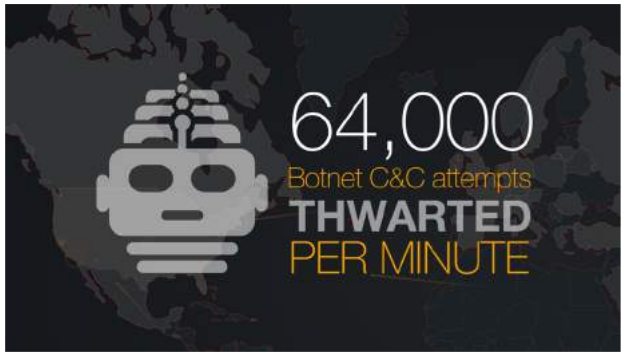
FORTINET

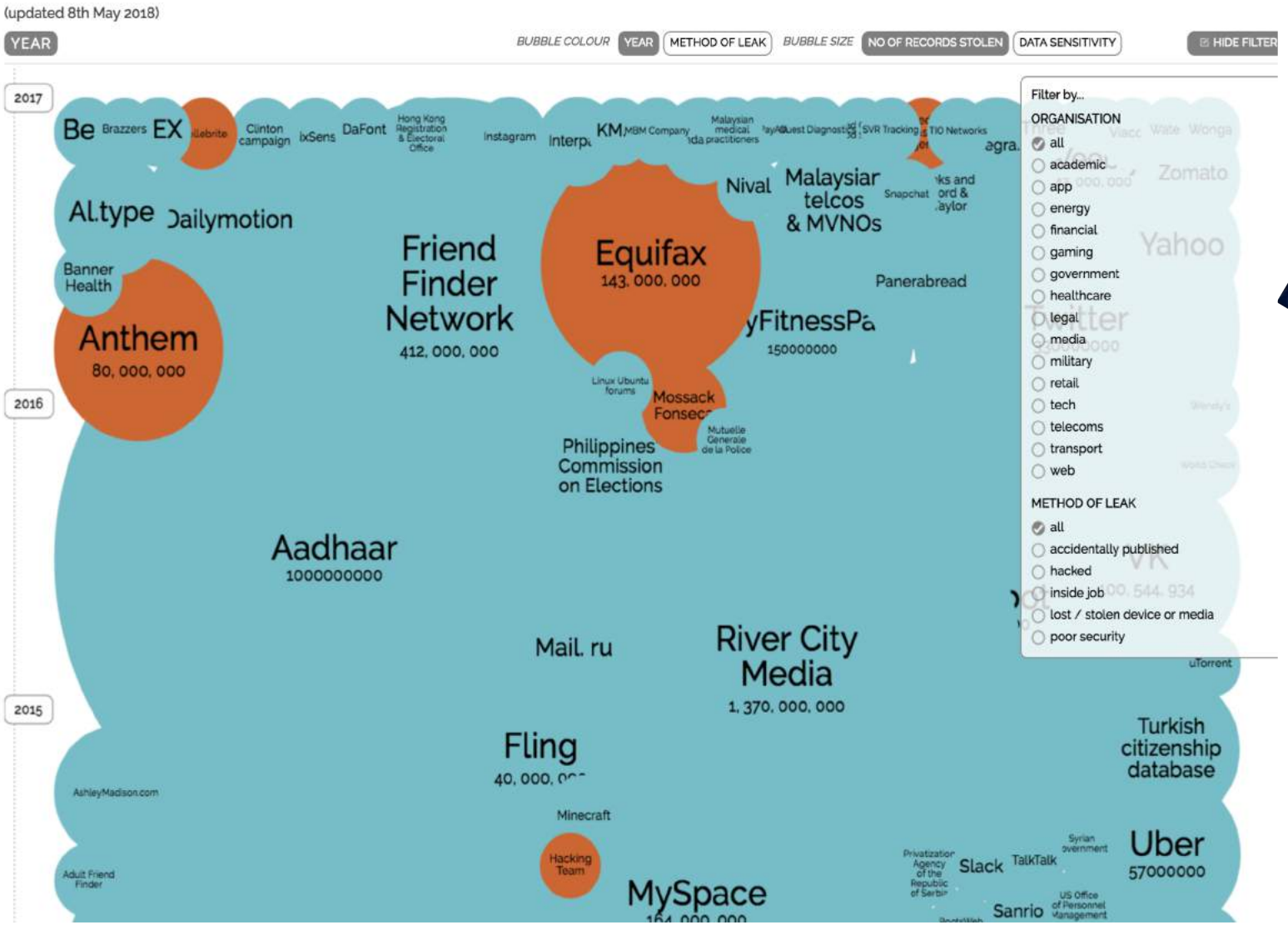
KYBERNETICKÁ BEZPEČNOST

Výzvy a příležitosti pro ISP

Martin Fišer
Key Account Manager
SP/MSSP

FortiGuard by the numbers





