

KYBERNETICKÁ BEZPEČNOST

Výzvy a příležitosti pro ISP

Martin Fišer

Key Account Manager

SP/MSSP



KAM KRÁČÍ

TELEKOMUNIKAČNÍ

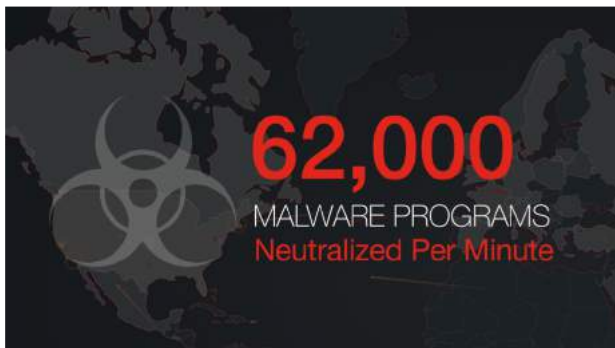
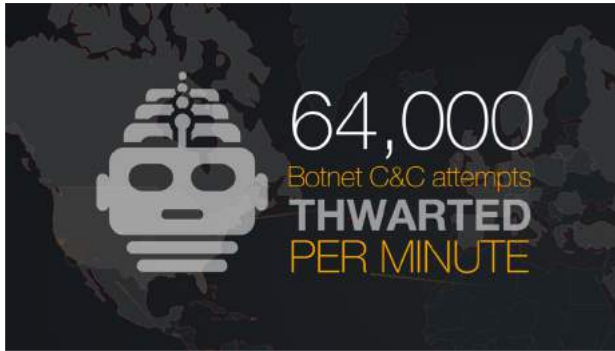
SÍTĚ

13. 9. 2018

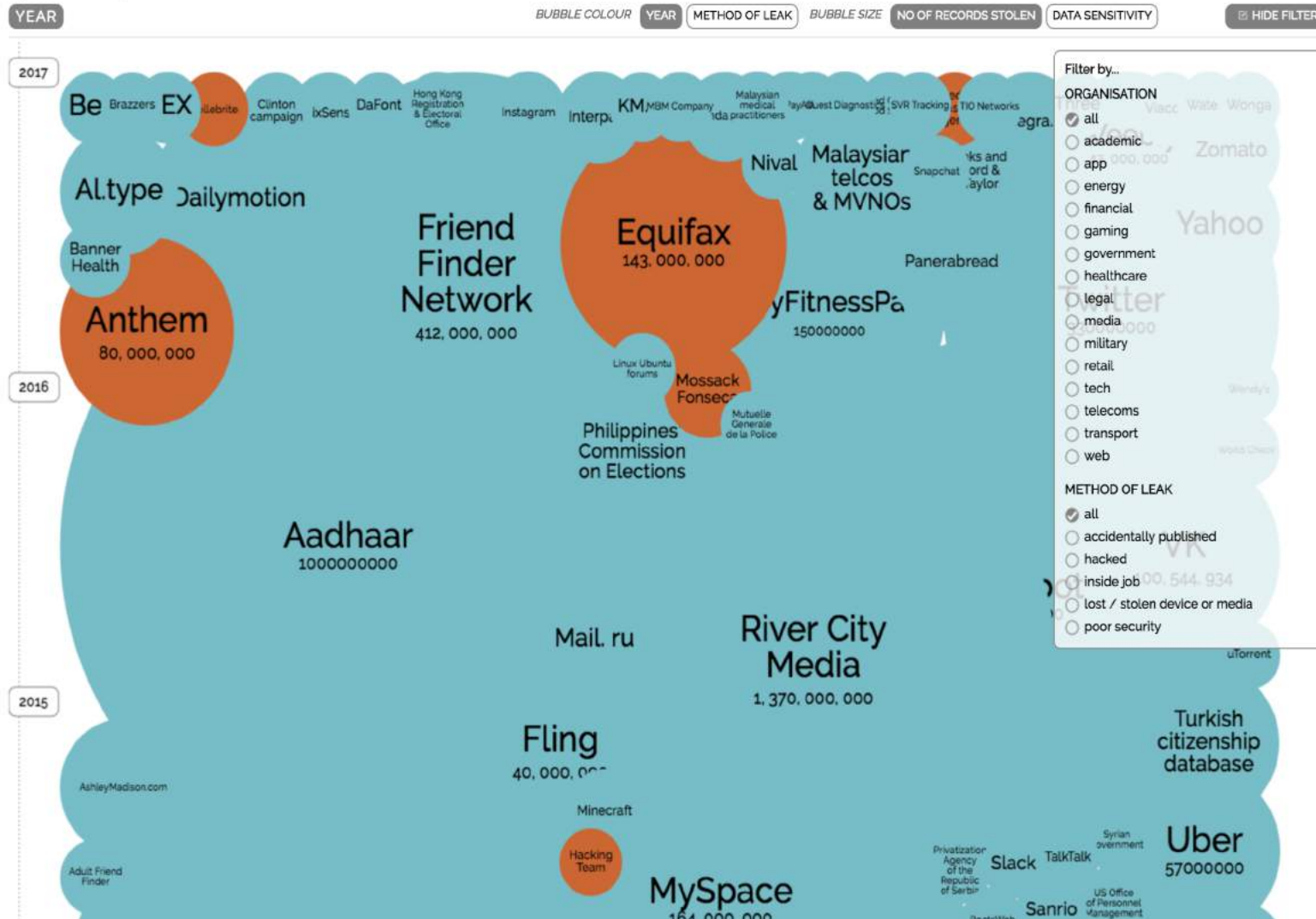
PLZEŇ

PARKHOTEL PLZEŇ****

FortiGuard by the numbers



(updated 8th May 2018)



THE BIGGEST DATA BREACHES OF 2017

Fakta

Ransomware within malware incidents

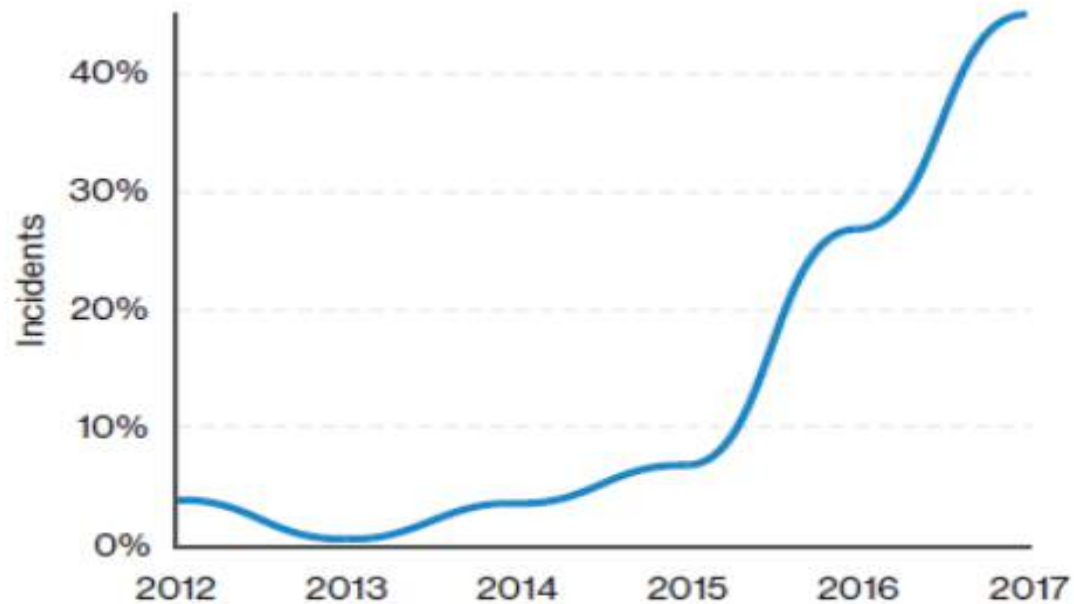


Figure 15. Ransomware within malware incidents over time

Frequency of malware vectors

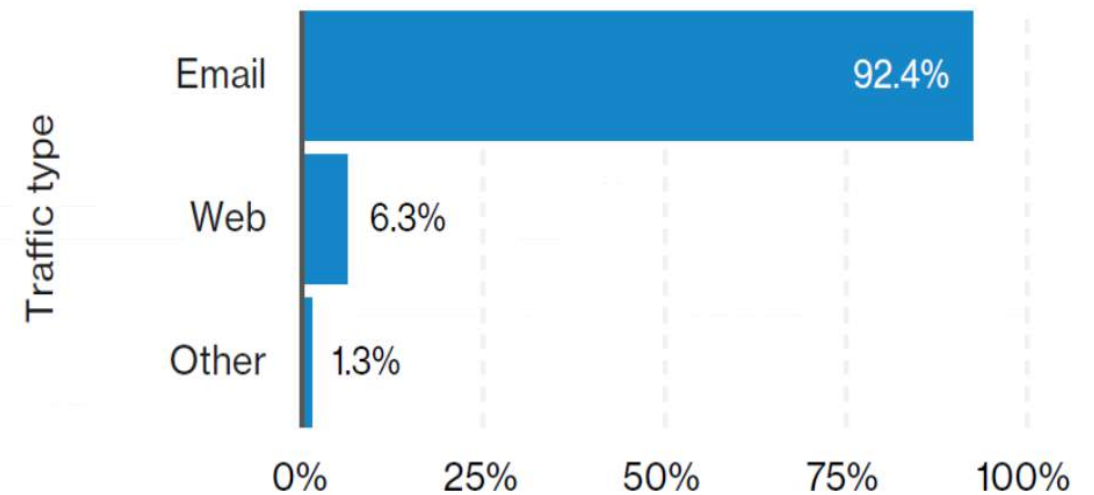
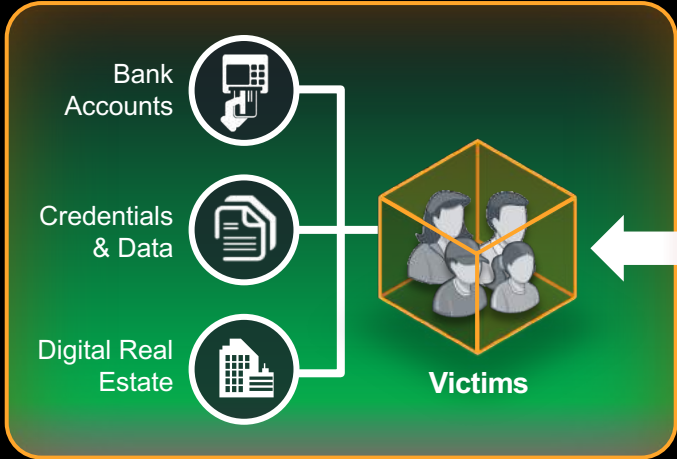
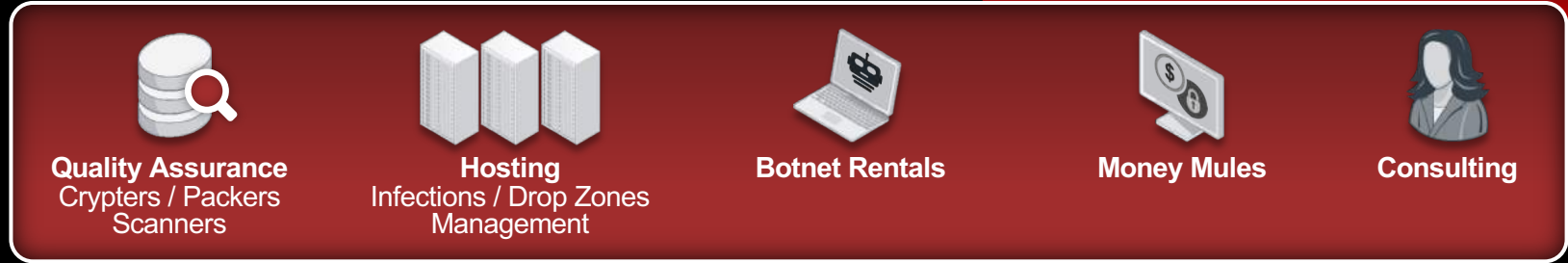


