RansomWare, GDPR a Security Fabric

Zsolt Géczi, Regional account manager SK
zgeczi@fortinet.com

Fortinet: Global Network Security Leader

- **Highlights:** 2000 - present

FOUNDED IN
2000
BY KEN XIE

HEADQUARTERED IN
SUNNYVALE
CALIFORNIA

100+
OFFICES
ACROSS
THE GLOBE

4,650

EMPLOYEES WORLDWIDE

IN EXCESS OF
$1bn
REVENUE

$1.3bn
IN CASH

30%

GROWTH
YEAR ON YEAR

2.8m
SHIPPED
SECURITY
DEVICES

300K
CUSTOMERS

358
PATENTS
ISSUED

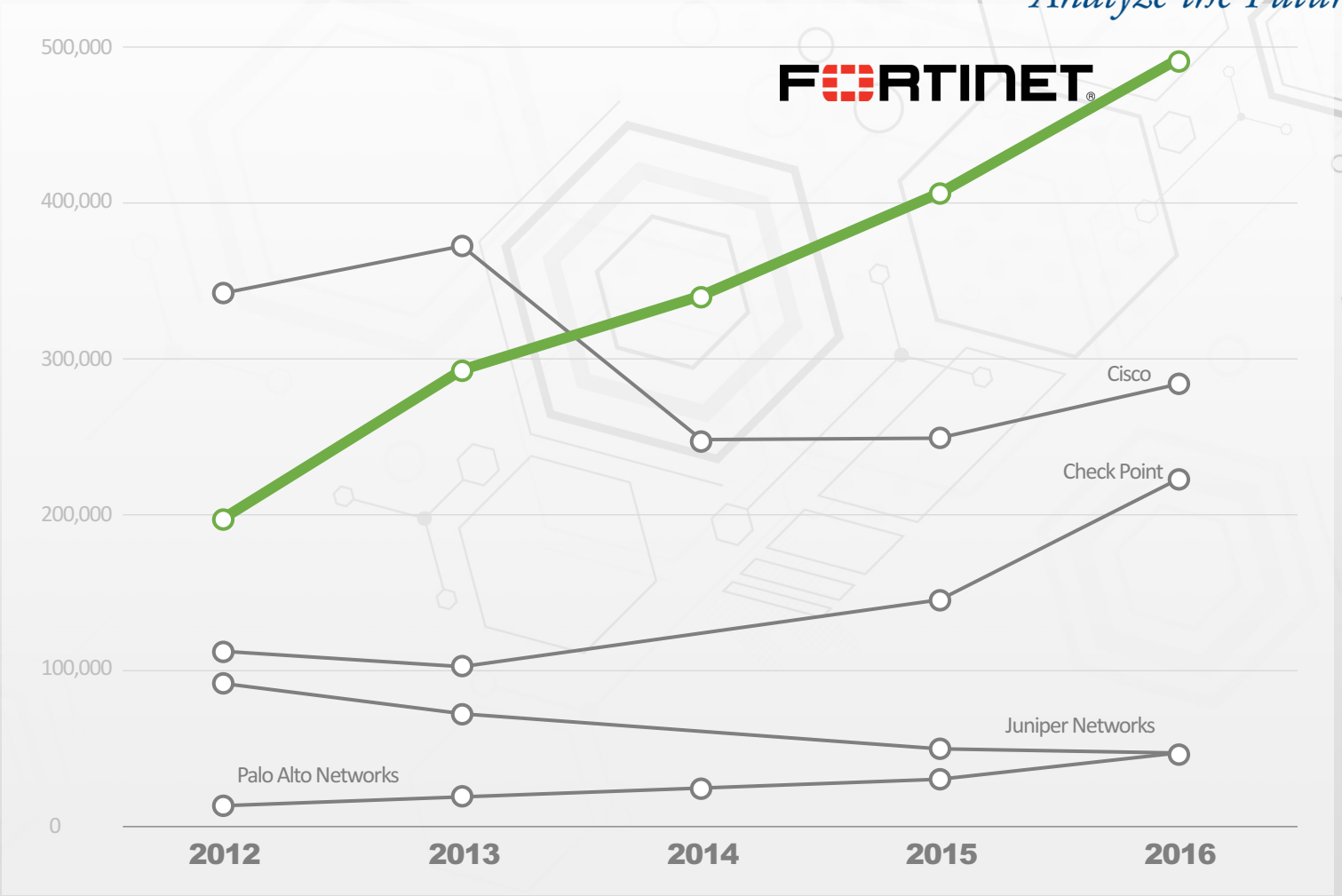
292 IN
PROCESS

Fortinet: Získava Podieľ na Rastúcom Trhu

- Fortinet vs Konkurencia

Riešenie širokého spektra výziev ...