http://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Fakta

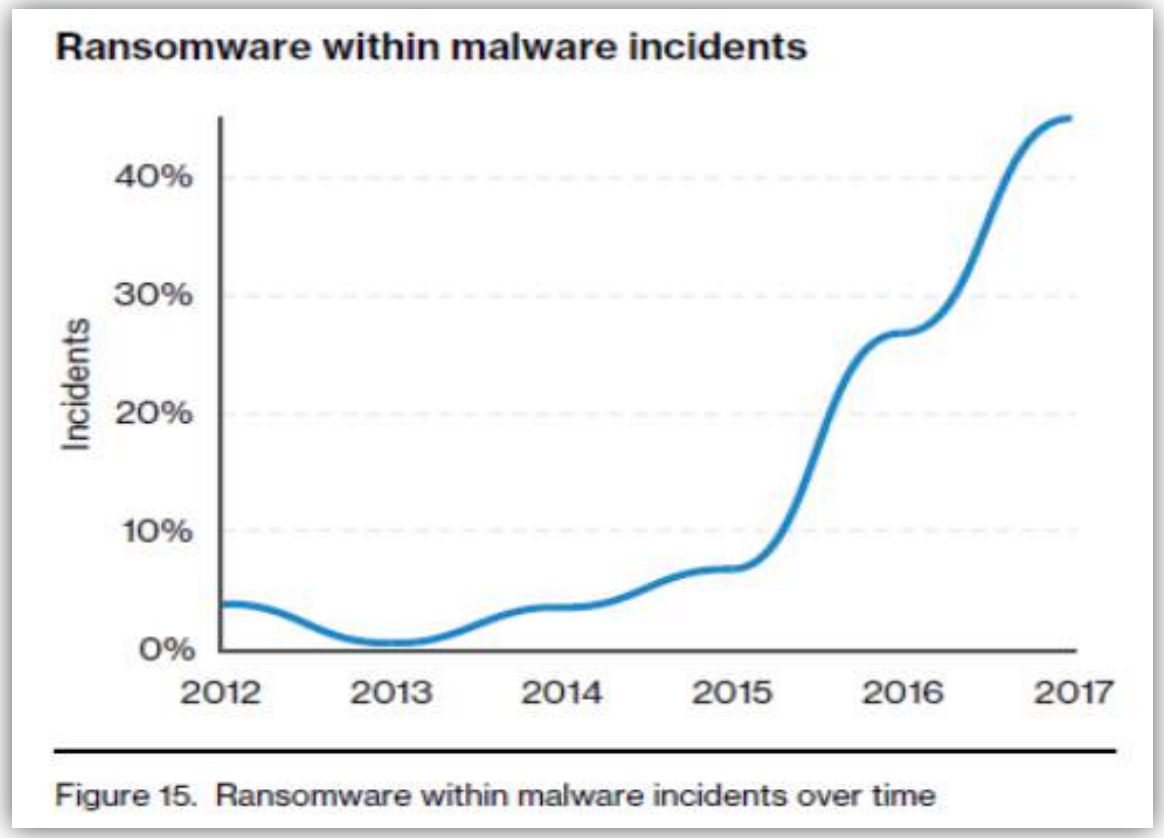


Figure 15. Ransomware within malware incidents over time

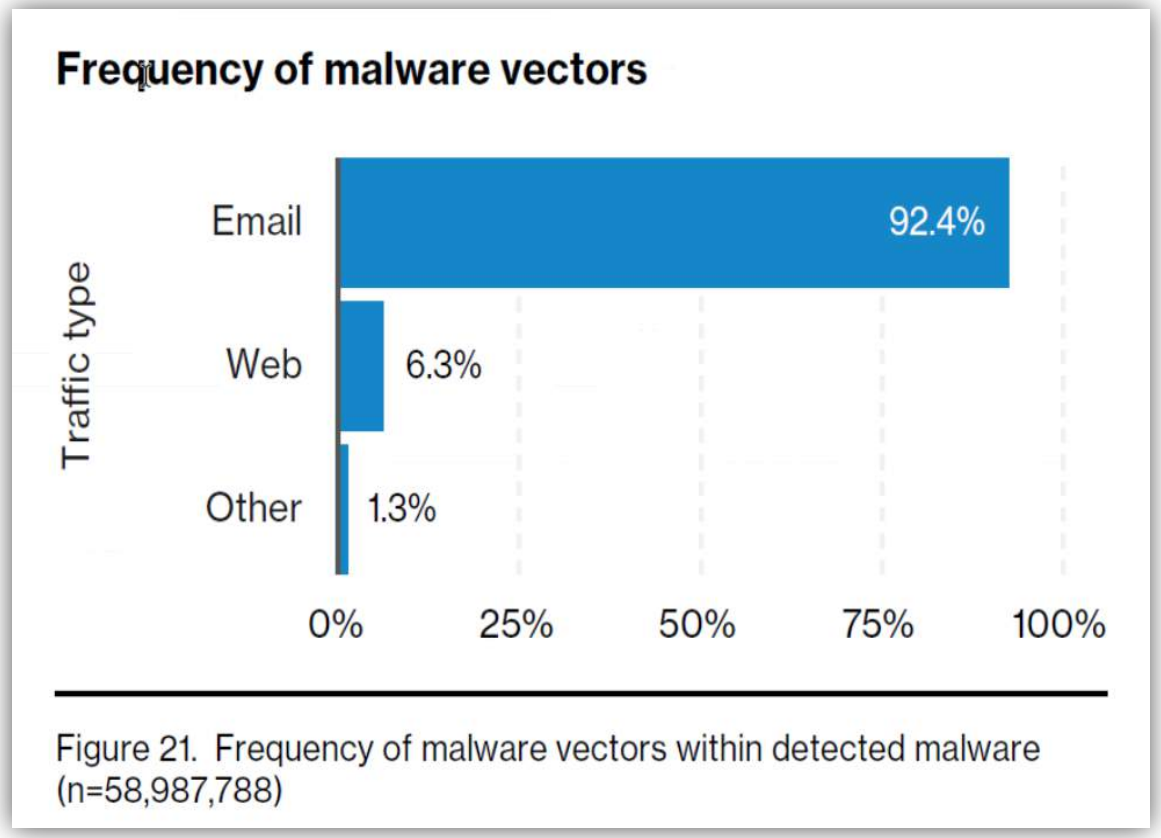
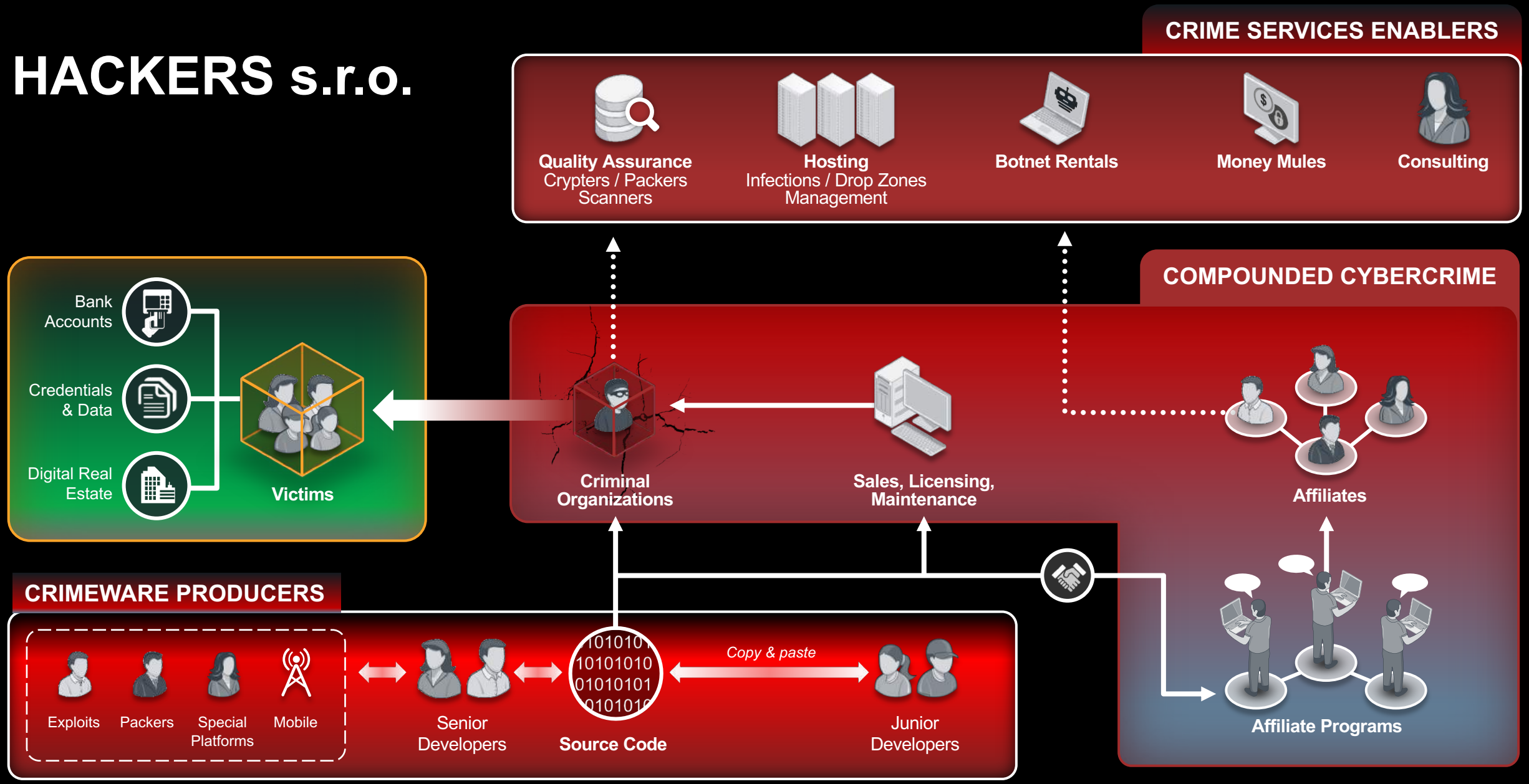