Figure 21. Frequency of malware vectors within detected malware (n=58,987,788)

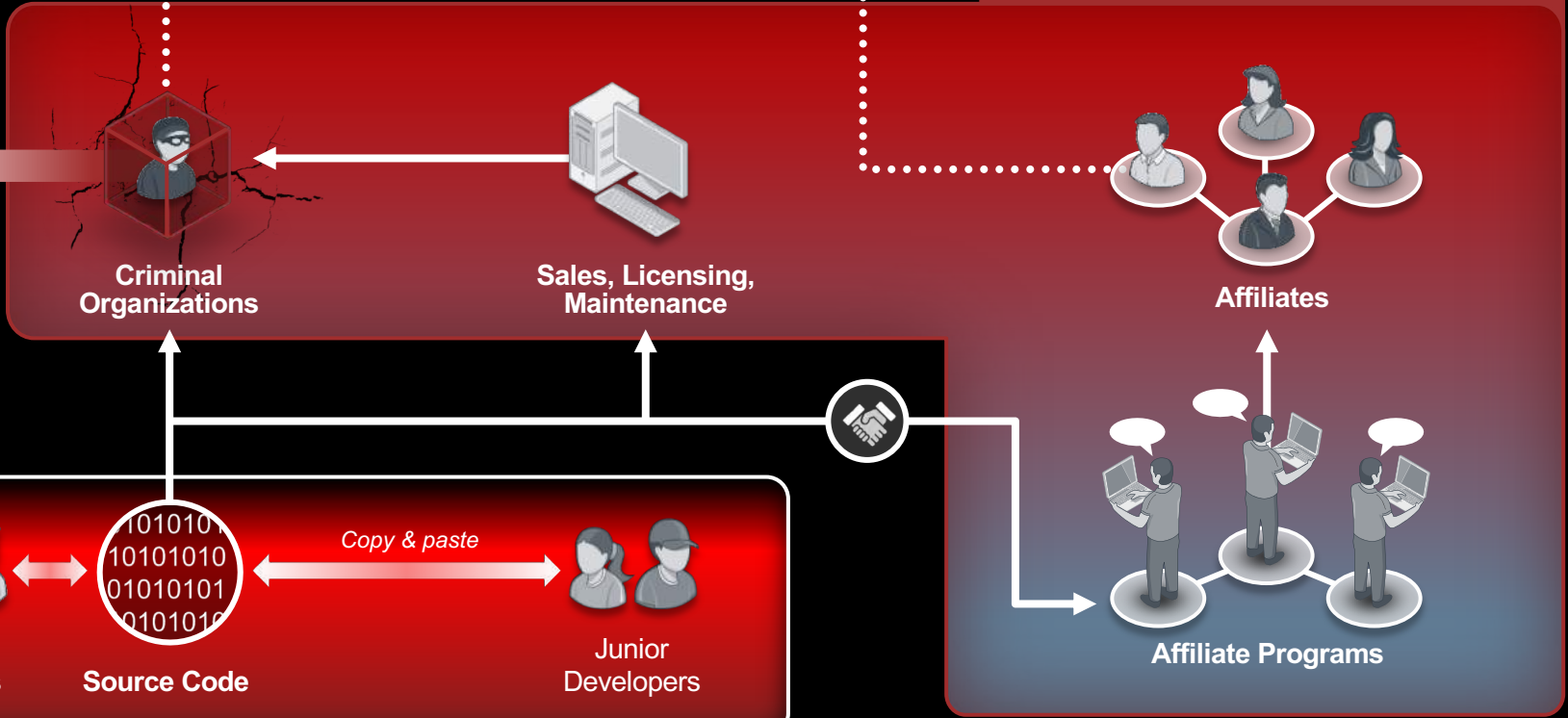
Source: Verizon lab DBIR report 2018
<https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

HACKERS s.r.o.

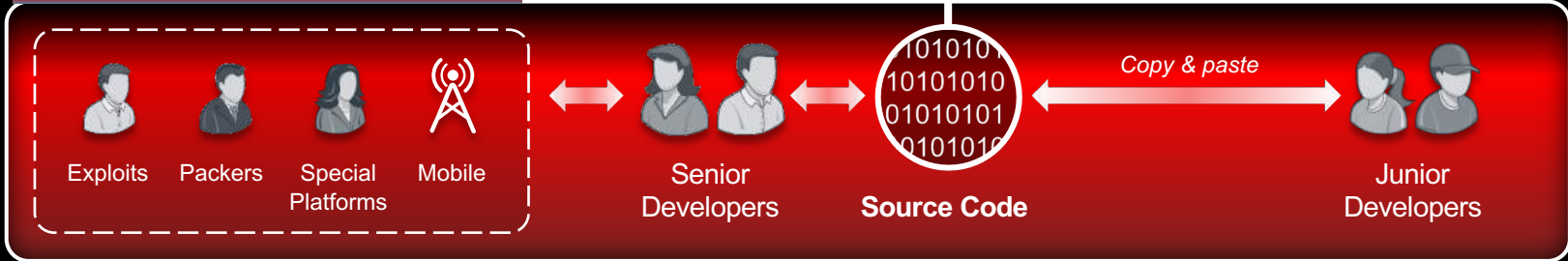
CRIME SERVICES ENABLERS



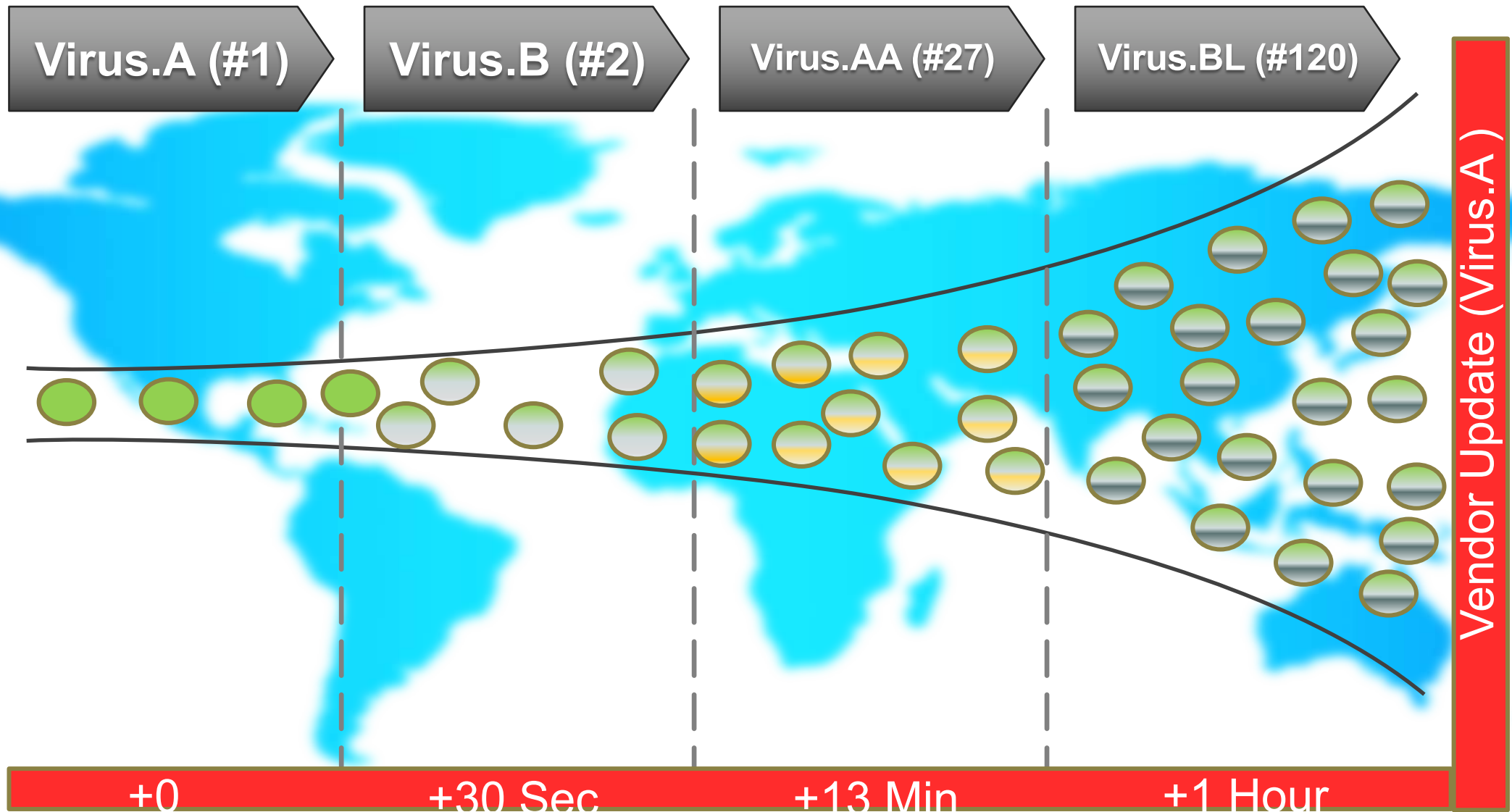
COMPOUNDED CYBERCRIME



CRIMEWARE PRODUCERS



Virus Lifecycle to Scale



2017
\$512Mld. tržby
+15% !!!

