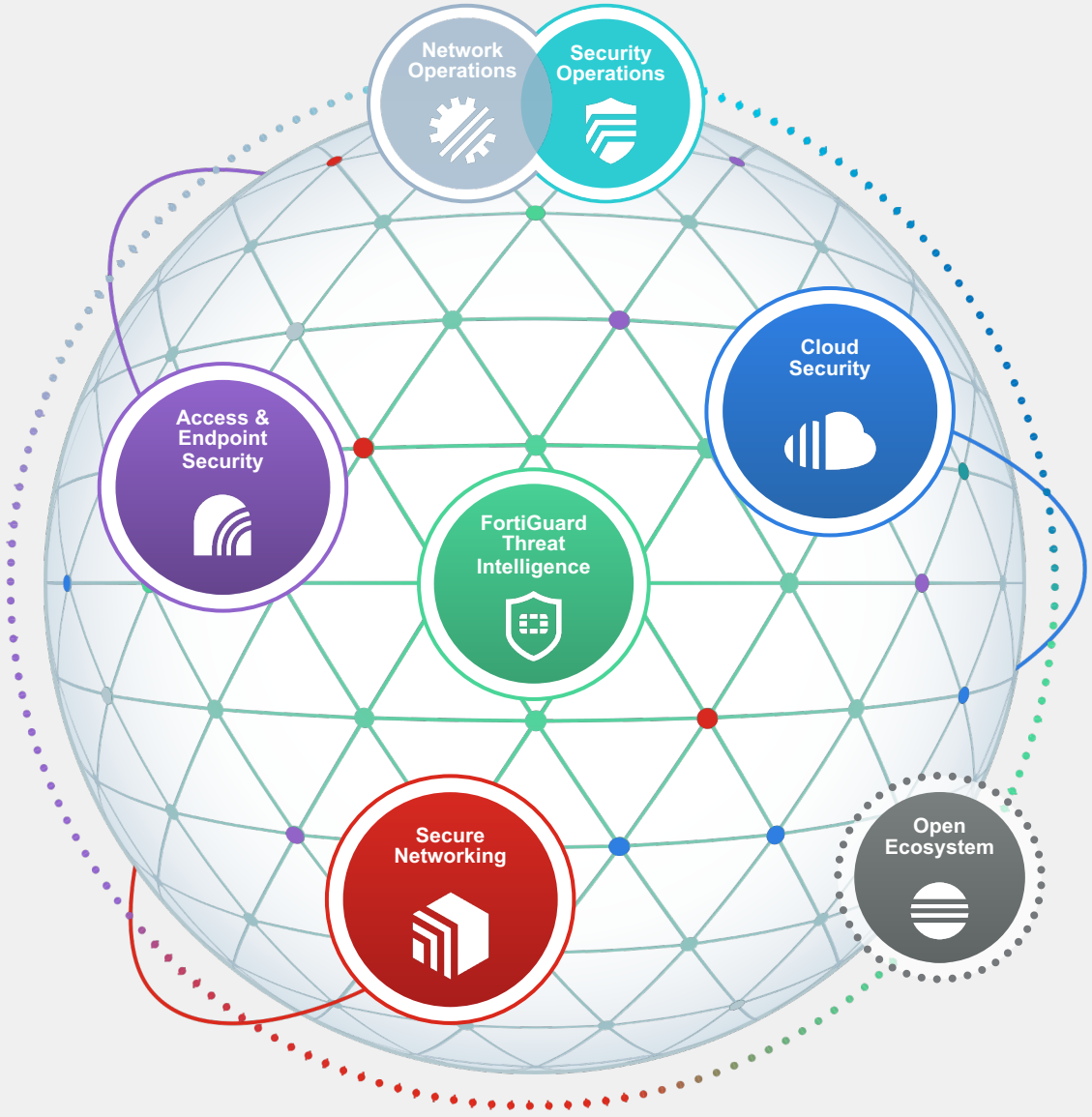
Visibility and protection of the entire digital attack surface to better manage risk