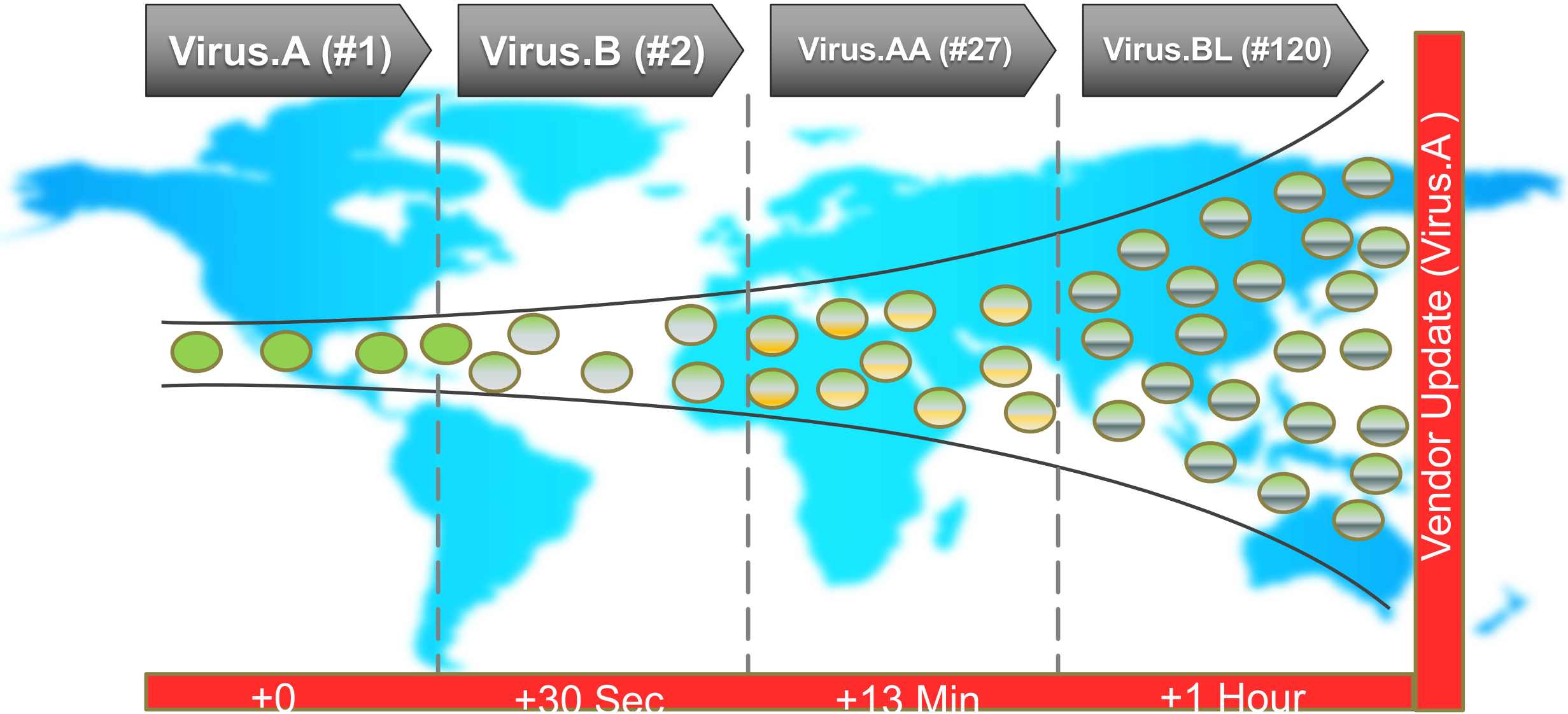
Figure 21. Frequency of malware vectors within detected malware (n=58,987,788)

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

HACKERS s.r.o.


CRIME SERVICES ENABLERS
Quality Assurance
Crypters / Packers
Scanners
Hosting
Infections / Drop Zones
Management
Botnet Rentals
Money Mules
Consulting
COMPOUNDED CYBERCRIME
Bank Accounts
Credentials & Data
Digital Real Estate
Victims
Criminal Organizations
Sales, Licensing, Maintenance
Affiliates
CRIMEWARE PRODUCERS
Exploits
Packers
Special Platforms
Mobile
Senior Developers
Source Code
Copy & paste
Junior Developers
Affiliate Programs

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)

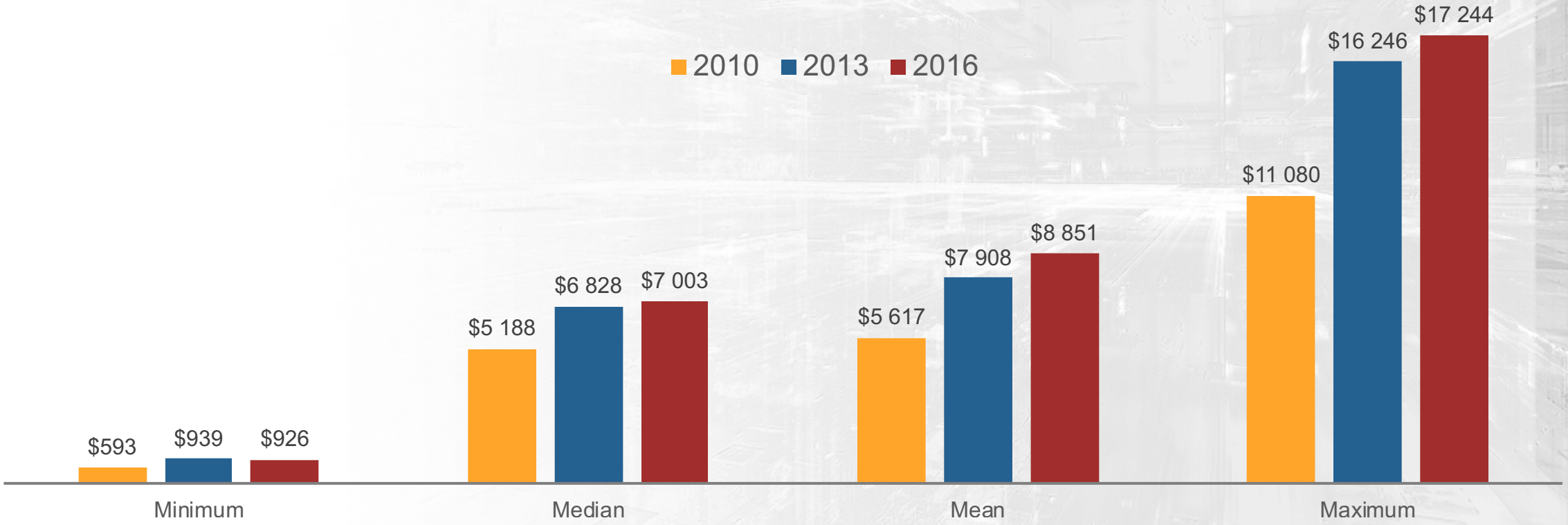
FORTINET

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

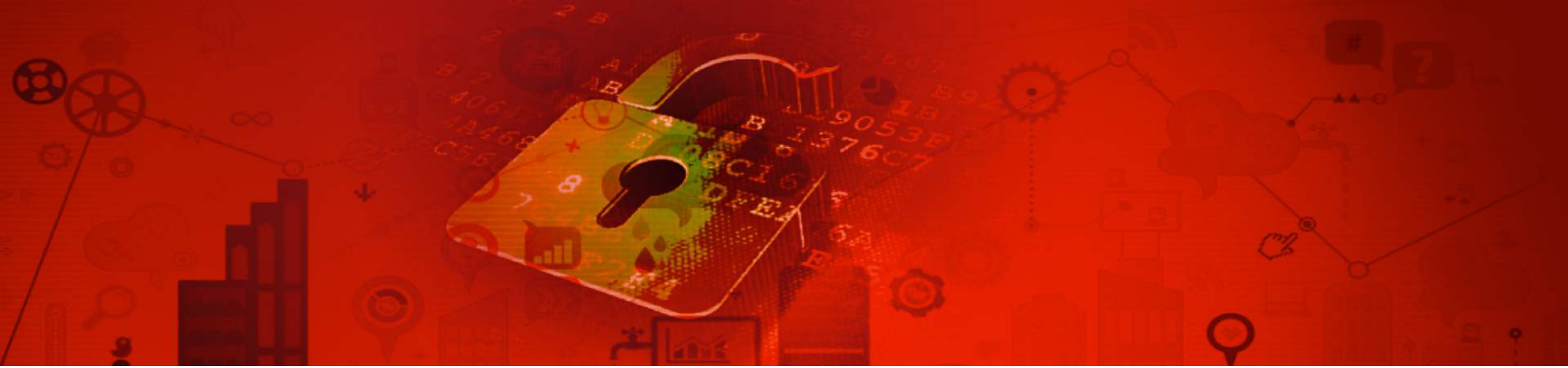


Svět se mění

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]