Global Drugs Trade \$652B In Revenue

Table A. Global Drug Market Annual Values (US\$)

Market	Value
Cannabis	\$183 billion to \$287 billion
Cocaine	\$94 billion to \$143 billion
Opiates	\$75 billion to \$132 billion
ATS	\$74 billion to \$90 billion
Global Total	\$426 billion to \$652 billion

(Source: [Global Financial Integrity](#))

THE GLOBAL 500: THE TOP 10

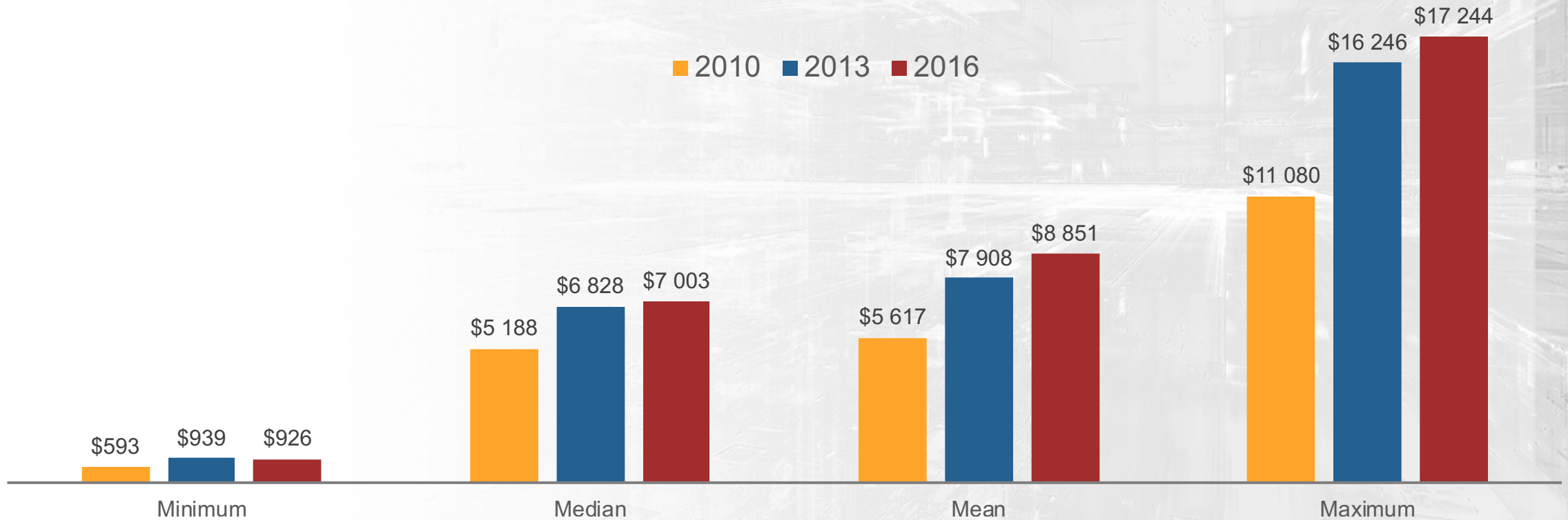
THE TOP 10

REVENUES (\$M)

1	Walmart	\$485,873
2	State Grid	\$315,199
3	Sinopec Group	\$267,518
4	China National Petroleum	\$262,573
5	Toyota Motor	\$254,694
6	Volkswagen	\$240,264
7	Royal Dutch Shell	\$240,033
8	Berkshire Hathaway	\$223,604
9	Apple	\$215,639
10	Exxon Mobil	\$205,004

Money money money

Cena 1min neplánovaného výpadku



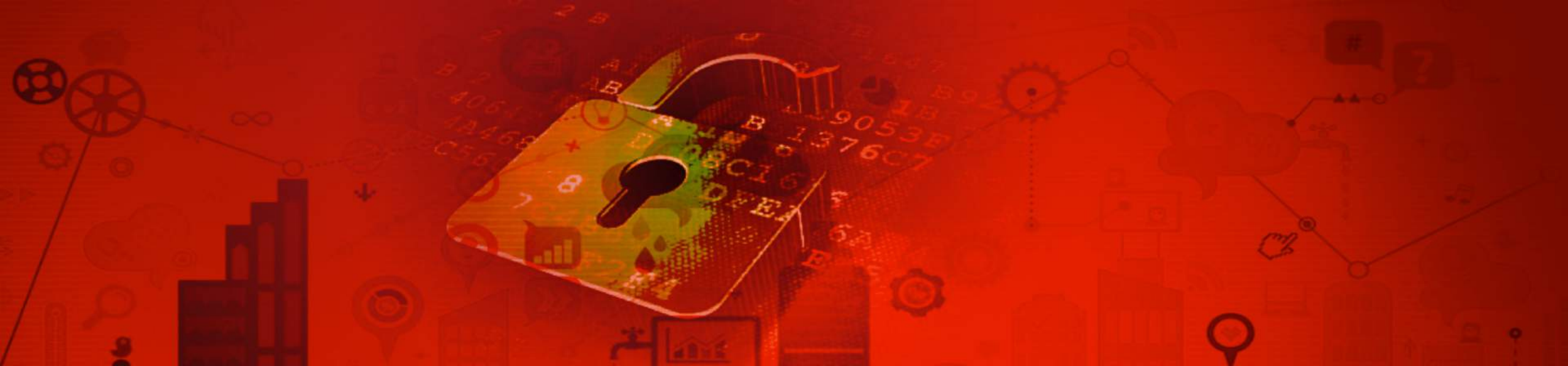
Svět se mění



DX

je integrace digitálních technologií do všech oblastí podnikání, což vede k zásadním změnám v tom, jak fungují podniky a jakou přinášejí hodnotu zákazníkům

[Digital Transformation]

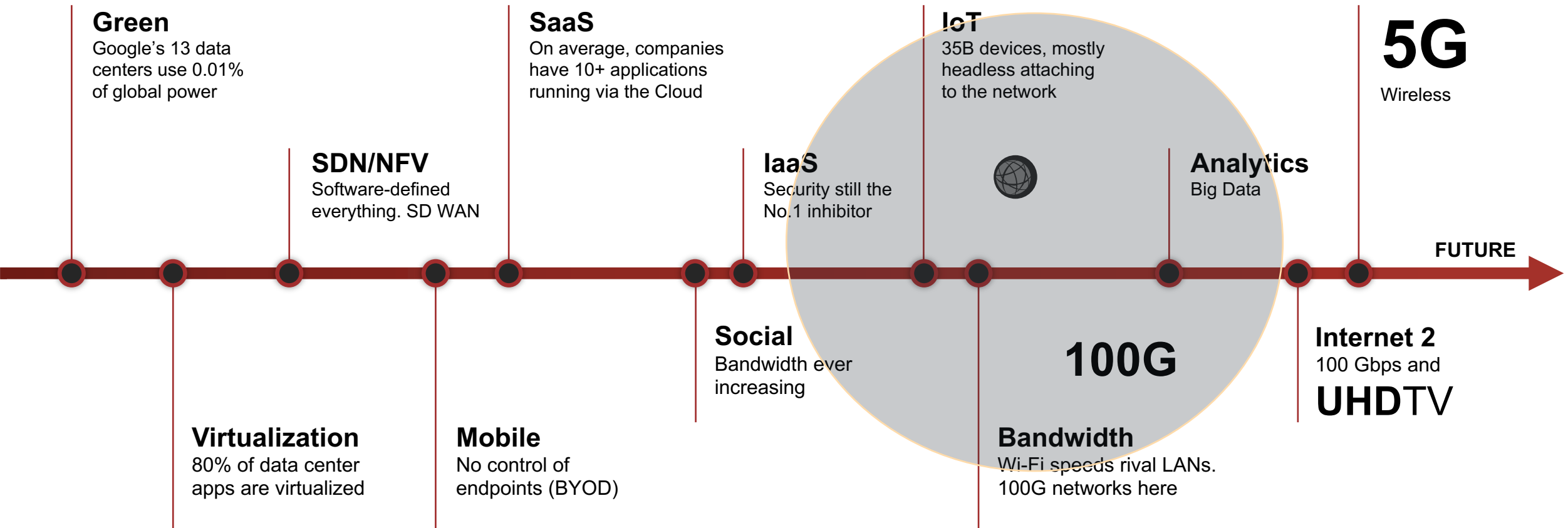


SX

je integrace zabezpečení do všech oblastí digitálních technologií, což vede k vytvoření architektury, která poskytuje ochranu dat a průběžné hodnocení důvěryhodnosti

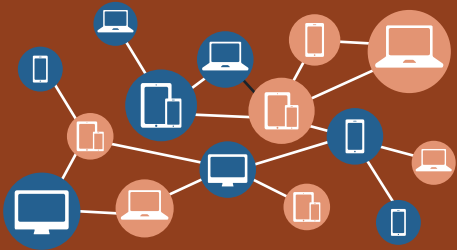
[Security Transformation]