- Fortinet je najväčším dodávateľom bezpečnostných zariadení na svete
- Spoločnosť Fortinet vyvinula vizionársku sadu bezpečnostných riešení



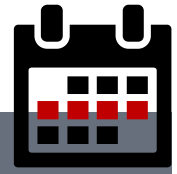
Source: IDC Worldwide Security Applicances Tracker, March 2016 (based on annual unit shipments)

Hrozby. Obrovské Množstvá.

Per Minute

35,000	Threat events
21,000	Spam emails intercepted
470,000	Network intrusions resisted
95,000	Malware programs neutralized
160,000	Malicious websites blocked
32,000	Botnet C&C attempts thwarted
43M	Website categorization requests

Per Week



46M	New & updated spam rules
1,000	Intrusion prevention rules generated
1.8M	New & updated AV definitions
1.4M	New URL ratings
8,000	Hours of threat research globally

Total Database

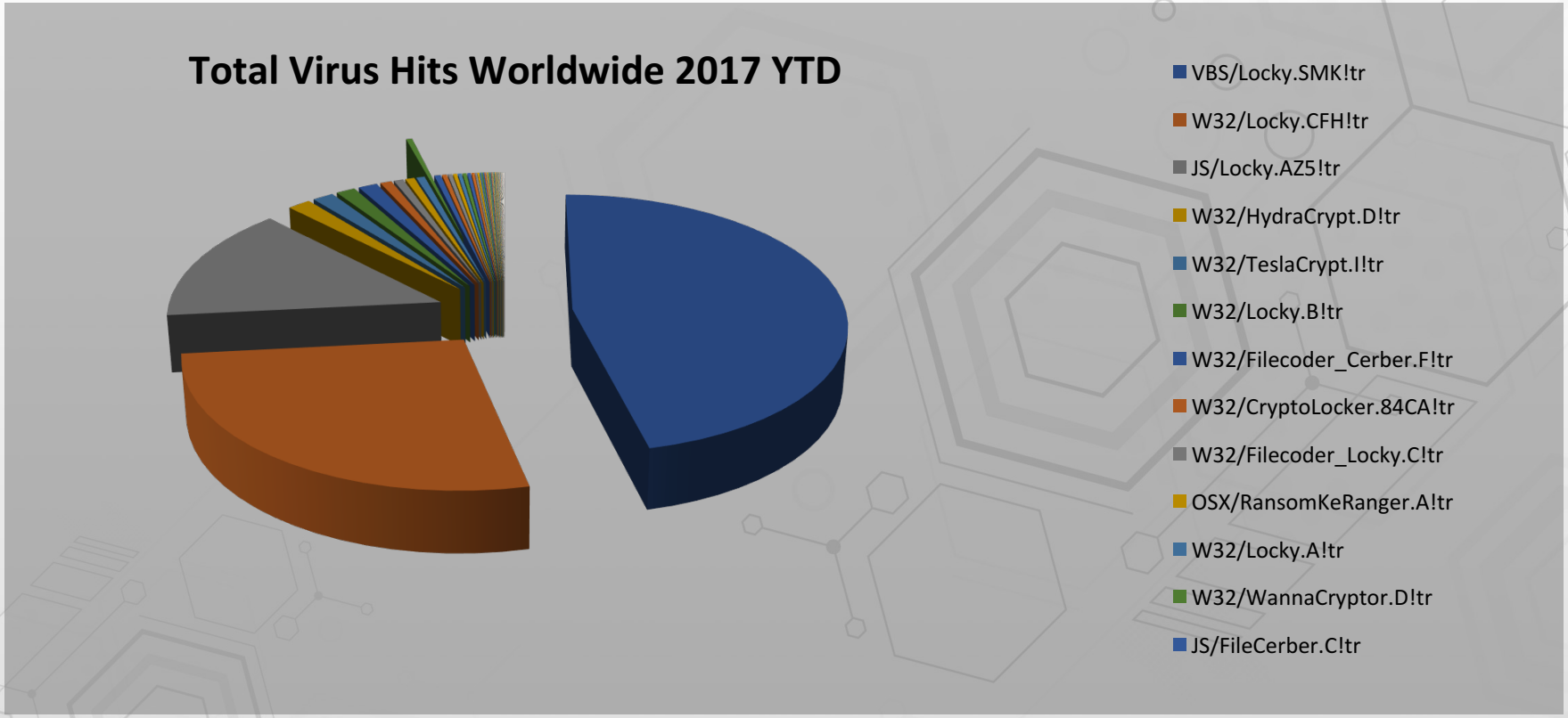
190	Terabytes of threat samples
18,000	Intrusion prevention rules
5,800	Application control rules
250M	Rated websites in 78 categories
262	Zero-day threats discovered