Integrated

Solution that reduces management complexity and shares threat intelligence

Automated

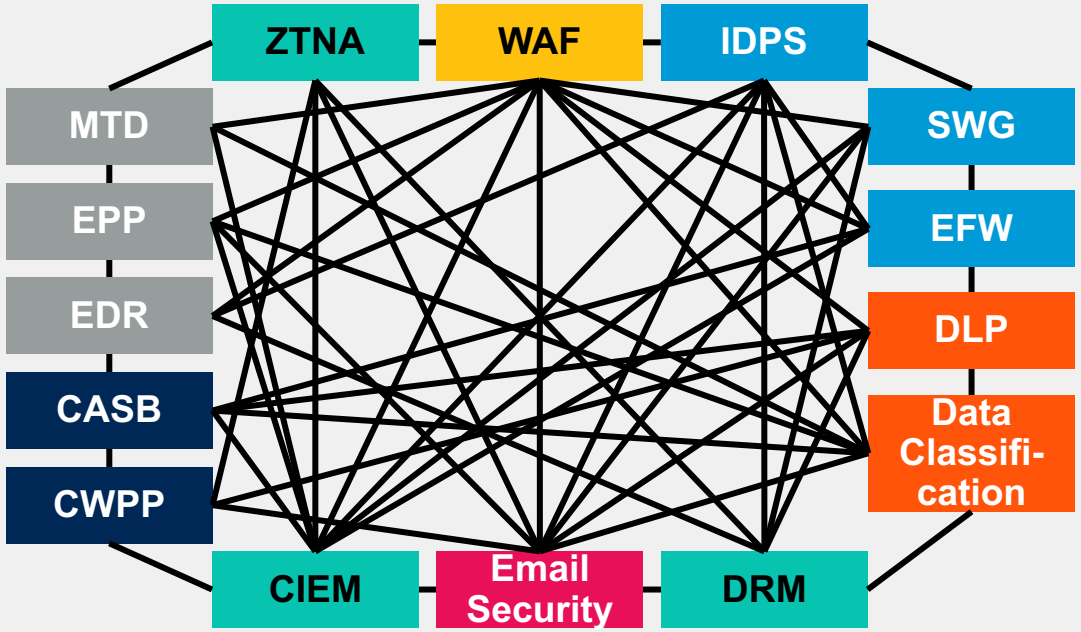
Self-healing networks with AI-driven security for fast and efficient operations



© Fortinet Inc. All Rights Reserved.