VNĚJŠÍ INFRASTRUKTURA - Konstantní změny



ZMĚNY GLOBÁLNÍ

25B



connected things by 2020

6.5M



New Wi-Fi devices ship everyday

Globally, mobile data traffic will reach

24.3 Exabytes



per month by 2019

 76% of users think

Public Wi-Fi is not secure

62% still use it 

84%

of users say that bad Wi-Fi has kept them from doing their job



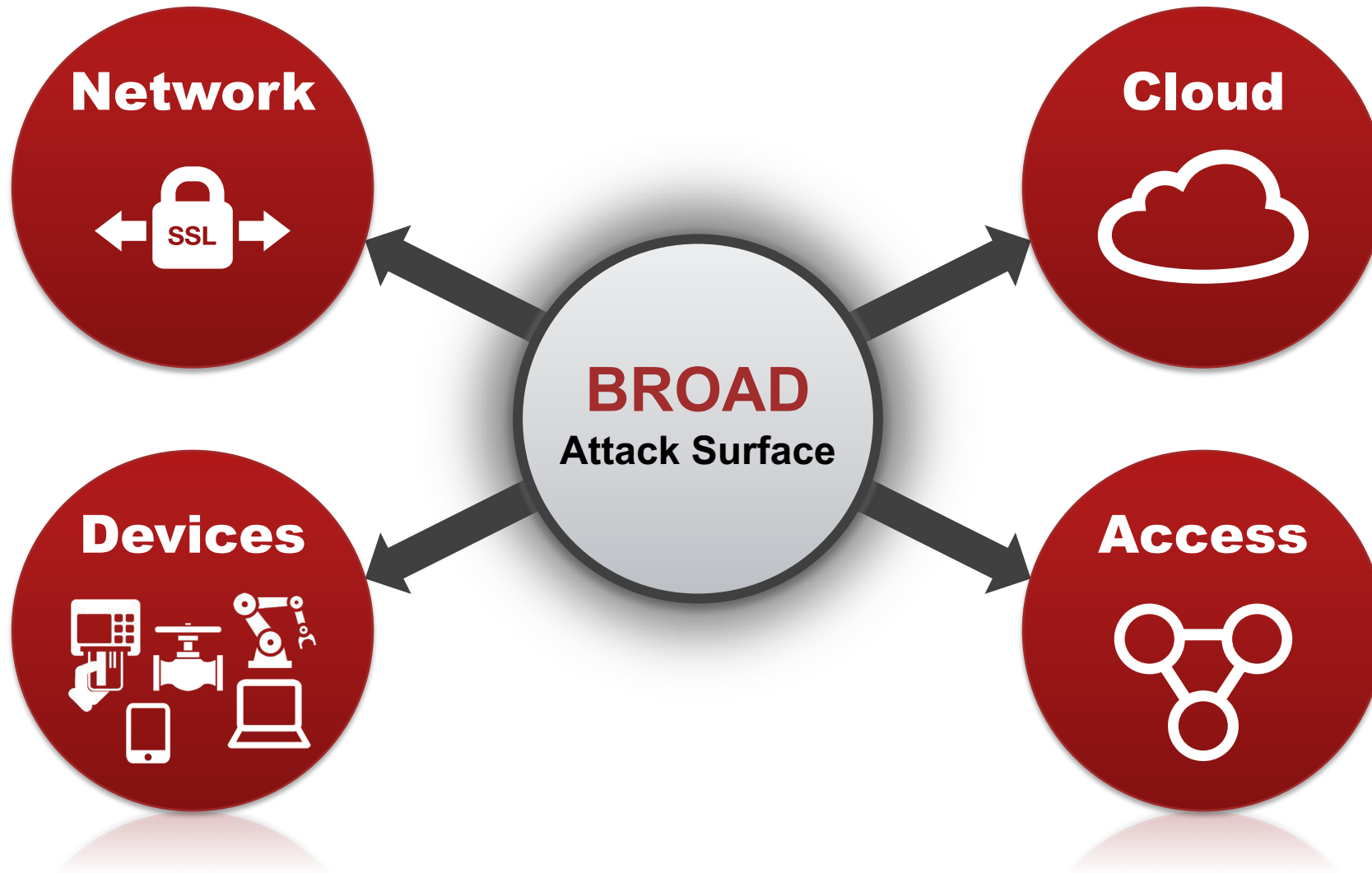
The average smartphone will generate

4GB

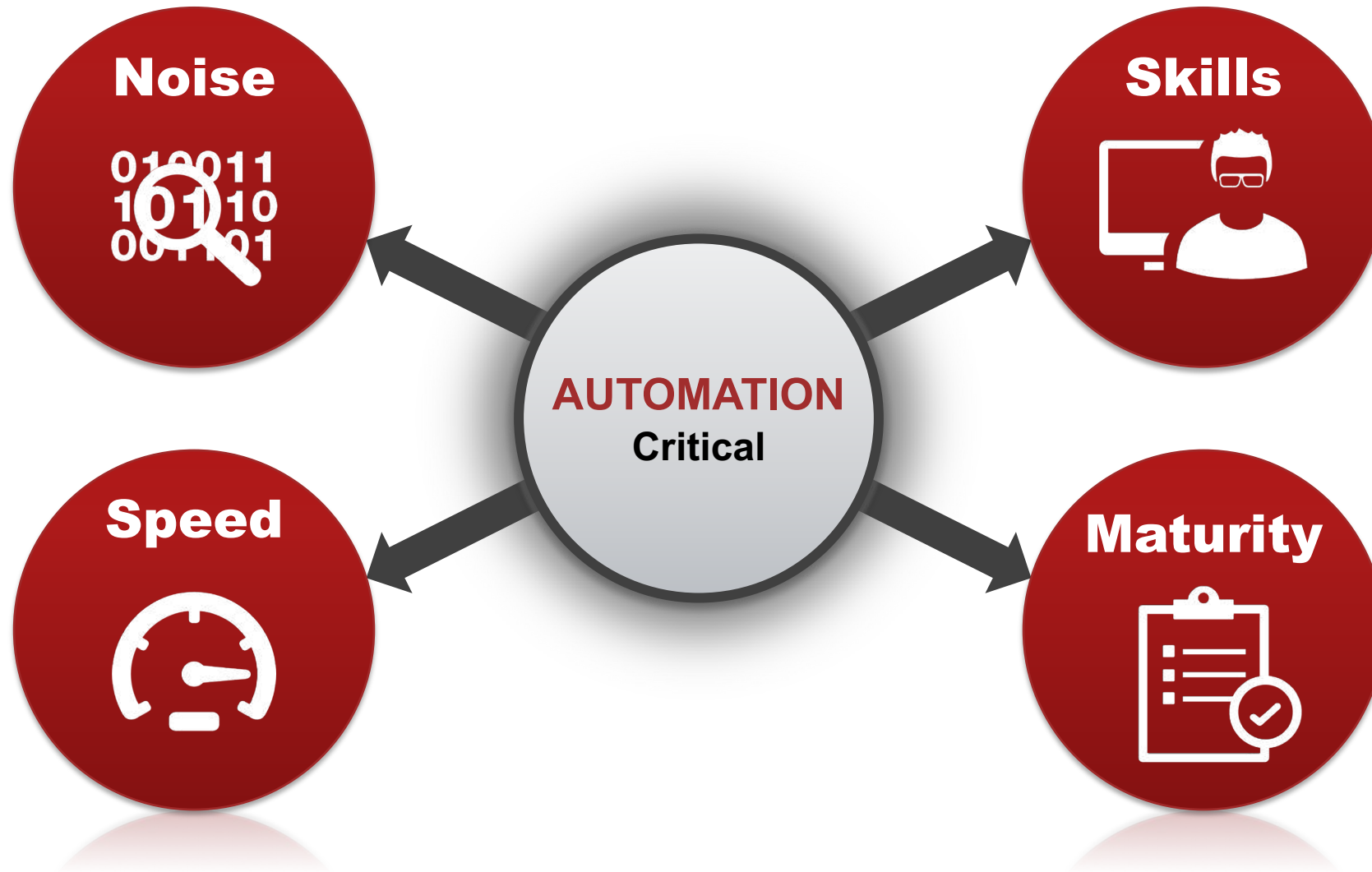
of traffic per month by 2019

SOURCE: Cisco VNI Mobile, Dell'Oro Group, Wireless LAN Report Five Year Forecast 2014-2018, Gartner, Gartner Strategy Analytics, Morgan Stanley Research

Neviděl někdo pana Perimetra?



Rychle se měnící pokročilé a neznámé hrozby a nedostatek zdrojů a odbornosti na trhu



Změna požadavků zákazníka

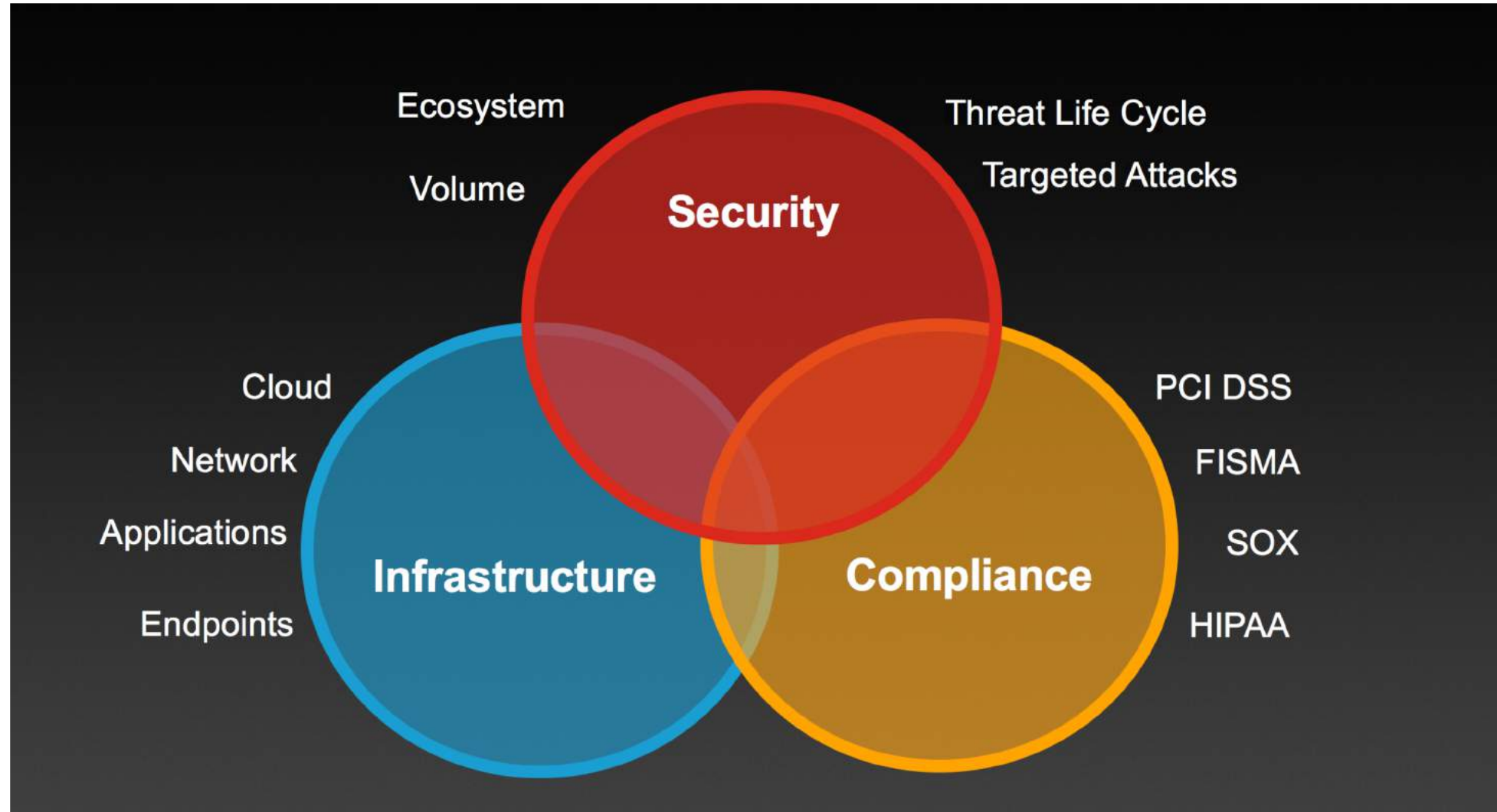
Kapitulace na domobranu

ZÁKAZNÍK

- **Konektivita** - stále více
- **Připojení** - kdykoliv, odkudkoliv a z čehokoliv
- **Investice** - Změna Capex na Opex
- **No IT Crowd** – nedostatek kvalifikovaných pracovníků
- **Virtuální adresa** - BYOD, Home office, Cloud, Host WiFi