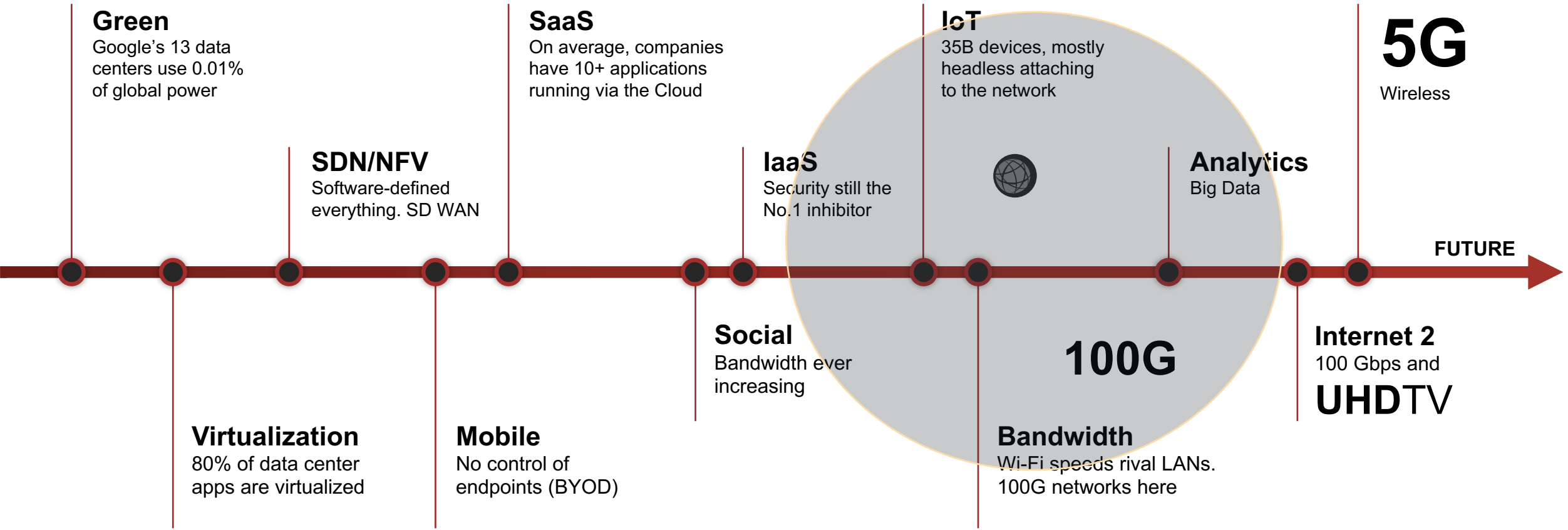


SX

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

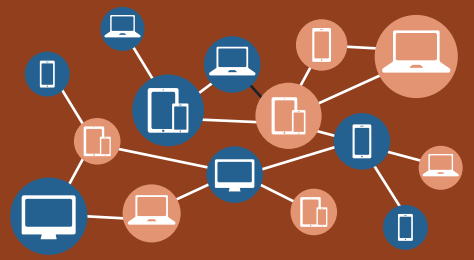
[Security Transformation]