FortiGuard Labs
Global threat research and response

RansomWare

...napr. *vs* DDoS

Top Ransomware 2017



- Nárast Ransomware >150x za posledné 3 roky
- Locky je najaktívnejší ransomware
- Najbežnejšie útočené platformi – Adobe, MSOffice, Web sites…

FORTINET

Ransomware **WannaCry** z Piatku minulého týždňa

…WCry, WannaCry, WanaCrypt0r, WannaCrypt, or Wana Decrypt0r

200,000 obetí v 150 krajinách

....šíri sa prostredníctvom údajného zneužita NSA s názvom **ETERNALBLUE** (CVE-2017-0144), ktorý minulý mesiac unikol online hackerskou skupinou známu ako *The Shadow Brokers*. Služba ETERNALBLUE využíva **zraniteľnosť v protokole Microsoft Server Message Block 1.0 (SMBv1)**.

Zasiahnuté Microsoft producty:

- Windows XP
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8.1
- Windows Server 2012 and 2012 R2
- Windows RT 8.1
- Windows 10
- Windows Server 2016
- Windows Server Core installation option

Dôrazne odporúčame všetkým zákazníkom vykonať tieto kroky:

- **Apply the patch published by Microsoft** on all affected nodes of the network MS17-010
- Ensure that the Fortinet **AV and IPS inspections** as well as web filtering engines are **turned on and updated** to prevent the malware from being downloaded, and to ensure that web filtering is blocking communications back to the command and control servers.
- Isolate communication to UDP ports 137 / 138 and TCP ports 139 / 445.

Odporúčame tiež nasledujúce preventívne opatrenia:

- Establish a **regular routine for patching operating systems, software, and firmware on all devices.** For larger organizations with lots of deployed devices, consider adopting a centralized patch management system.
- **Deploy IPS, AV, and Web Filtering technologies**, and keep them updated.
- **Back up data regularly**. Verify the integrity of those backups, encrypt them, and test the restoration process to ensure it is working properly.
- **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.
- **Schedule your anti-virus and anti-malware programs to automatically conduct regular scans**.
- **Disable macro scripts in files transmitted via email**. Consider using a tool like Office Viewer to open attached Microsoft Office files rather than the Office suite of applications.
- **Establish a business continuity and incident response strategy** and **conduct regular vulnerability assessments**.

A ak ste to už schytali...

- **Isolate infected devices immediately** by removing them from the network as soon as possible to prevent ransomware from spreading to the network or shared drives.

- If your network has been infected, **immediately disconnect all connected devices**.

- **Power-off affected devices** that have not been completely corrupted. This may provide time to clean and recover data, contain damage, and prevent conditions from worsening.

- Backed up data should be stored offline. When an infection is detected, **take backup systems offline** as well and scan backups to ensure they are free of malware.

- **Contact law enforcement immediately** to report any ransomware events and request assistance.

Analýza sledovania ukazuje, že od 1. januára 2016 došlo **denne** v priemere viac ako **4 000 RansomWare útokov**.

DocuSign

Nitrianska Nemocnica

Je zodpovedná???

...a čo kritické infraštruktúry,

ICS/SCADA systémy,

Energetika, elektrárne, vodárne, plynárne...

sú pripravené???