Gartner Cybersecurity Mesh Architecture

Gartner



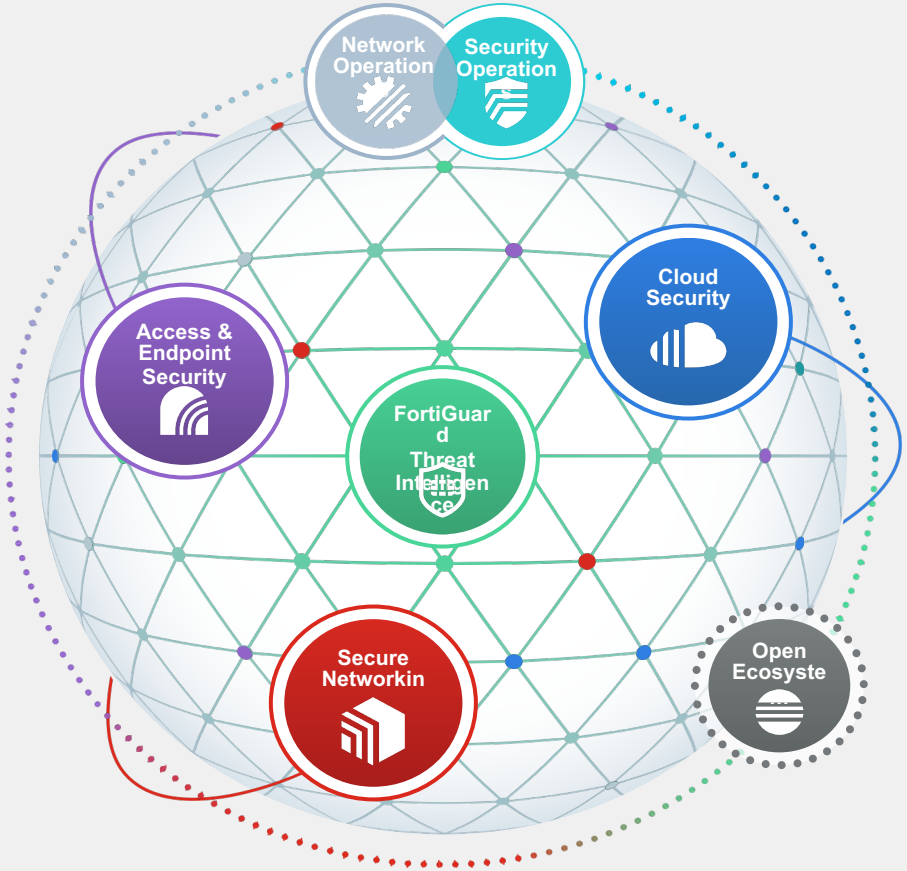
Executive Guide to Cybersecurity Mesh, 2022

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



Appliance
Virtual
Hosted
Cloud
Agent
Container

© Fortinet Inc. All Rights Reserved.

FortiGuard Labs – Industry-leading Threat Intelligence

Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. A pioneer and security industry innovator, FortiGuard Labs develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence.

Ai/ML-driven Threat Intelligence

Over 100B global security events analyzed to provide over 1B security updates daily

Actionable Information and Services

- Incident Response
- Zero Day Research
- Penetration Testing
- Anti-Phishing training
- And More

Actionable Information and Services

CYBER THREAT ALLIANCE · WORLD ECONOMIC FORUM · INTERPOL · NCI AGENCY

ADVANCED THREAT PROTECTION	UNIFIED THREAT PROTECTION	ENTERPRISE PROTECTION	
Content Security	**Web Security**	**Device Security**	**SOC/NOC Tools**
Optimized to monitor and protect against file-based attack tactics	Optimized to monitor and protect against web-based attack tactics	Optimized to protect against device & vulnerability-based attack	Additional a-la-carte services for your SOC team

© Fortinet Inc. All Rights Reserved.

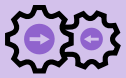
Open Ecosystem

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.

Fyzická bezpečnost

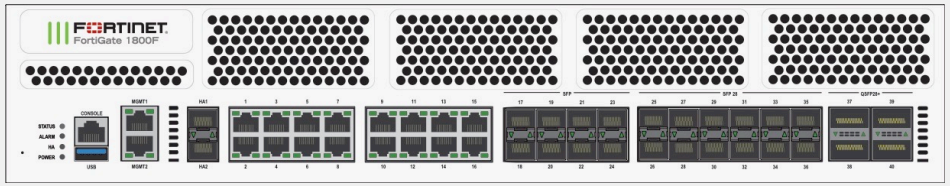
FortiCamera, FortiRecorder

- FC a její serverová část FR
- Bezpečnostní platforma pro sledování a ochranu jak venkovních, tak vnitřních prostor
- Jednotné management rozhraní shodné s ostatními produkty - jednotný koncept komplexního zabezpečení

© Fortinet Inc. All Rights Reserved.