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

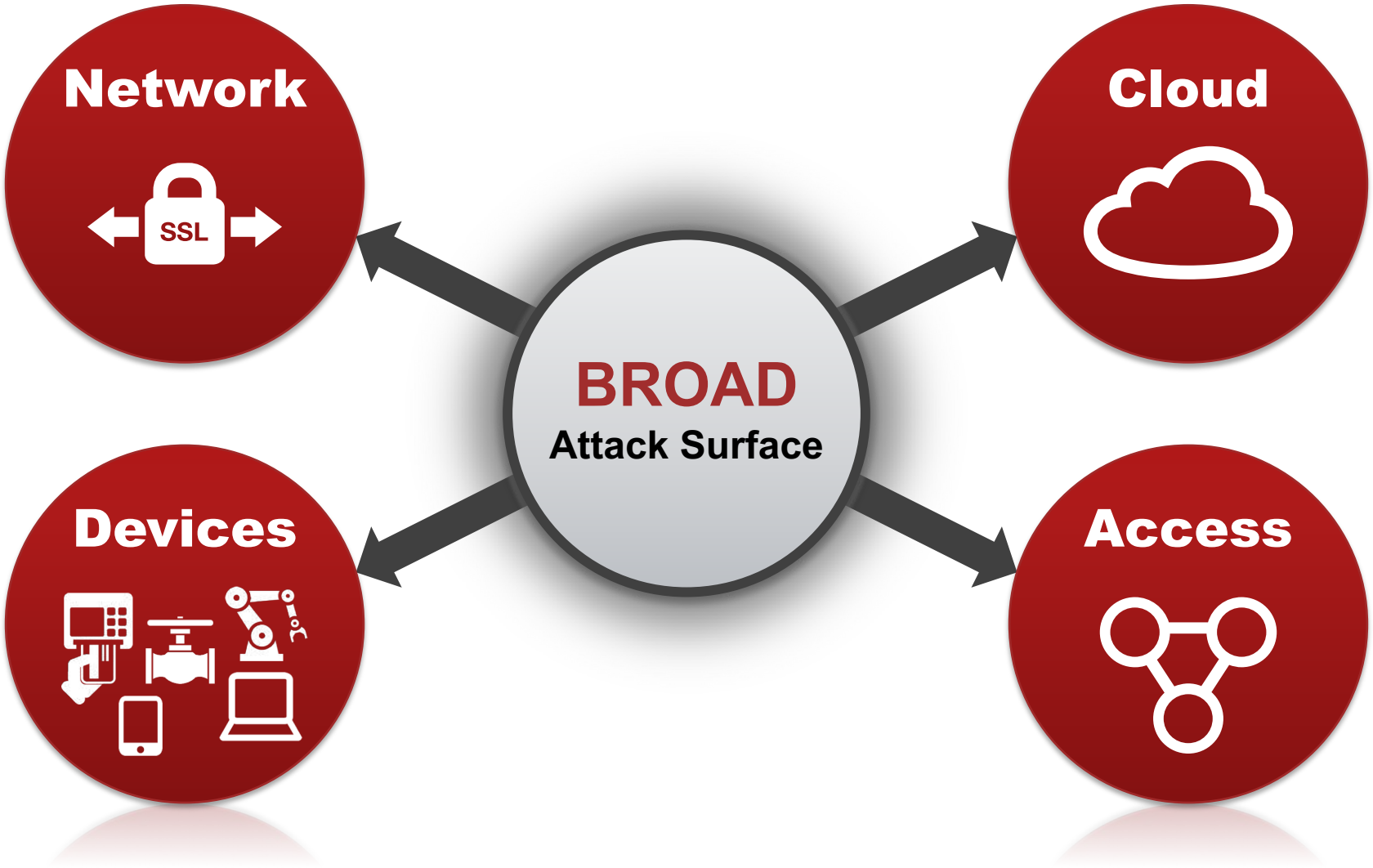
62% still use it

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

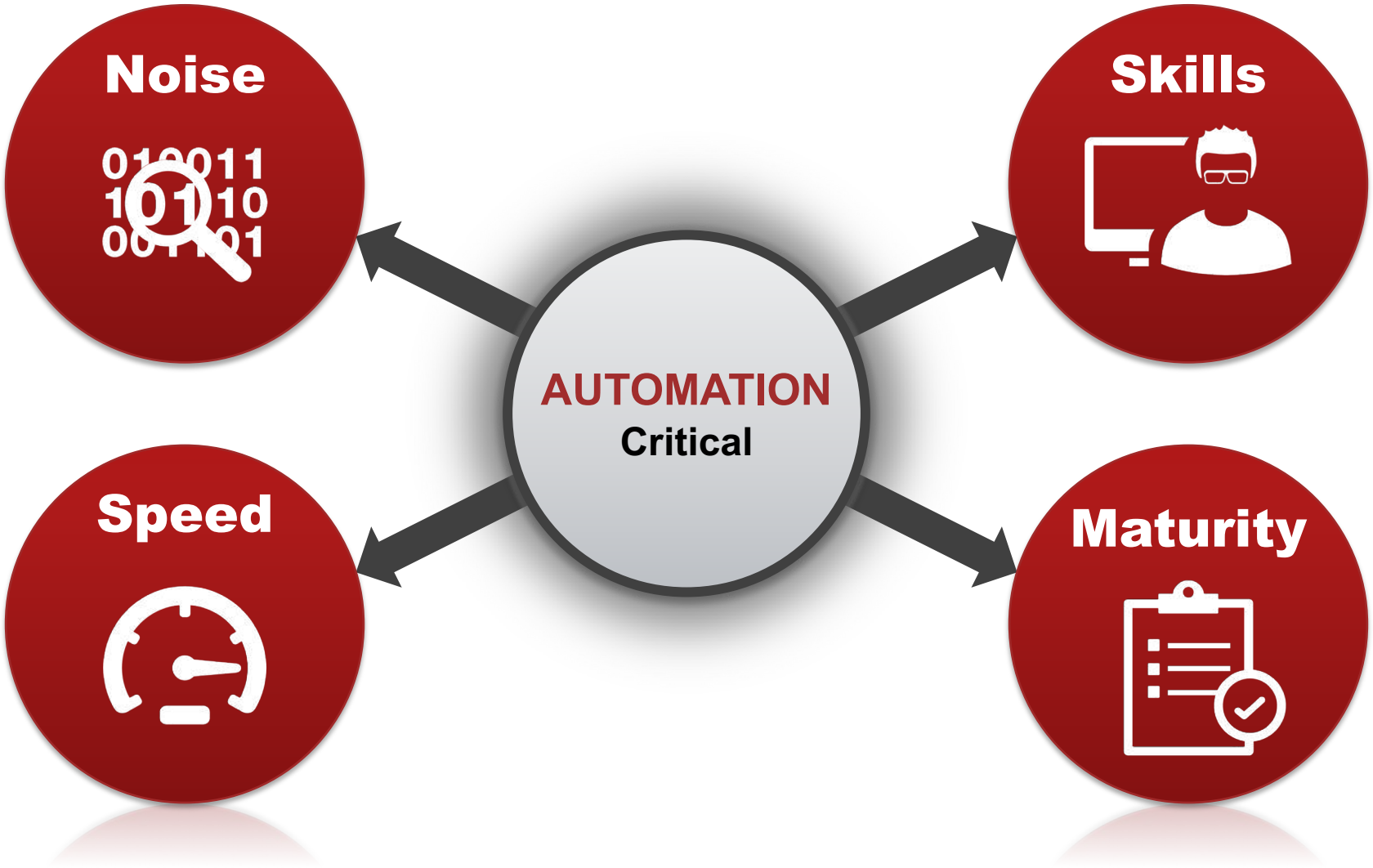
The average smartphone will generate **4GB** **of traffic per month by 2019**

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

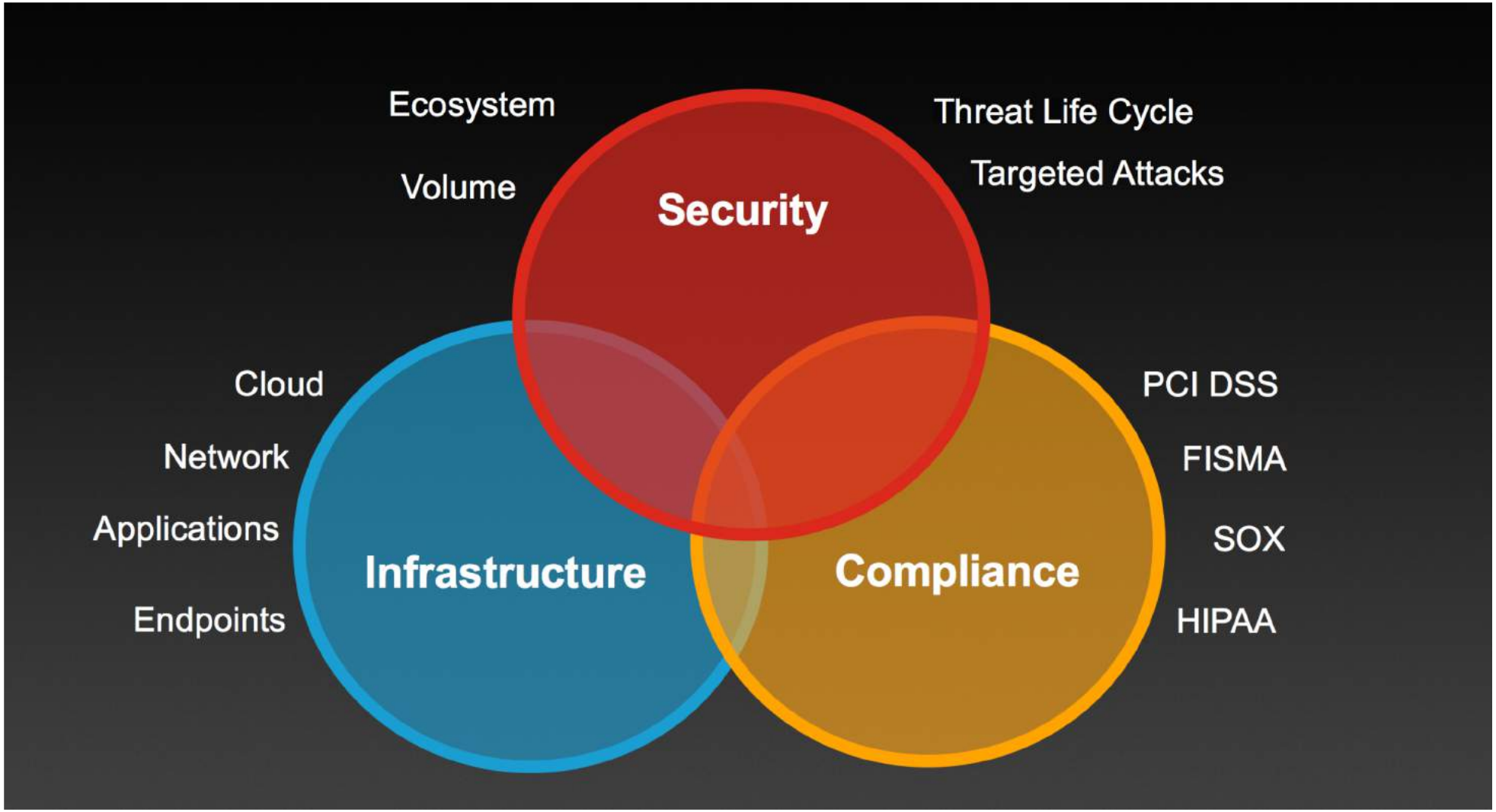
Kapitulace na domobranu

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

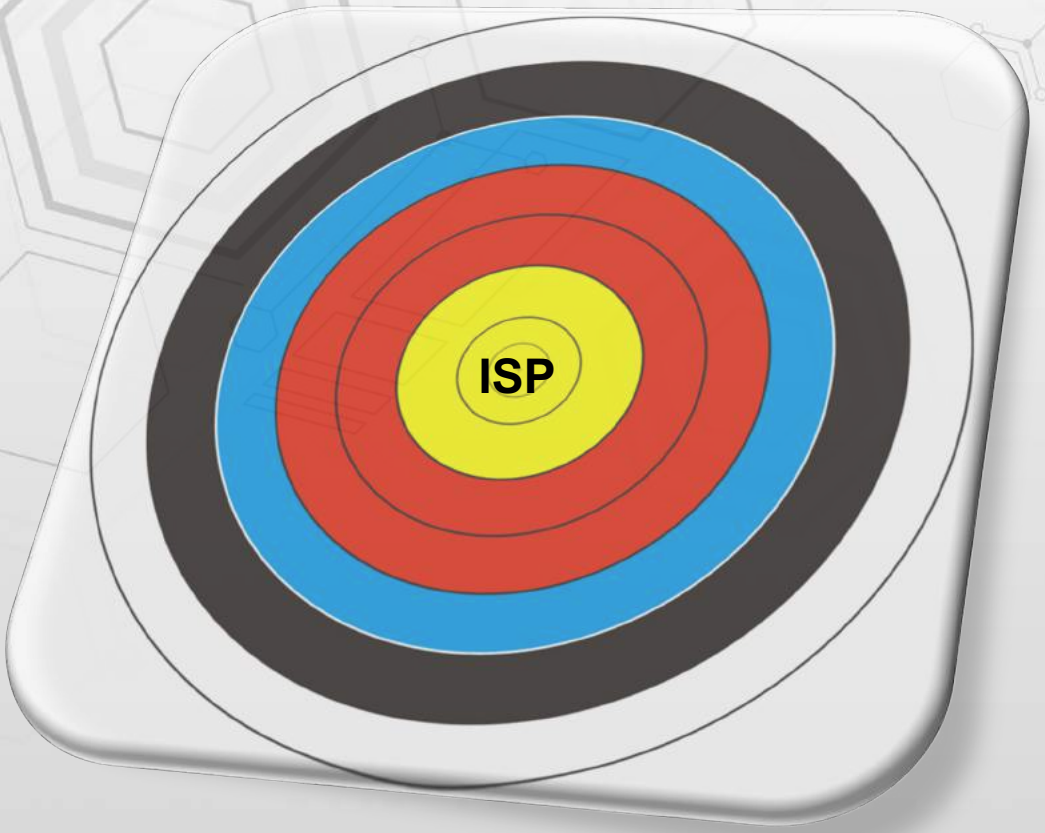
- Kybernetický zákon
- Anti hazard
- IP adresa jako osobní údaj
- GDPR (General Data Protection Regulation)
- Compliance reports (PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls)