Shadow Brokers Launches 0-Day Exploit Subscriptions for $21,000 Per Month

Monday, May 29, 2017 Swati Khandelwal


General
Data Protection
Regulation

General Data Protection Regulation

Právo jednotlivca

GDPR poskytuje jednotlivcom nasledujúce práva:

1. Právo byť informovaný
2. Právo na prístup
3. Právo na opravu
4. Právo na vymazanie
5. Právo obmedziť spracovanie
6. Právo na prenos údajov
7. Právo na námietku
8. Práva súvisiace s automatizovaným rozhodovaním a profilovaním.

General Data Protection Regulation™

Data protection by design and by default

V rámci GDPR máte všeobecnú povinnosť implementovať technické a organizačné opatrenia, aby ste preukázali, že ste zohľadnili a integrovali ochranu údajov do vašich spracovateľských činností.

General Data Protection Regulation

GDPR je legislatíva o bezpečnosti údajov a *nie kybernetickej bezpečnosti*

Security technológie môžu ale určite pomôcť a niekedy sú potrebné na to, aby ste sa udržali v súlade... ;)

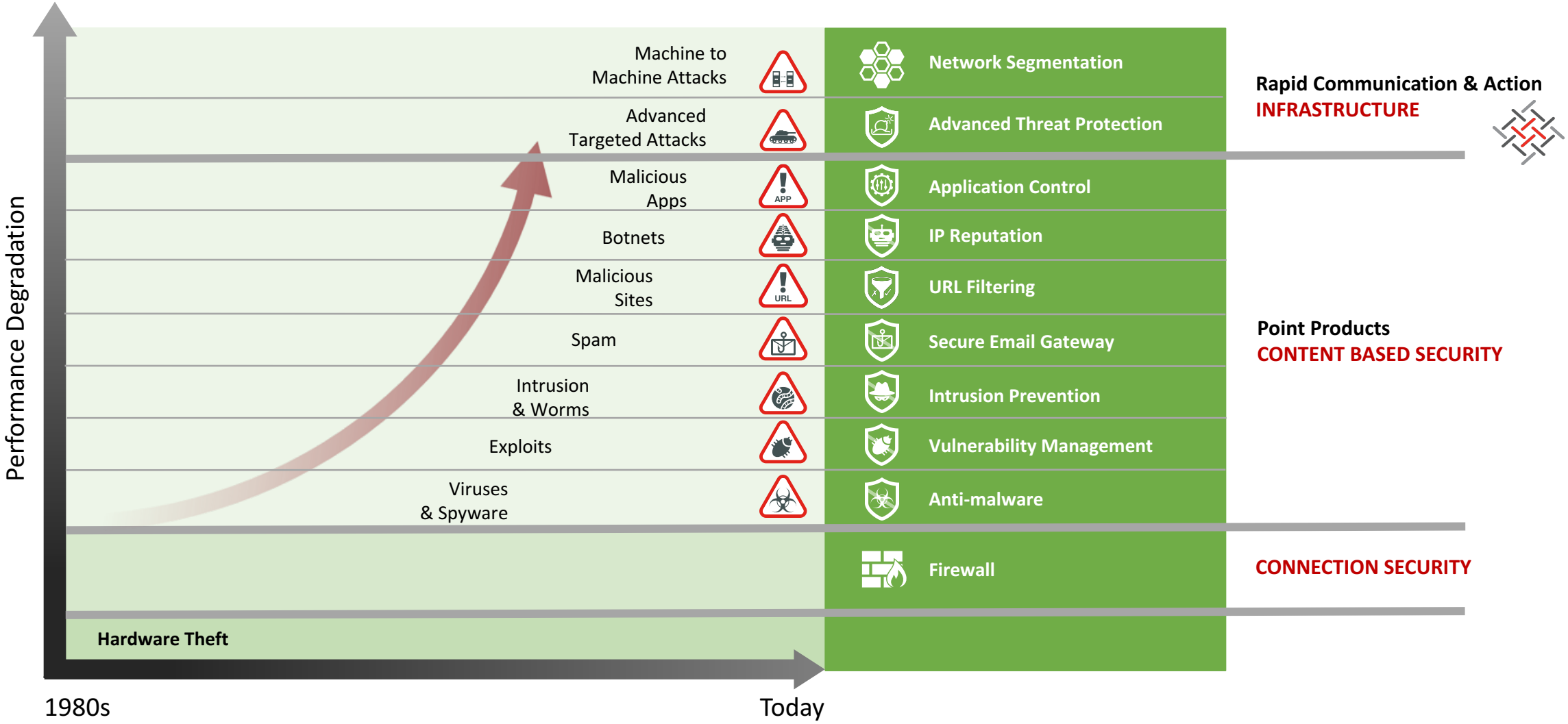
Článok 25: Ochrana údajov by design and by default