Nástroj pro ochranu integrity komunikačních sítí a nástroj pro detekci kybernet. bezpečnostnbích

FortiGate, FortiSandbox, FortiIsolator, FortiDeceptor, FortiDDoS



① 2 x GE RJ45 MGMT Ports
② 2 x 10 GE SFP+ / GE SFP HA
③ 16 x GE RJ45 Ports
④ 8 x GE SFP Slots
⑤ 12 x 25GE SFP28/10GE SFP+ Slots
⑥ 4 x 40GE QSFP+ Slots

198 Gbps
Firewall throughput

12 / 40* Mil
Concurrent Sessions

12 Gbps
SSL Inspection Throughput

17 Gbps

IPS Throughput

11 Gbps
NGFW Throughput

9.1 Gbps
Threat Protection Throughput

- NGFW FG nativně umožní například
  - L2/L3 stavový FW
  - FortiLink NAC
  - L7 LB
  - DLP

- NGFW FG zajistí segmentaci a zabezpečení komunikační sítě
- NGFW FG umožní nasadit globální zabezpečené SD-WAN řešení bez další licence
- HW akcelerace samostatnými SPU potlačuje degradaci výkonu
- FortiSanbox a FortiIsolator poskytne bezpečné prostředí pro analýzu dat a detonaci škodlivého kódu
- FortiDeceptor umožní nasadit a centrálně spravovat inteligentní nástrhy v lokální síti
- FortiDDoS umožní ochránit propustnost WAN konektivity sítě během DoS a DDoS útoku

© Fortinet Inc. All Rights Reserved.

Nástroj pro ověřování identity uživatelů

FortiGate,FortiToken (HW, Mobile), FortiAutenticator, FortiNAC

- Všechny platformy ověřují identitu uživatele nebo koncové stanice v rámci interní databáze nebo proti centrální databázi identit
- Možnost rozšíření o dvou faktorovou autentizaci pomocí jednorázových OTP a Fido2 tokenů, tokenů zasílaných pomocí emailů nebo SMS
  - Ověření identity před zahájením aktivity
  - Řízení počtu možných neúspěšných pokusů
  - Odolnost uložených či přenášených autentizačních údajů a jejich ukládání ve formě odolné proti off line útokům
  - Opětovné ověření po určené době nečinnosti
  - Centralizovaná správa identit

© Fortinet Inc. All Rights Reserved.

Nástroj pro řízení přístupových oprávnění

FortiGate, FortiAuthenticator, FortiNAC

- Nástroje pro řízení přístupových oprávnění
  - Které zajistí řízení oprávnění pro přístup k jednotlivým aplikacím a segmentům sítě
  - Zaznamenává použití přístupových oprávnění v souladu s bezpečnostním potřebami a výsledky hodnocení rizik
- Možnost vytvářet bezpečnostní pravidla na základě identity uživatele nebo stavu koncové stanice
- Systém je možné propojit se stávajícími databázemi identit (například AD)

© Fortinet Inc. All Rights Reserved.

Nástroj pro ochranu před škodlivým kódem

FortiGate, FortiSandbox, FortiIsolator, FortiMail, FortiWeb FortiClient/FortiEDR

Co je třeba zabezpečit?

S ohledem na důležitost aktiv zajišťuje použití nástroje pro nepřetržitou automatickou ochranu

- Koncových stanic včetně serverů
- Mobilních zařízení
- Emailové komunikace
- Datových uložišť
- Komunikační sítě a jejich prvků

Jak toho dosáhneme?

- Kombinací perimetrových a lokálně instalovaných systémů
  - NGFW
  - SandBox
  - WAF
  - Email Security Gateway
  - Klientská ochrana
  - NAC nástroje pro řízení přístupu do sítě
- Vše s možností implementace jak on-prem, tak i v cloud

© Fortinet Inc. All Rights Reserved.