- Útočníky nezajímá jestli jste dostatečně „Compliance“

ZMĚNY VE SVĚTĚ ISP

- **DŘÍVE**
  - Hlas, Data, Internet
  - Minuty, tarifikace,
  - Rychlost, bajty, FUP, SLA
- **NYNÍ**
  - CLOUD
  - BYOD
  - IPTV
  - Video On Demand
  - Data BackUp and restore
  - Smart Home
  - VPN služby
  - Šifrovanou komunikaci
  - Security
- **ISP?**
  - TCS — Telecommunication Services Provider
  - CSP — Communication Services Provider
  - MSP — Managed Services Provider
  - VASP — Value Added Services Provider
  - MSSP — 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

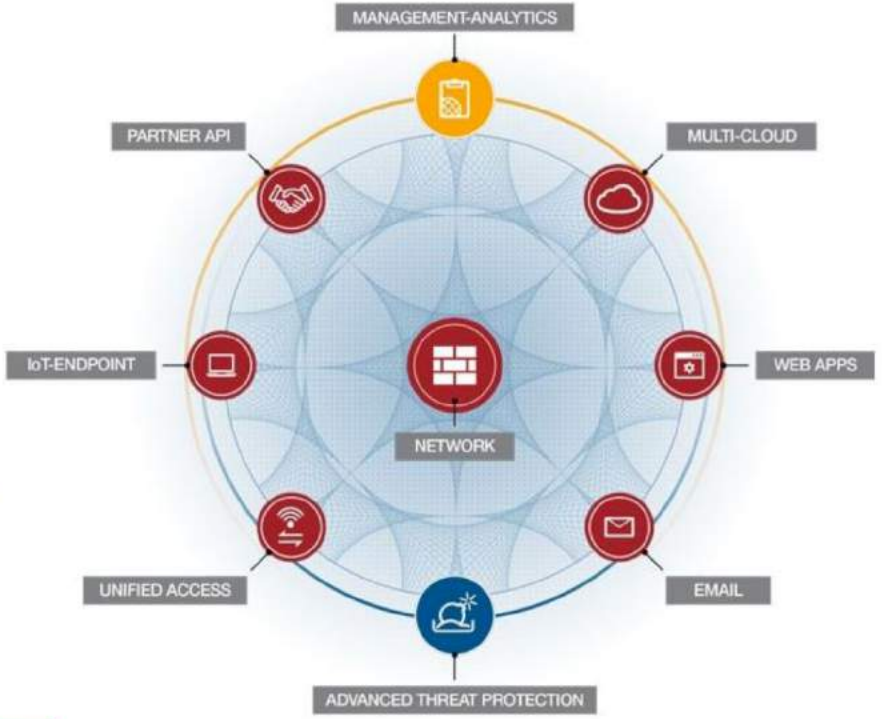
MSSP PORTFOLIO – cross sale

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



FORTINET Fabric-Ready

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 multitenatní 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

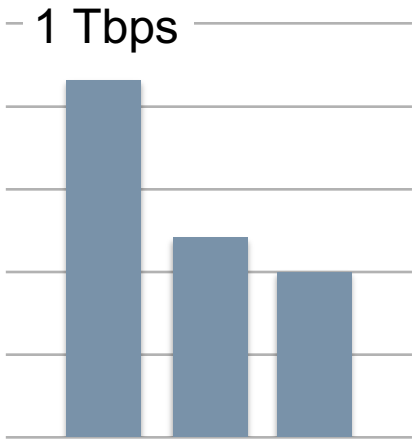
Security Processors (SPU's)