Článok 32: Bezpečnosť pri spracovaní

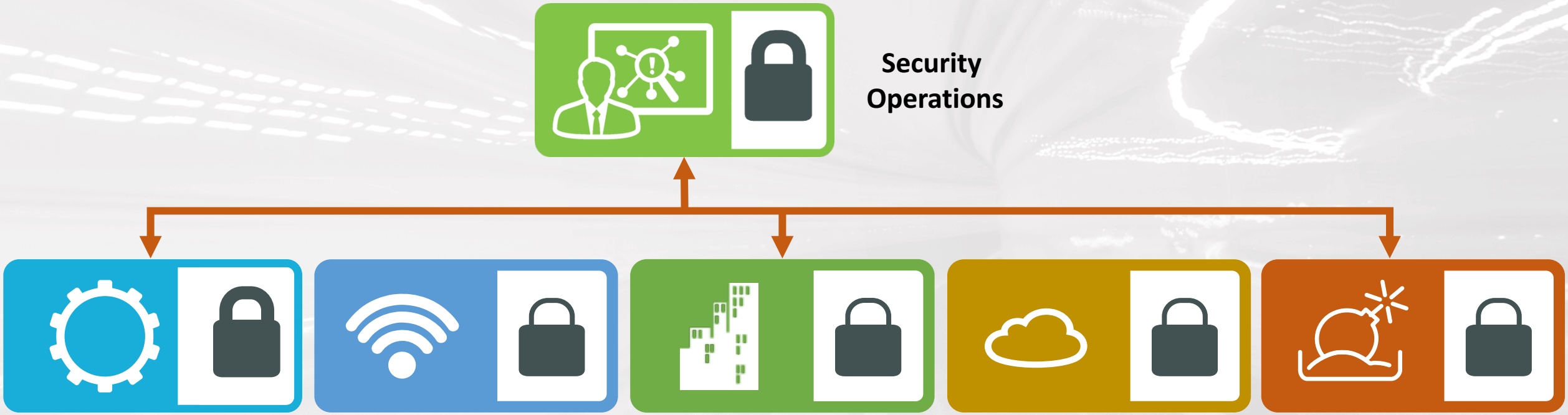
Články 33 a 34: Oznámenie o narušení/úniku [napr. SIEM...?]

Článok 35: Hodnotenie vplyvu ochrany údajov

Zastavenie Pokročilých Hrozieb vyžaduje rýchlu komunikáciu Bezpečnostných prvkov



The Elements of the Fortinet Security Fabric



Technology Integration and Collaboration

APPLICATION SECURITY

- FortiMail
- FortiWeb
- FortiADC
- FortiDDoS
- FortiWAN
- FortiCache

SECURE ACCESS

- FortiAP
- FortiWiFi
- FortiSwitch
- FortiAuthenticator
- FortiToken
- FortiExtender

ENTERPRISE FIREWALL

- FortiGate
- FortiWiFi

CLOUD SECURITY

- ForitGate VM (Virtual FW)
- FortiGate VMX (SDN Virtual FW)
- FortiGate VM for Public Cloud
  - AWS
  - Microsoft Azure
  - OpenStack