- **Standardní CPE model je nedostačující**

NOVÉ NÁROKY NA IT



Nová pravidla a povinnosti

Ve městě je nový šerif

ZMĚNY V LEGISLATIVĚ

- Kybernetický zákon
- Anti hazard
- IP adresa jako osobní údaj
- GDPR (General Data Protection Regulation)
- Compliance reports (PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls)
- Útočníky nezajímá jestli jste dostatečně „Compliance“

ZMĚNY VE SVĚTĚ ISP

■ DŘÍVE

- » Hlas, Data, Internet
- » Minuty, tarifkace,
- » Rychlost, bajty, FUP, SLA

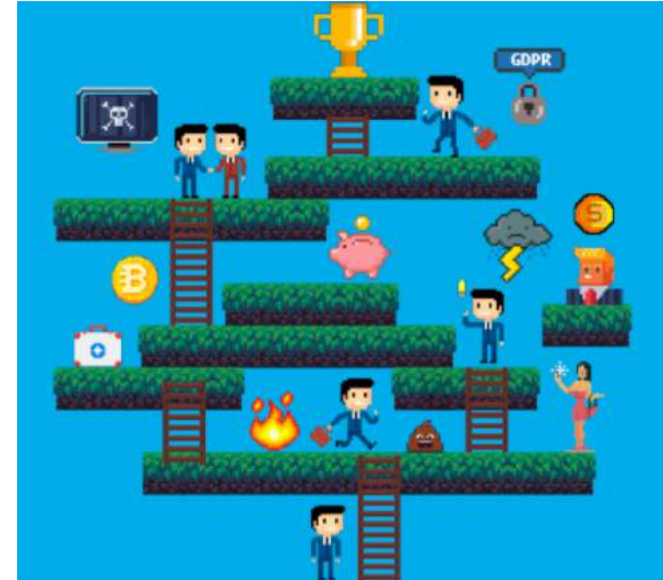
■ NYNÍ

- » CLOUD
- » BYOD
- » IPTV
- » Video On Demand
- » Data BackUp and restore
- » Smart Home
- » VPN služby
- » Šifrovanou komunikaci
- » Security

■ ISP?

- » TCS
- » CSP
- » MSP
- » VASP
- » MSSP

Telecommunication Services Provider
Communication Services Provider
Managed Services Provider
Value Added Services Provider
Managed Security Services Provider



ISP jako terč





• TYPY ÚTOKŮ

- **Necílený útok**
 - Spam
 - Amplifikační útok na VoIP, NTP, DNS
- **Cílený útok**
- **Hybridní (kombinovaný) útok**
- **Útok na kritickou infrastrukturu**

▪ PROČ?

- » **Výpočetní výkon**
- » **Kompromitace**
- » **Konkurence**

• Co je cílem?

- **Znepřístupnění služby (Dos/DDoS)**
- **Útok na zranitelnost služby (L3- L7)**
- **Zneužití špatného zabezpečení (POP)**
- **Útok na uživatele (L8)**

• KAM SE MÍŘÍ

- **Konektivita**
- **Data centrum**
- **Služby (web, dns, mail, voip, iptv)**
- **Databáze**
- **Přístupové body sítě (CPE router, AP, uzly)**
- **Na zákazníka**

ISP jako dodavatel



MSSP PORTFOLIO

Device Management
Log collection and retention
Basic Monitoring Services
Vulnerabilities scanning

Unified Threat Management
Vulnerabilities management
Incident Response/investigation
Governance, Risk & Compliance
Identity and access management

TRADITIONAL MSS

ADVANCED MSS

MSSP PORTFOLIO – cross sale

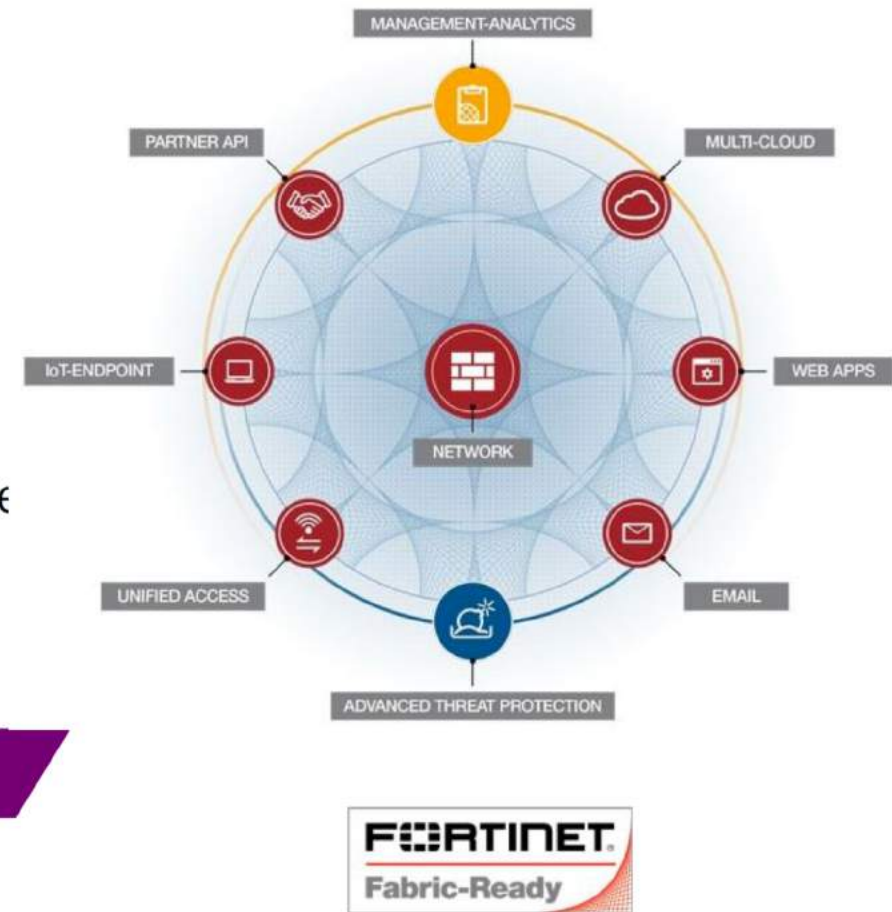
Unified Threat Management
Vulnerabilities management
Incident Response/investigation
Governance, Risk & Compliance
Identity and access management
Device Management
Log collection and retention
Basic Monitoring Services
Vulnerabilities scanning

Advanced threat management
Big data security analysis
MSS Cloud services
Managed Detection and Response
Forensic and malware analysis

INTELLIGENT MSS

ADVANCED MSS

TRADITIONAL MSS



Telefónica is “not just a reseller”.

We have a broad portfolio of security services



Comms Security



Anti-DDoS



Clean Pipes



IT Security



Web Security Gateway



Clean Email



Secure Mobile Device Mgmt



Secure VDC



Security Mgmt & Governance



Sandas



Sandas GRC



Security Monitoring



Data Management



Cybersecurity Services



CyberThreats



Vamps



Faast



Metashield



Tacyt



Sinfonier



Path6



Identity & Privacy



SmartID



mobile connect



Latch



SealSign



A stále je co nabídnout – budoucnost MSSP

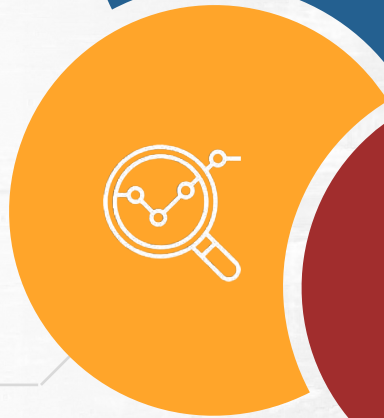
**Regulatory
Compliance**



**Incident
Response**



**Advanced
Analytics**



**Threat
Intelligence**

PROČ FORTINET

PROČ FORTINET

- **Fortinet je v segmentu ISP od roku 2002**
 - » 1. multifunkční HW, přes 440 patentů, od startu multitenantní prostředí
- **Security Fabric ecosystem je MSS Ready**
 - » Prokazatelná úspora OPEX/CAPEX
 - » Broad/Automation/Integration a Security partners Ready Program
 - » Ideální platforma pro Value added services a škálovatelnost služeb
- **Partnerský vztah a nejen dodavatel**
 - » Školení
 - » Obchodní i technická podpora
 - » Motivační system spolupráce

Základní požadavky ISP na platformu

- **VÝKON**
- **VARIANTNÍ A SNADNÉ NASAZENÍ**
- **MULTITENANTNOST**
- **AUTOMATICKÉ PROCESY**
- **OTEVŘENOST SYSTÉMU VŮČI JINÝM VÝROBCŮM**
- **SAMOOBSLUŽNÝ PORTÁL**
- **CENTRÁLNÍ A PŘEHLEDNÝ MANAGEMENT**
- **ŠKÁLOVATELNOST SLUŽEB**
- **REPORTING A INTERNÍ AUDIT**

VÝKON

Security Processors (SPU's)