NP6 — Accelerates Network Traffic

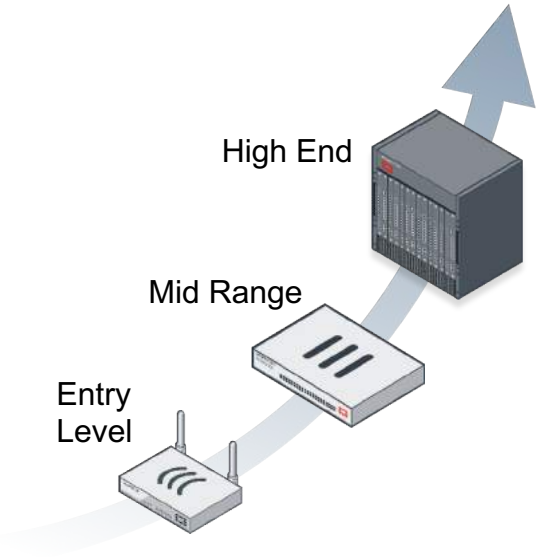
CP9 — Accelerates Content Inspection

SoC3 — Optimized Performance for Entry Level

Parallel Path Processing



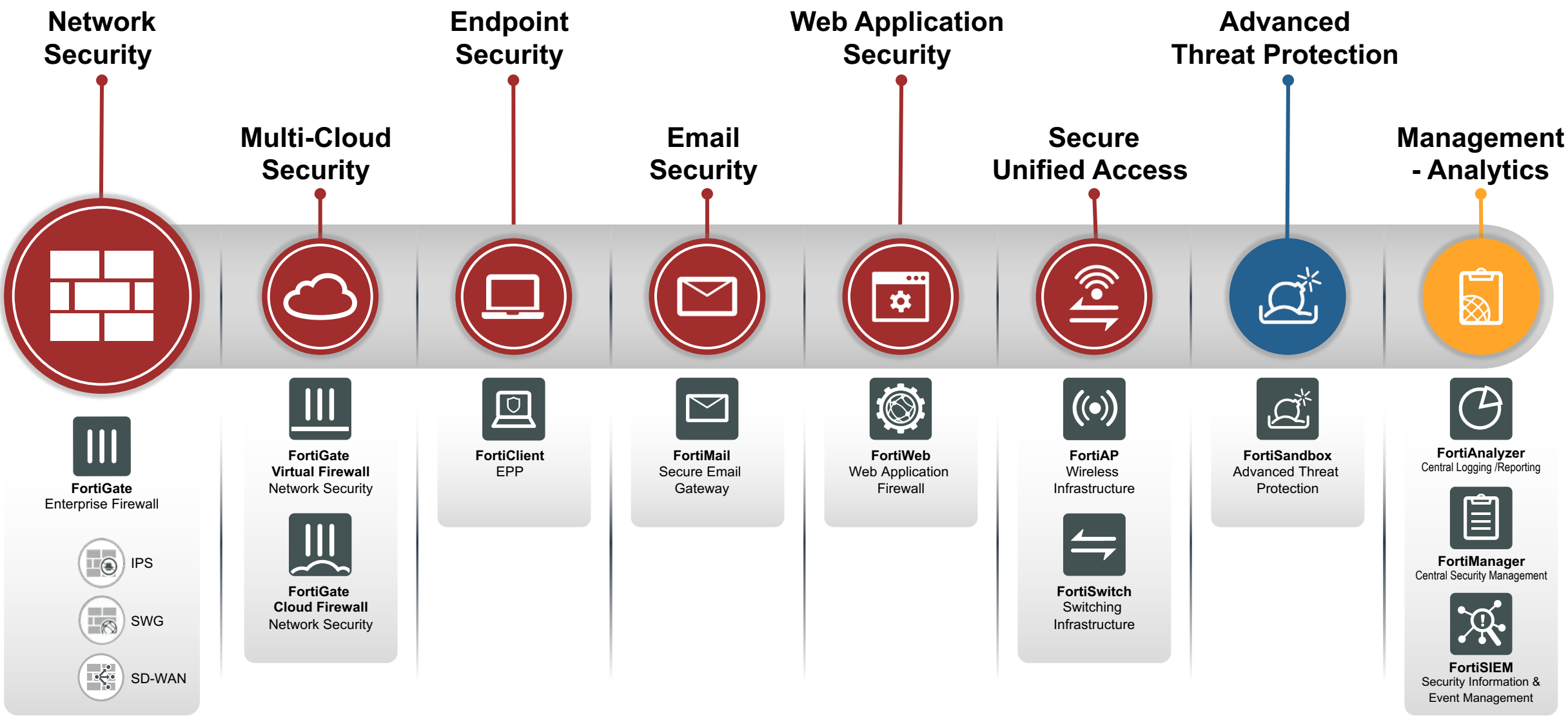
Comprehensive Range





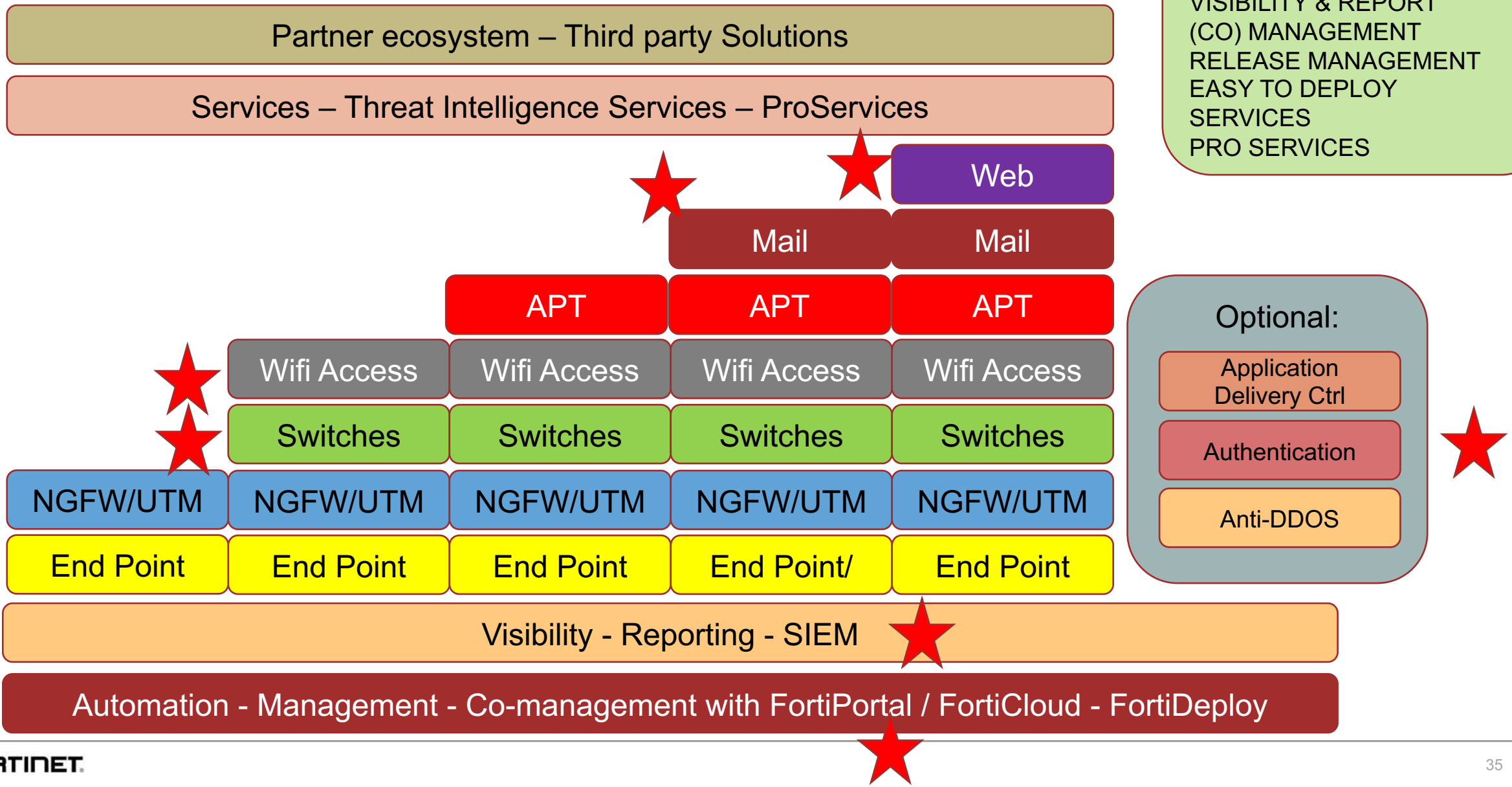

FortiGate FortiWiFi Models	30E, 50E 60E	70D, 80D, 90D, 90E, 92D	100D	200D	300D 400D 500D	600D 800D 900D	1000 2000 3000	FG-5000 Series	FG-VM Series
Hardware									
Product Range / Form Factor	Entry / Desktop	Entry / Desktop-2 RU	Mid Range / 1 RU	Mid Range / 1-2 RU	Mid Range / 1 RU	Mid Range / 1 RU	High 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