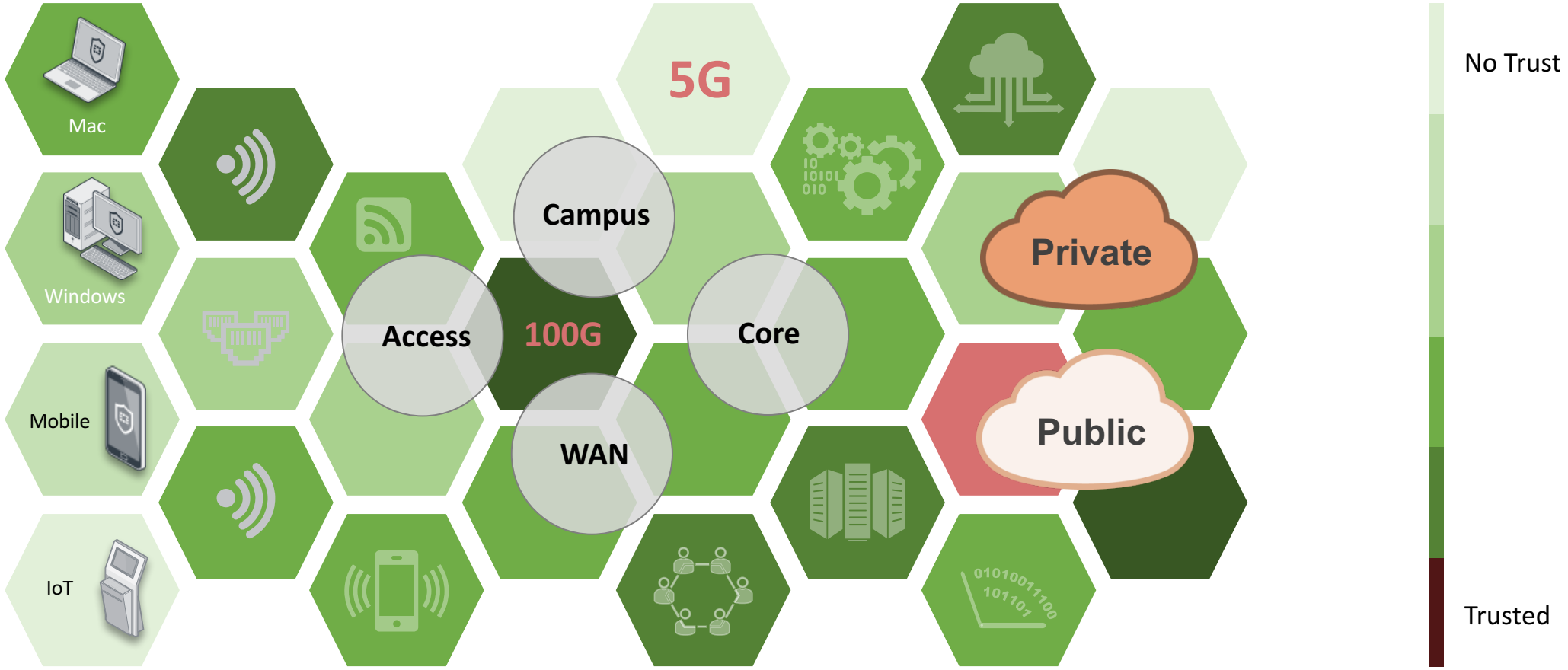
ADVANCED THREAT PROTECTION

- FortiSandbox
- FortiMail
- FortiWeb
- FortiClient

SECURITY OPERATIONS

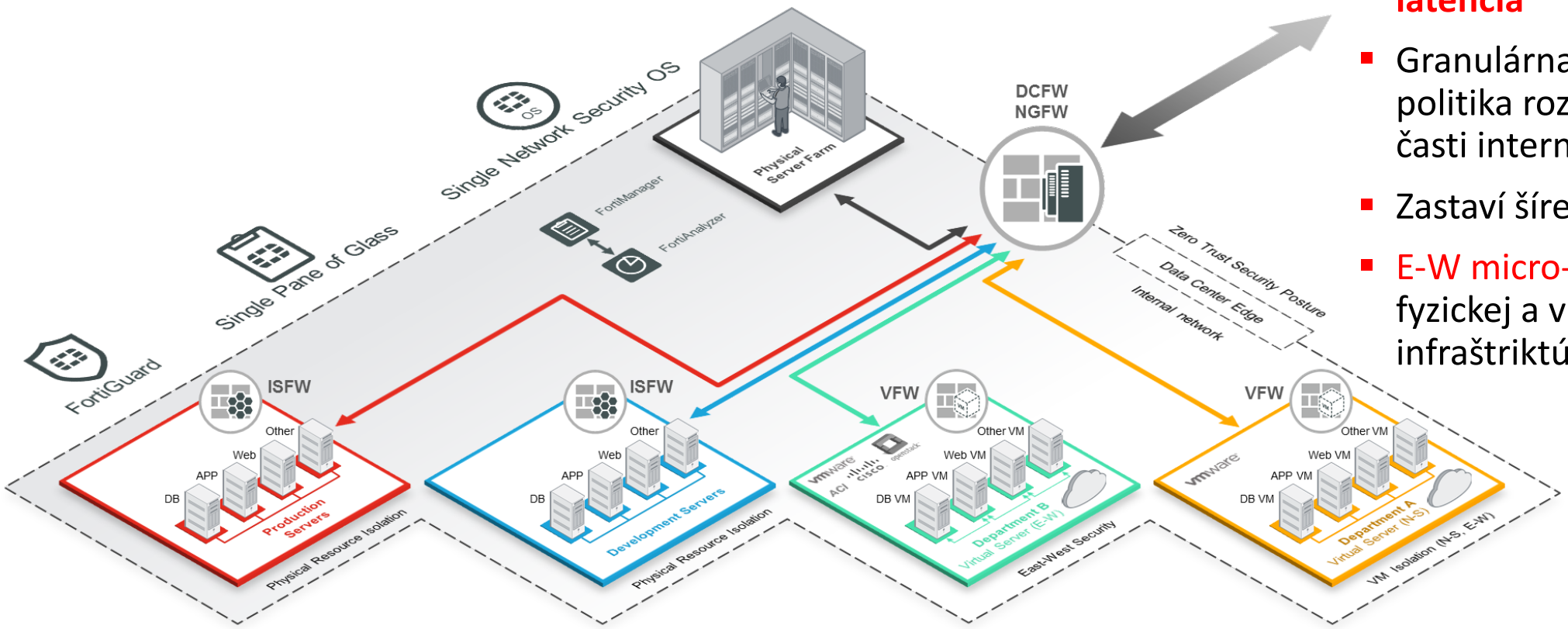
- FortiManager
- FortiAnalyzer
- FortiSIEM

Dnešná sieť je Bezhraničná - Architektúra Segmentácie Siete je Nevyhnutná



Segmentácia v DataCentre

Kľúčové faktory – Súlad s požiadavkami, Riadenie rizík, Zero Trust Security



- **Vysoká priepustnosť**, vysoká hustota portov, **veľmi nízka latencia**
- Granulárna bezpečnostná politika rozdeľuje a segmentuje časti internej siete