Accelerates Network Traffic

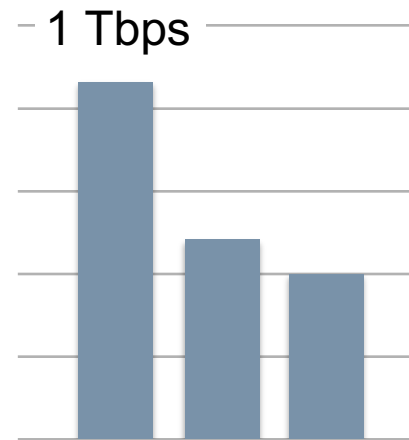


Accelerates Content Inspection

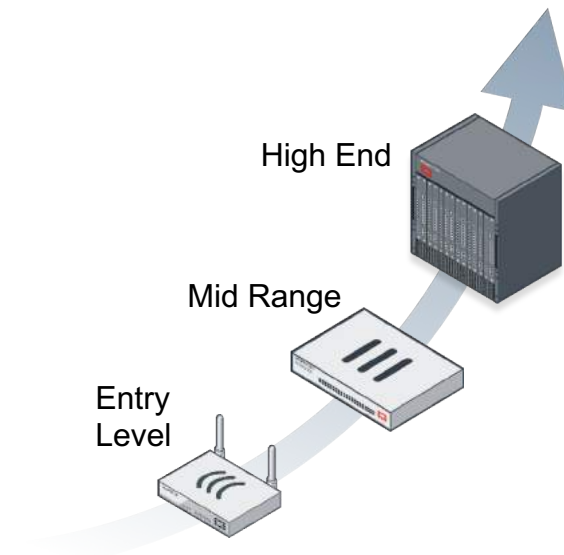


Optimized Performance for Entry Level

Parallel Path Processing



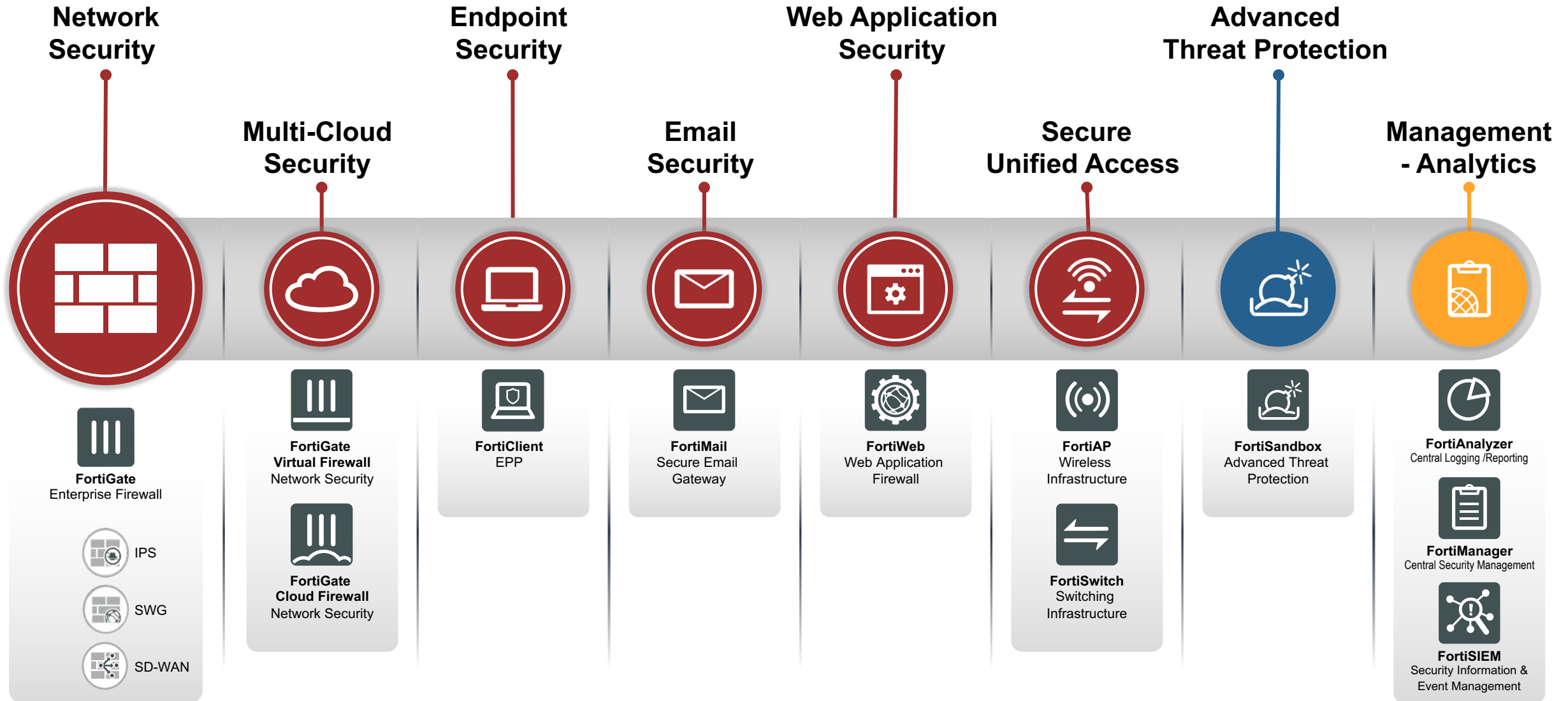
Comprehensive Range





FortiGate FortiWiFi Models	30E, 50E 60E	70D, 80D, 90D, 90E, 92D	100D	200D	300D 400D 500D	600D 800D 900D	1000 2000 3000	FG-5000 Series	FG-VM Series
Hardware									
Product Range / Form Factor	Entry / Desktop	Entry / Desktop-2 RU	Mid Range / 1 RU	Mid Range / 1- 2 RU	Mid Range / 1 RU	Mid Range / 1 RU	High End / 2-3 RU	High End / 3-13 RU	-
GE Interfaces	5-10	4 - 78	8 - 40	18 - 88	10 - 18	16-34	18 - 34	2 - 28	Refer to Data Sheet
10 GE	-	-	-	-	-	0 - 2	2 - 48	2 - 112	Refer to Data Sheet
40 GE	-	-	-	-	-	-	4	-	-
100 GE	-	-	-	-	-	-	6	2	-
Capacity									
Supported APs (Tunnel Mode)	2 - 5	16	32	64	256	512	1,024	14,336 (1,024/blade)	32 - 1,024
Supported APs (Total)	2 - 20	32	64	128	512	1,024	4,096	Up to 57,344 (4,096/blade)	64 - 4,096
Max number of SSIDs	32	32	256	256	256	256	1,024	Up to 14,336 (1,024/blade)	32 - 1,024
Max CAPWAP throughput	250 Mbps - 1.9 Gbps	260 Mbps - 2.2 Gbps	1.2 Gbps	1.8 Gbps	5.4 - 10 Gbps	5.5 Gbps - 11 Gbps	11 Gbps - 22 Gbps	Refer to Datasheet	Host dependent

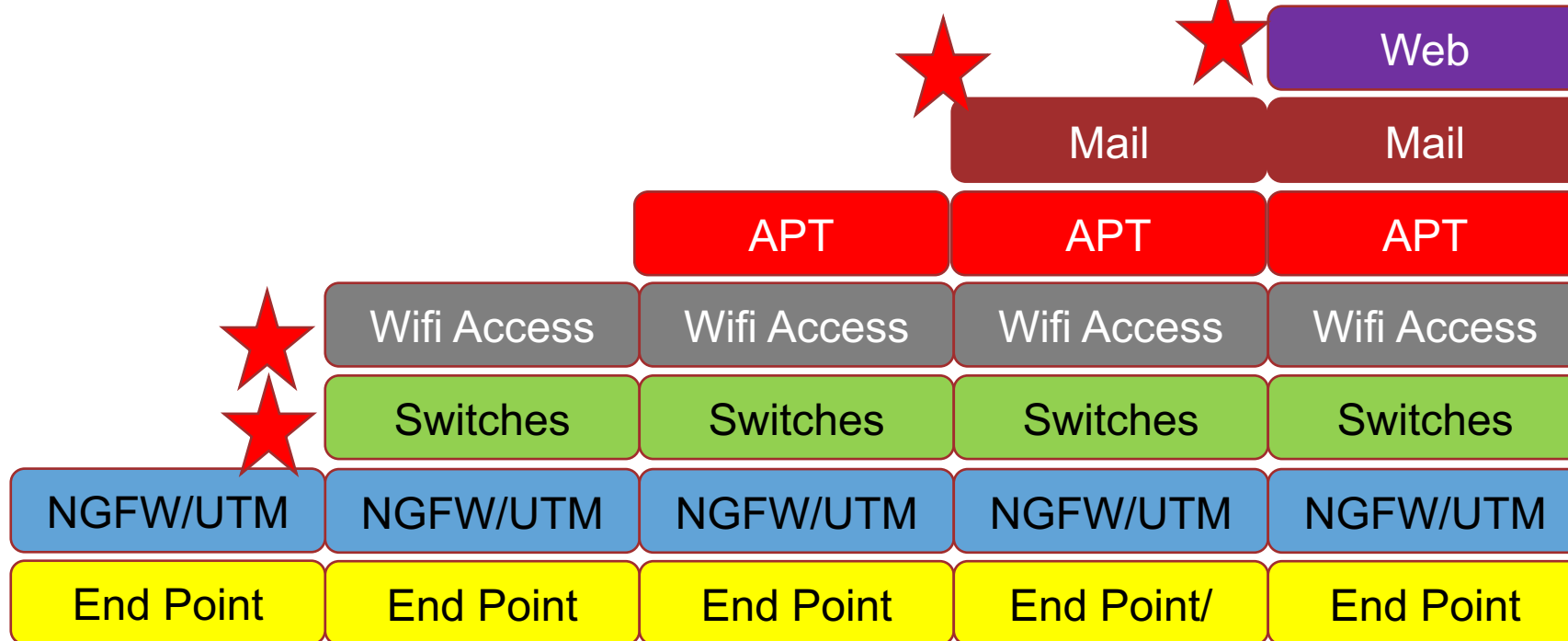
ARZENÁL pro každý segment sítě



Škálovatelnost - CROSS SALE

Partner ecosystem – Third party Solutions

Services – Threat Intelligence Services – ProServices



SOLUTION
 SOLUTION PORTFOLIO
 AUTOMATION
 VISIBILITY & REPORT
 (CO) MANAGEMENT
 RELEASE MANAGEMENT
 EASY TO DEPLOY
 SERVICES
 PRO SERVICES

Optional:

- Application Delivery Ctrl
- Authentication
- Anti-DDOS

Detailní a navolitelný reporting

Prepare

Figure 4. Network Topology

Prepare-2 Application Inventory

Overview

This category provides awareness to the operating systems and applications that reside on the target functional area. The data is derived from the log of operating systems and installed applications on Microsoft Windows. It is a complete list of all applications present on the target.

Risk

Not implementing change control processes can result in unauthorized changes and could increase potential for data loss.

Recommendations

Review each change in this report and cross-reference it with the change control and approval management. If you do not have a change control process, you should implement one. If you do have a change control process, you should ensure that all changes are properly documented and approved.

Protect

Pro-2 Change Control - Security

Overview

This category provides awareness to all changes made to the target functional area. The information will be the count of changes, including the date, time, and details of the change, and the user who made the change.

Risk

Not implementing change control processes can result in unauthorized changes and could increase potential for data loss.

Recommendations

Review each change in this report and cross-reference it with the change control and approval management. If you do not have a change control process, you should implement one. If you do have a change control process, you should ensure that all changes are properly documented and approved.

Figure 17. Summary of Changes

Review Sections

Quick View

This section provides a quick view into the aggregate severity level of findings for each functional area allowing you to prioritize your focus. Below is a description of risk levels.

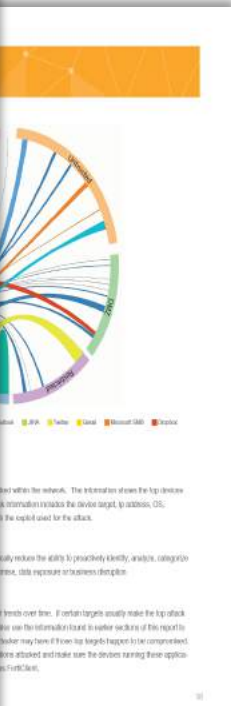
Feature	Score
Prepare	High (1-5)
Protect	High (1-5)
Detect	High (1-5)
Respond & Recover	High (1-5)

High - Significant impact to information and services
 Medium - Some impact to information and services
 Low - Minimal impact to information and services

Situation Awareness Report Sections

The following is a brief description of each functional area and its importance to a strong security posture.