Nástroj pro sběr a vyhodnocení KBU a nástroj pro zaznamenávání činností informačního a komunikačního systému, jeho uživatelů a administrátorů

FortiAnalyzer, FortiSiem, FortiSoar

- Sběr a vyhodnocení událostí zaznamenaných dle pravidel pro zaznamenávání a detekci KBU
- Vyhledávání a seskupování souvisejících záznamů
- Poskytování informací o KBU pro určené role
- Vyhodnocování KBU pro identifikaci KB incidentů včetně varování určených rolí
- Omezení případů nesprávného vyhodnocení pravidelnou aktualizací nastavení pravidel pro vyhodnocování událostí a varování
- Využívání získaných informací pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému

© Fortinet Inc. All Rights Reserved.

Aplikační bezpečnost

Web aplikační firewall

- FortiWeb je dedikovaný WAF nástroj pro zabezpečení aplikačního přístupu s možností využití L7 LB a strojového učení na základě příchozího provozu pro eliminaci IPS false positive blokací
- Kromě ochrany umožňuje provádět testy zranitelností webových stránek a aplikací s výsledkem ve formě grafického reportu s kompletním seznamem všech zranitelných míst a doporučením řešením

FortiGate (IPS, AppCtrl, DLP)

- IPS poskytuje pokročilou ochranu před bezpoečnostními hrozbami
- AppCtrl umožňuje kontrolu komunikace na základě konkrétních aplikací a lze využít pozitivní i negativní model (tedy zvolit povolené aplikace a ostatní zakázat, či naopak)
- DLP umožňuje chránit síť před únikem citlivých informací ať už chybou či záměrem uživatele.

© Fortinet Inc. All Rights Reserved.

Kryptografické prostředky
FortiGate (SSLVPN, IPSecVPN), FortiAutenticator

- Centrální autentizační server FortiAutenticator umožňuje plně spravovat prostředí kryptografických klíčů (PKI). V kombinaci s moderními kryptografickými algoritmy použitými pro vzdálený přístup a šifrování pak umožňuje kompletně zabezpečit celou spravovanou síť
- Používá aktuální odolné krypt. Algoritmy a kryptografické klíče
- Používá systém správy klíčů a certifikátů který:
  - Zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů, likvidaci klíčů
  - Umožní kontrolu a audit
- Prosazuje bezpečné nakládání s kryptografickými prostředky
- Zohledňuje doporučení v oblasti krypt. klíčů vydaná příslušným úřadem

© Fortinet Inc. All Rights Reserved.

Nástroj pro zajišťování úrovně dostupnosti informací
FortiGate, FortiWeb, FortiADC, FortiGSLB

- FortiGate a FortiWeb díky integrované funkci rozdělování zátěže na úrovni 7. vrstvy ISO/OSI umožňuje rozklad zátěže mezi aplikačními servery
- FortiADC je specializované LB zařizení s vysokou propustností, které je možné využít pro pokročilé metody rozkládání záteže (2.-7. vrstva ISO/OSI)
- FortiGSLB je cloud based řešení pro geografickou redundanci pomocí úpravy DNS záznamů při nedostupnosti sledované služby
- Všechna naše zařízení podporují režim vysoké dostupnosti
- Co je třeba zabezpečit?
  - Dostupnost informačního a komunikačního systému (IKS)
  - Odolnost IKS vůči incidentům snižujícím jeho dostupnost
  - Dostupnost důležitých technických aktiv IKS
  - Redundanci aktiv nezbytných pro zajištění dostupnosti IKS

© Fortinet Inc. All Rights Reserved.

Bezpečnost průmyslových a řídících systémů
FortiGate/ FG-rugged

- Použití technických a programových prostředků do specifického prostředí
  - FortiGate – Rugged – varianta pro provoz v průmyslovém prostředí s odlišnou HW konstrukcí
    - Nasazení v problematických prostředích – prašnost, elektromagnetické rušení…..
    - Obě platformy poskytují kompletní ochranu pro prům. systémy jak na úrovni firewallu, tak na úrovni detekce konkrétních průmyslových aplikací

© Fortinet Inc. All Rights Reserved.


FORTINET