- Zastaví šírenie škodlivého kódu
- E-W micro-segmentácia via fyzickej a virtuálnej infraštriktúry

ISFW Technologická Požiadavaka No.1: VÝKON

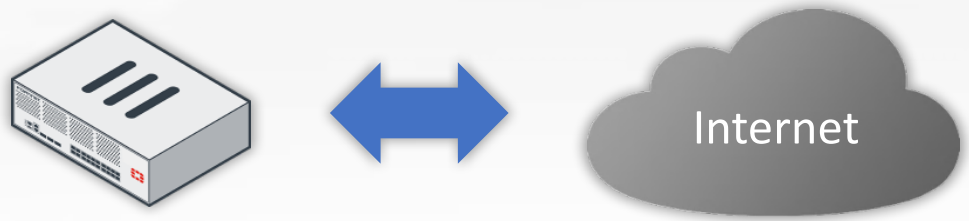
Internal Segmentation Firewall (ISFW)

Interfaces → 10G, 40G & 100G

No. of Ports → 8 to 48GbE/10GbE

Throughput → 10 Gbps to 100+ Gbps

Perimeter Firewall (NGFW)



Ports Speeds → 1G, 10G

No. of Ports → 2 to 12

Throughput → Mbps to Gbps

Riešenie FORTINET

FortiSandbox

- Zkrátenie doby od nakazenia k identifikácii
- Historické súbory
- Podateľne

Integrácia s:

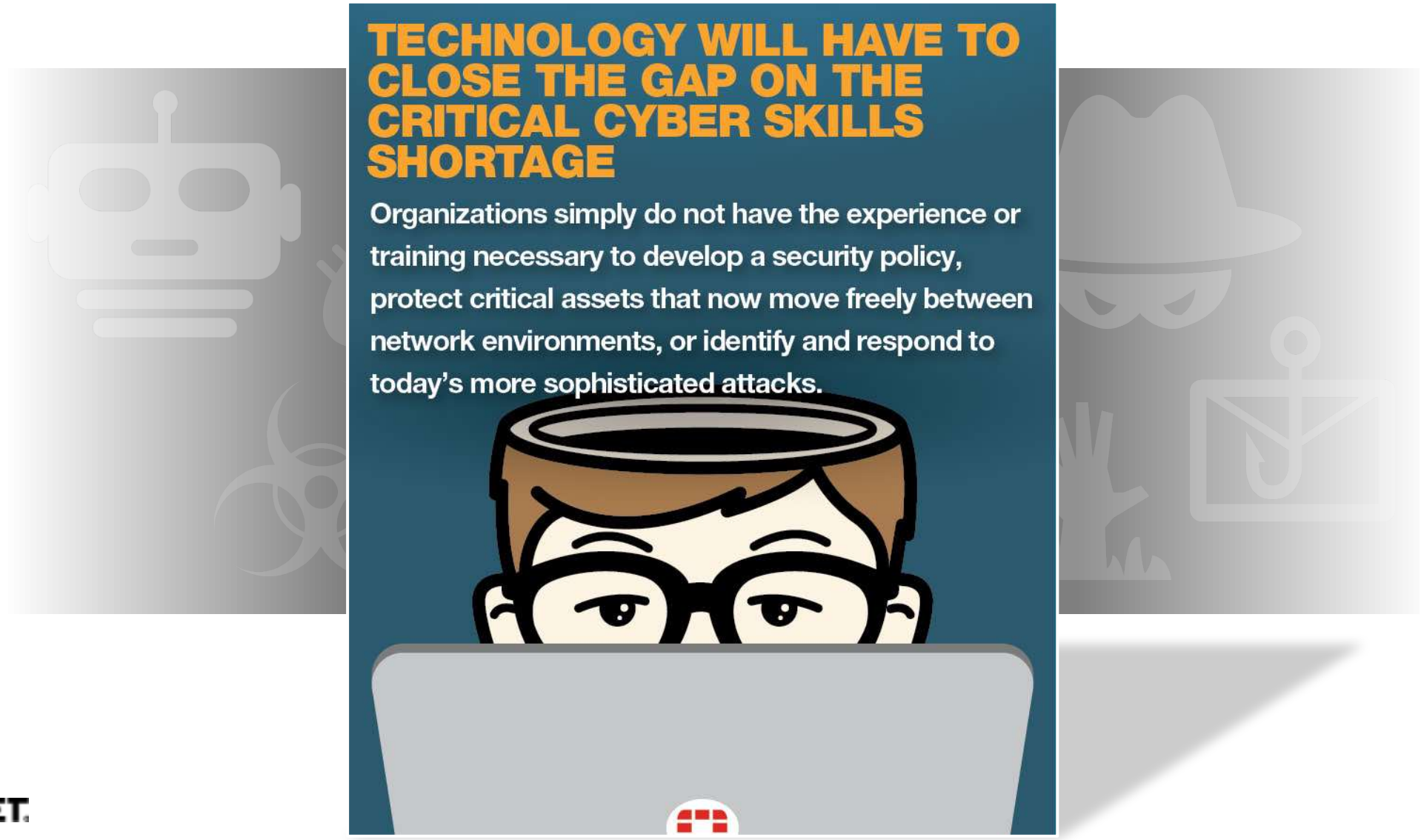
- Mail bránami
- Firewallmi (NGFW)
- WebAplikačnými Firewallmi
- Endpointami

Threat Predictions - 2017

RANSOMWARE WAS JUST THE GATEWAY MALWARE

We expect to see very focused attacks against high-profile targets, such as celebrities, political figures, and large organizations. Automated attacks will introduce an economy of scale to ransomware that will allow hackers to cost-effectively extort small amounts of money from large numbers of victims simultaneously, especially by targeting IoT devices.

Threat Predictions - 2017



Ďakujem za pozornosť!


FORTINET