Prepare	If you don't know what you are running, how can you protect it adequately? The Prepare functional area is based on providing awareness of your cyber assets such as servers and services, applications including IP/MAC, network topology and user accounts associated with the assets.
Protect	Does your team have a good understanding of your cyber environment so you can react to protect your cyber assets? The Protect functional area is based on providing awareness of your cyber assets allowing you to know and reduce the potential impact of a cybersecurity event. This includes providing awareness of your baseline security configuration, change control, vulnerabilities and remediation efforts and remote access to external cyber assets.
Detect	As the attack surface remains so large the risk of a breach making it important to detect events in a timely manner and understand the potential impact. The Detect functional area is based on providing awareness of your data flow, log attack targets, log response details, security events and compliance violations and ensuring log integrity.
Respond & Recover	Proactive incident response is becoming more important to not only quickly identify threats, but also respond to and recover from them. The Respond/Recover functional area is based on providing awareness of actions taken to identify threats within the network and containment of those threats.



Ransomware Activities in Your Network

Last 2 Years

This Year
Last Year
Last 2 Years
Last 3 Years
Last 4 Years

WannaCry

Description: WannaCryptor is a generic detection that utilizes exploits identified in Microsoft Windows SMB Server (401389)

Severity: Critical

Type: Ransomware: Trojan

CVE ID: CVE-2017-0144, CVE-2017-0145, CVE-2017-0147

Patch: Microsoft 17-010

IPS Signatures: MS.SMB.Server.SMB1.Trans2... W32/CVE.2017.0147.A!tr, W32/FarFlATVE!tr.bdr, W32/Filecoder_WannaCryptor.B!tr, W32/Filecoder_WannaCryptor.D!tr, W32/Gen.DK!tr, W32/Gen.DLC!tr, W32/Gen.Kryp!tr.1C25!tr

Vulnerability Criteria: XP, Vista, Server 2008/R2, Server 2012/R2, Server 2016, B/O.1/RT.0.1

10 Vulnerable Hosts
14 Total Hosts

Vulnerable to WannaCry

John Smith

johnsmith@j.smith
j.smith@j.smith
j.smith@j.smith

Windows 10 professional
IP Address: 172.16.79.215
MAC Address: 94:57:a5:c3:d2:a5
FortiClient Telemetry @: Connected

Malware Activities

12 Ransomware Incidents

- Exploits blocked by IPS
- Outbound Tor traffic blocked by App Control
- Botnet C2 blocked by AV
- Malicious email attachments blocked by AV



Containment

This category provides awareness to the containment status for malware threats within the network. The information will be the number of containment actions taken for the device target, by address, OS, and the exploit used for the attack.

This category provides awareness to the containment status for malware threats within the network. The information will be the number of containment actions taken for the device target, by address, OS, and the exploit used for the attack.

Security Fabric Audit - audit a doporučení změn

The screenshot displays the FortiGate 92D Security Fabric Audit interface. The top navigation bar shows the device name 'FortiGate 92D PM-Gateway' and the user 'admin'. The main content area is titled 'Security Fabric Audit' and includes a progress bar with steps: Detect Security Fabric FortiGates, Audit, and Easy Apply. A summary shows a Security Score of -1,295.7 (-1,315.7) with 46 Failed and 78 All Results. A bar chart indicates the distribution of scores: Passed (green), Low (blue), Medium (yellow), High (orange), and Critical (red).

Issue	FortiGate	Result	Recommendation
Firmware & Subscriptions 2 2			
Internal Segmentation Firewall (ISFW) 6 1			
Endpoint Compliance 3 3 0			
Endpoint Registration Interfaces which are classified as "LAN" should have FortiTelemetry enabled.	PM-Gateway	-30	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Interface Classification
	Building-1-FW	-30	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Interface Classification
	2ndFloor-FW	-60	Enable FortiTelemetry on the following interfaces: 📄 FSW-FOS-GUI (port40) 📄 ToFGT-100D (wan2) 🟢 Easy Apply
FortiClient Protected All supported devices should be registered via FortiClient.	PM-Gateway	-10	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
	Building-1-FW	-10	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
	2ndFloor-FW	-10	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
FortiClient Compliance All registered FortiClient devices should be compliant with FortiClient profile.	PM-Gateway	-10	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
	Building-1-FW	-10	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
	2ndFloor-FW	-10	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
FortiClient Vulnerabilities All registered FortiClient devices should have no critical vulnerabilities.	PM-Gateway	-50	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
	Building-1-FW	-50	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
	2ndFloor-FW	-50	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: ⚠ Endpoint Registration
Security Best Practices 4 2 2			

At the bottom of the interface, there are navigation buttons: '< Back', 'Next >', and 'Cancel'.

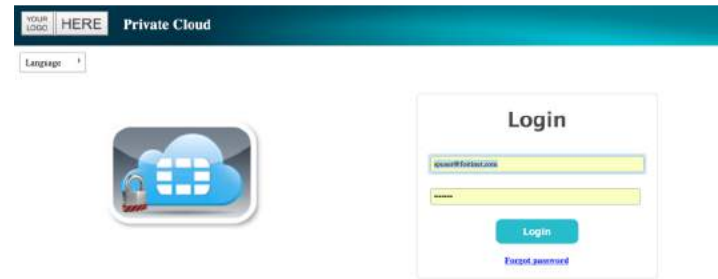
VARIANTNÍ NAsAZENÍ

- Cloud
- CPE
- Centralizovaný (HW, VM)
- Hybrid (CPE + VM) = FHV



SAMOOSLUHA – FortiPortal

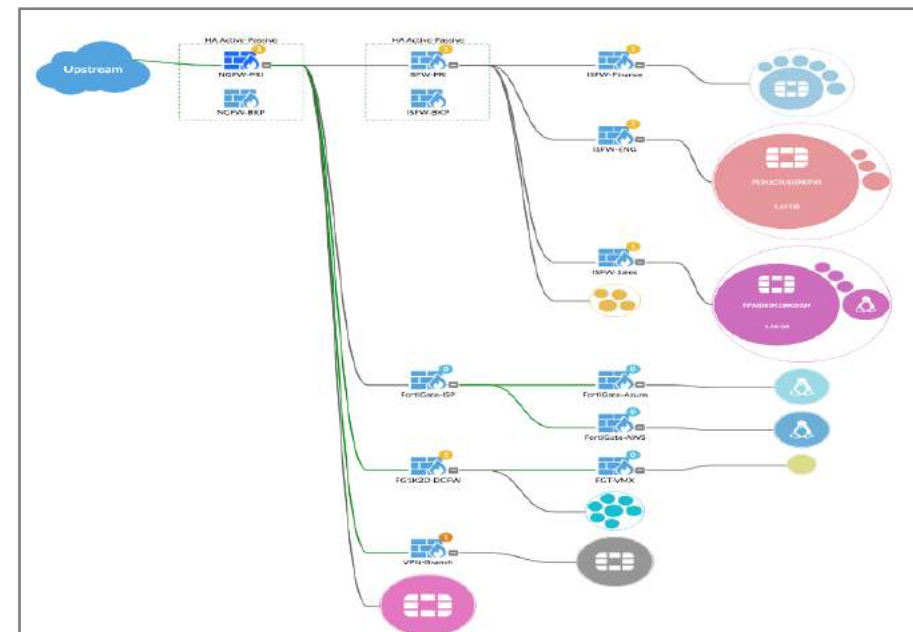
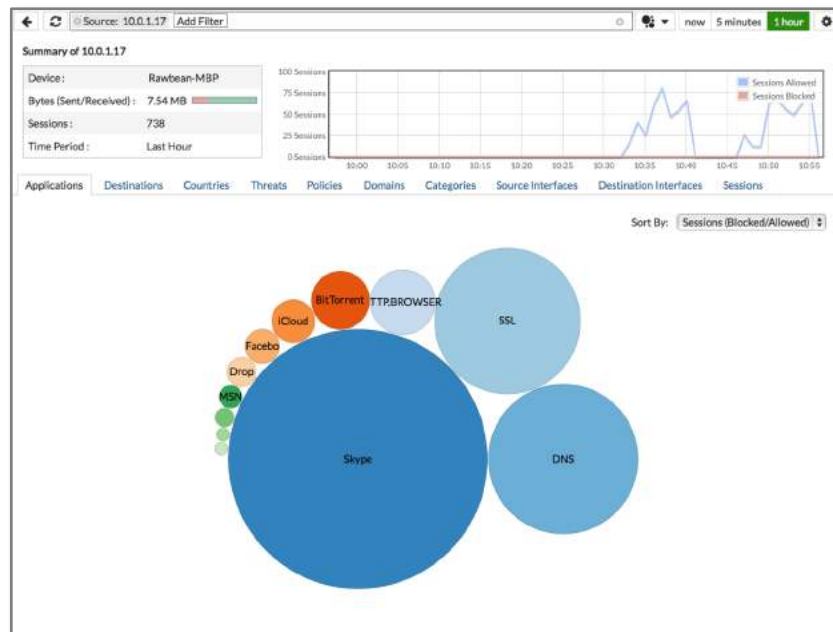
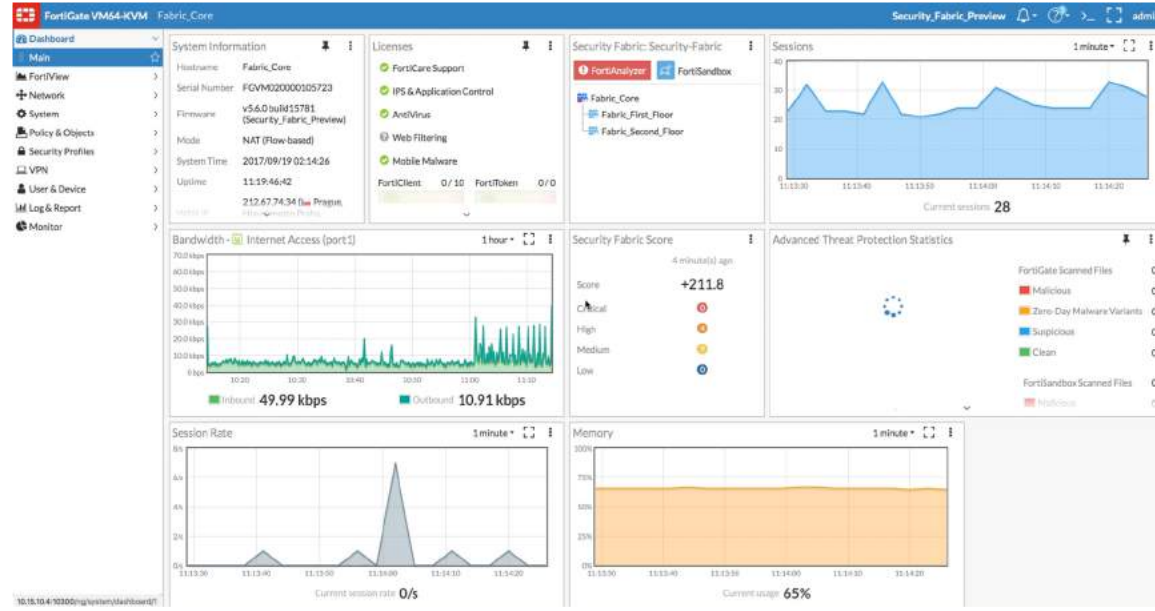
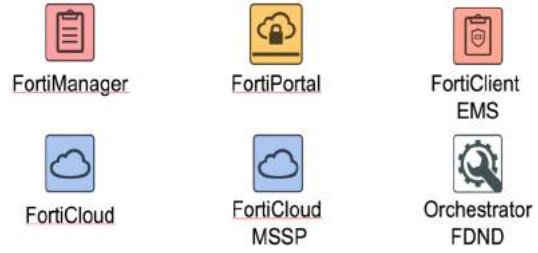
- Zákazník má na jednom místě:
 - » záznam událostí, definic a protokolů
 - » nastavený plán a generování sestav,
 - » statistiky a monitoring provozu
 - » Možnost změny konfigurace služeb
- MSSP umožňuje:
 - » monitorování stavu služeb
 - » nastavení nových zákazníků
 - » řešení problémů (trouble ticketing)



Cloud Based Security Analytics and Management for Carriers and Managed Security Service Providers.



Management



OTEVŘENOST - Fabric Alliance Ecosystem



Cloud



SDN



Endpoint



Management



Vulnerability/SIEM



IoT/OT/NAC



Identity



Technology



Automatizace a koordinace

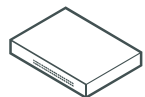
A Security Architecture that provides:

BROAD Visibility & Protection of the Digital Attack Surface

INTEGRATED Detection of Advanced Threats

AUTOMATED Response & Continuous Trust Assessment

Delivered as:



Appliance



Virtual Machine



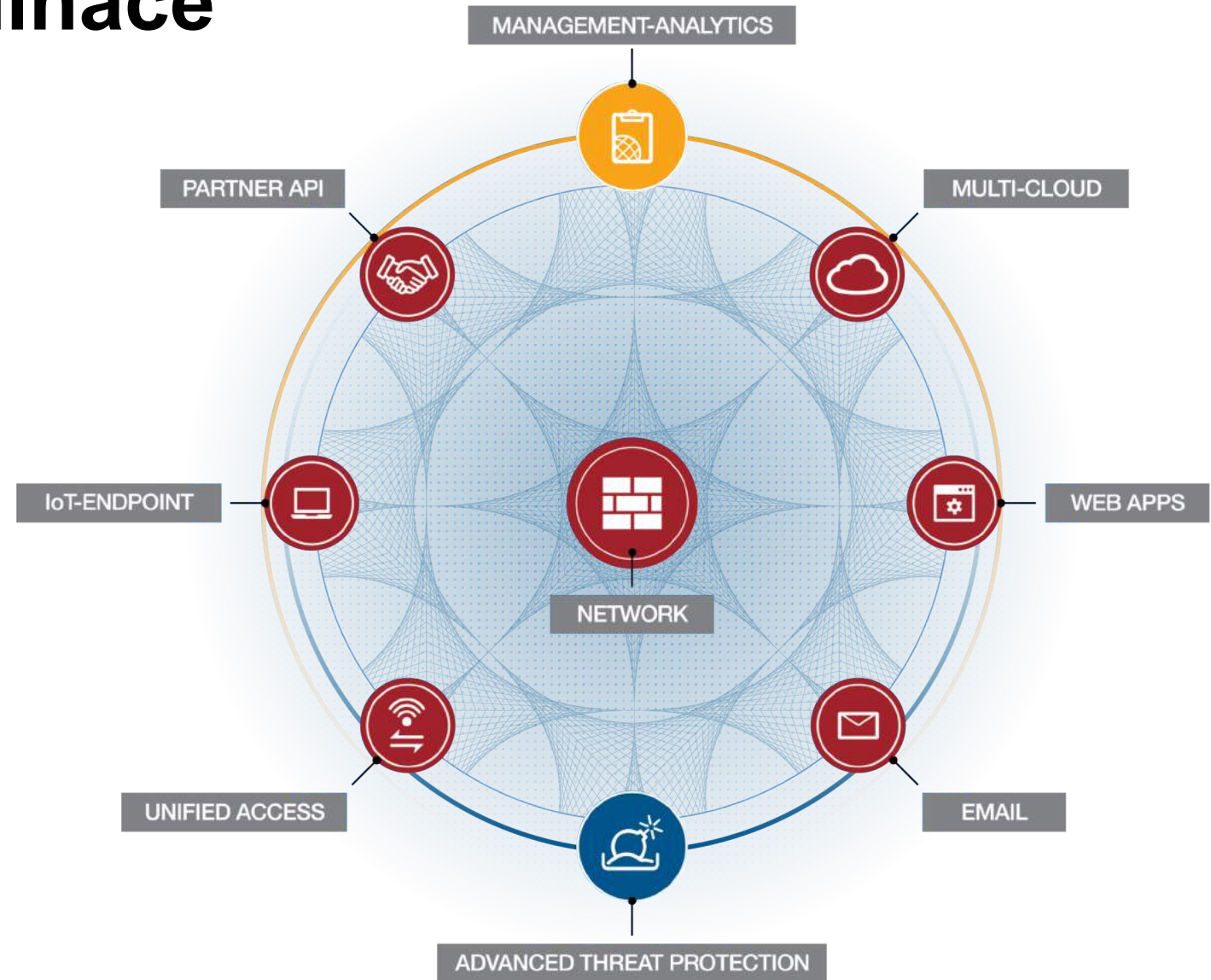
Hosted



Cloud



Software



MSP PLATFORMA – SPRÁVA A SLUŽBY

- **Management a analytika**
 - » FortiSIEM, FortiManager, FortiAnalyzer
- **Autentifikace přístupu**
 - » FortiAuthenticator
- **Základní bezpečnostní služby**
 - » NGFW (Firewall, IPS, VPN, Anti-Vir, Antispam, Anti-Malware, Web filtr, Application Control)
- **Doplňující účelová řešení**
 - » Ochrany webových aplikací - FortiWeb
 - » Ochrana před DDoS útoky - FortiDDoS
 - » Optimalizace a bezpečnost aplikací Secure - FortiADC
 - » Detekce a ochrana před dosud neznámými hrozbami - FortiSandbox
 - » Bezpečné řešení E-mail komunikace – FortiMail
 - » Bezpečné bezdrátové sítě – FortiWireless
 - » Detailní analýzy provozu zákazníků, přítomnosti, umístění a pohybu každého zákazníka
 - » Secure Access - Secure Wireless LAN

Update customer

Email: user@oust2.com

Customer Name: cust2

First Name: Customer

Last Name: Two

Enable Antivirus

Enable URL filtering

Enable Application Control

Enable Anti-spam

Enable Data Loss Prevention

Enable Sandbox

Monthly Cost: 90

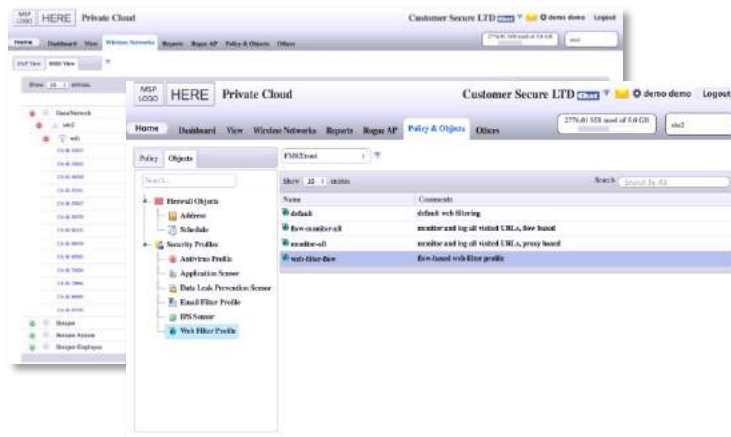
[Update](#) [Logout](#)

Souhrn hlavních funkcí

MSSP



Multi-tenantní prostředí



Jednotný management



Threat Landscape Analytics



Cloud Portal



V barvách ISP



SandBox Analýza

Fortinet: Partner pro MSP budoucnosti

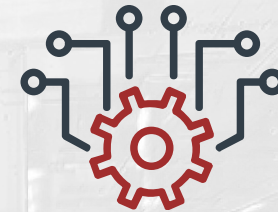
Silné regionální zastoupení



Široké portfolio produktů



Inovativní a výkonný motor



Motivační Partnerský
Ecosystem



Řešení pro každý segment



Obchodní podpora



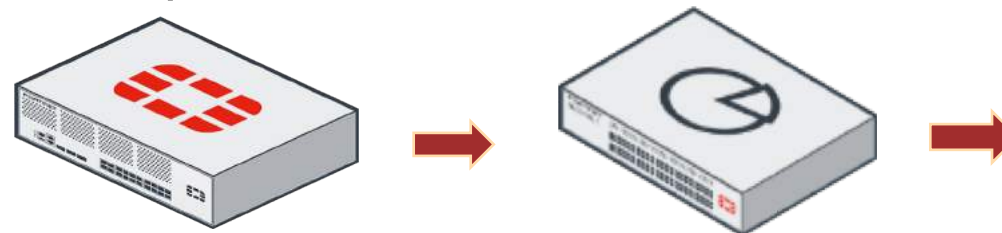
CTAP - Bezplatný test sítě

- Zapůjčíme FortiGate
- Připojíme bez nutnosti zásahu do Vaší sítě
- Vytvoříme detailní report a analýzu Vašeho provozu
- Probereme s Vámi výsledky a navrhujeme opatření



Pohled do vaší sítě pokrývající klíčové oblasti:

- » **Bezpečnostní hrozby** – odhalíme slabá místa, malware, botnety, atd.
- » **Produktivita** – přehled o uživateli a jejich chování
- » **Výkon** – aktuální zátěž sítě a návrh optimálního řešení



„Skvěle útočit umí ten vojevůdce, jehož protivník neví, kde se má bránit.

A skvěle se bránit umí ten vojevůdce, jehož protivník neví, kde má zaútočit.“

– Sun C'

The Fortinet logo graphic is a complex, multi-faceted geometric shape composed of numerous triangular and quadrilateral facets in shades of orange, red, and dark brown. It is centered on the page and partially overlaid by a dark horizontal bar containing the text 'FORTINET'. The background features a dark grey gradient with white circuit-like lines and a bright white horizontal band passing through the center of the logo.

FORTINET®

Martin Fišer

mfiser@fortinet.com

602 303 265