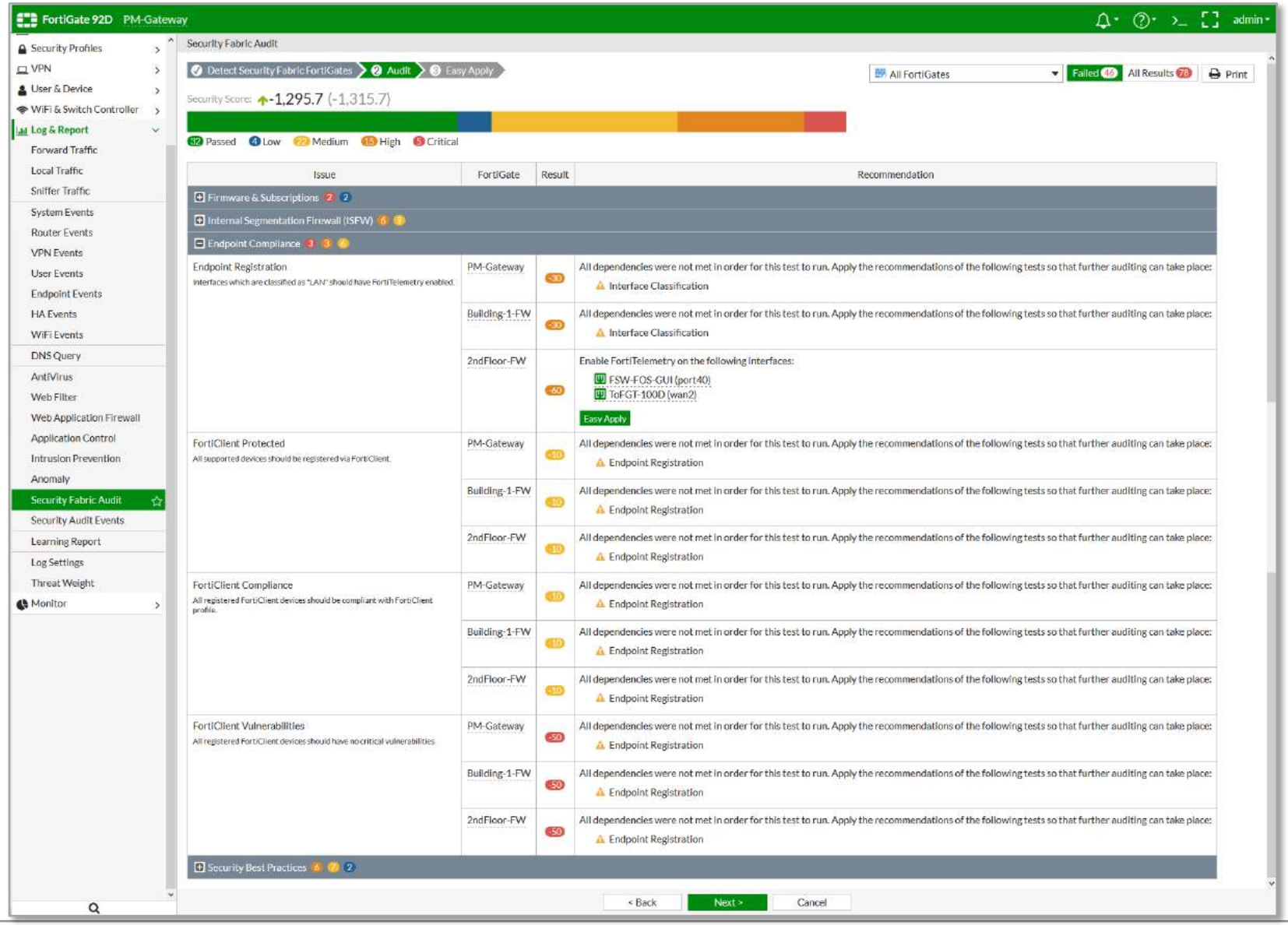
Škálovatelnost - CROSS SALE

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



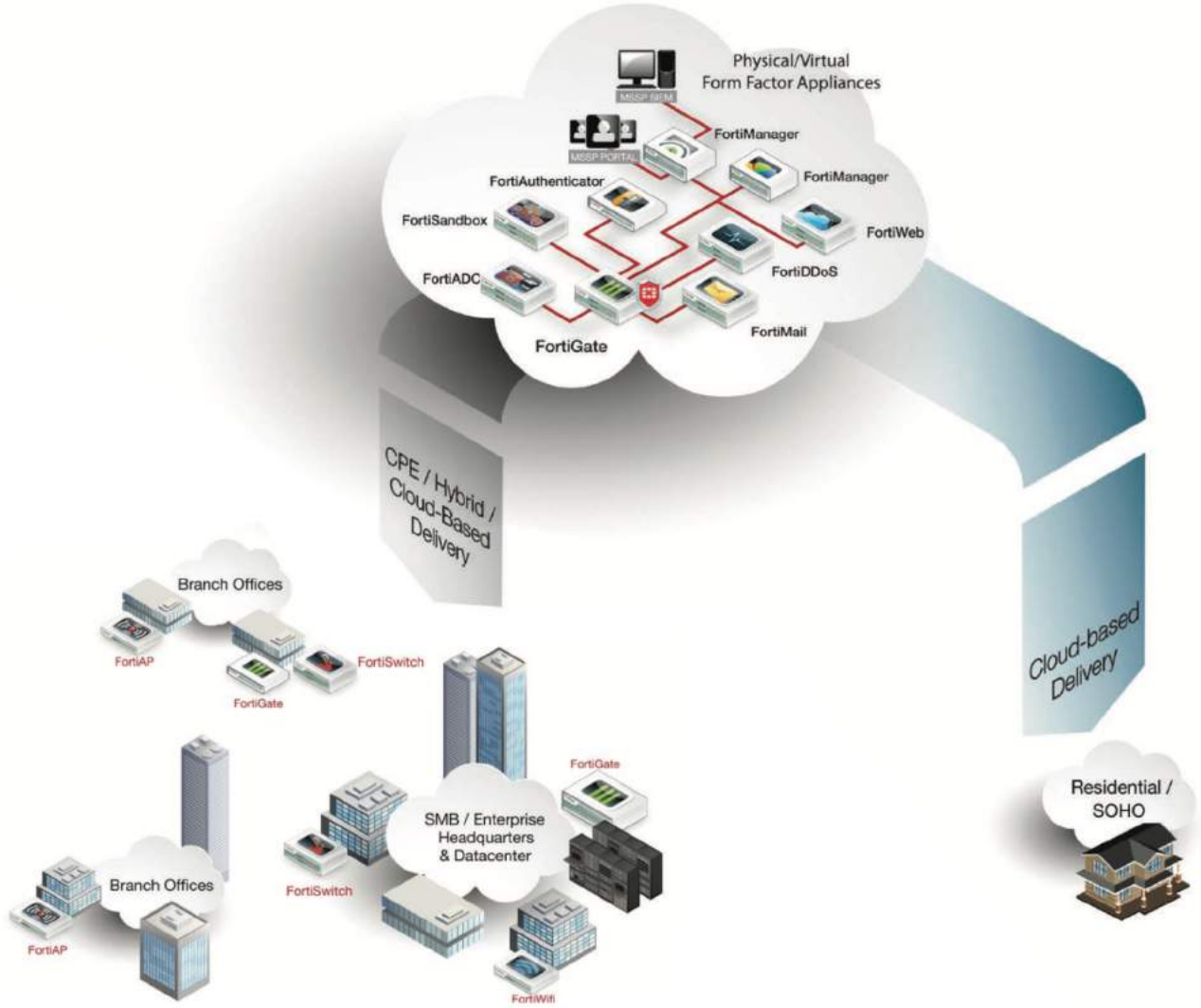
Detailní a navolitelný reporting

Security Fabric Audit - audit a doporučení změn



VARIANTNÍ NASAZENÍ

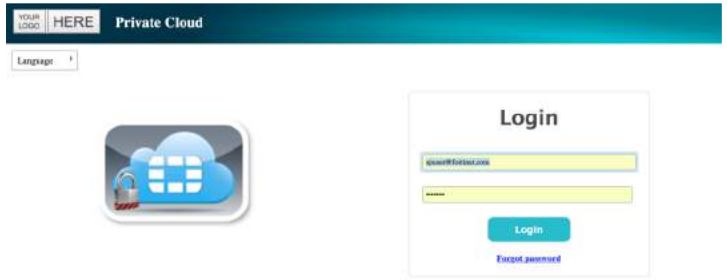
- Cloud
- CPE
- Centralizovaný (HW, VM)
- Hybrid (CPE + VM) = FHV



SAMOOBSLUHA – FortiPortal

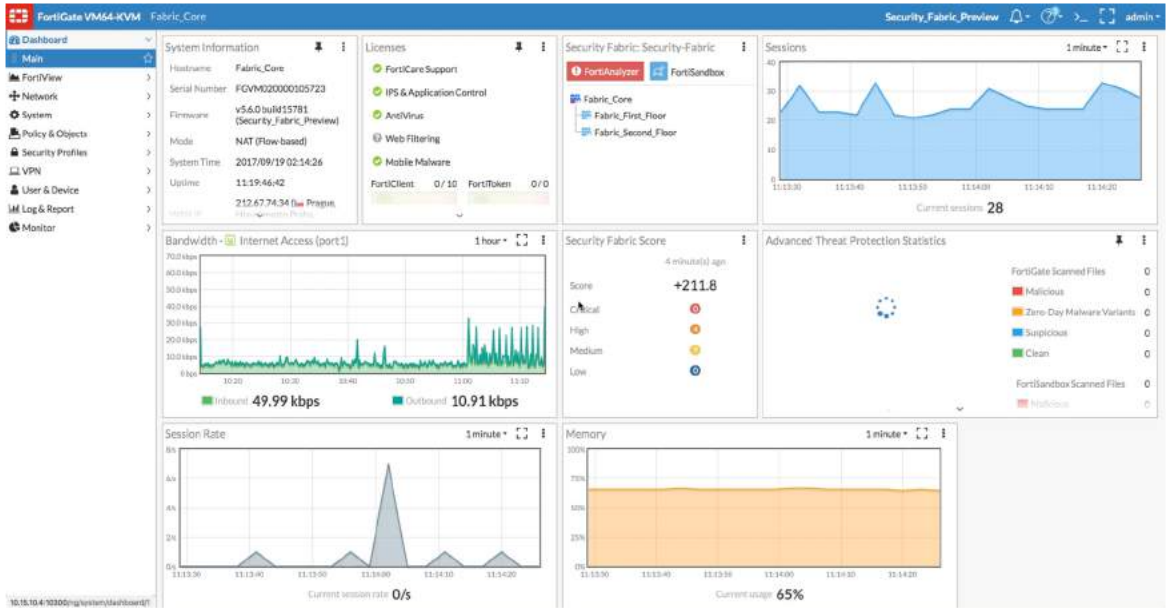
- Zákazník má na jednom místě:
  - » záznam událostí, definic a protokolů
  - » nastavený plán a generování sestav,
  - » statistiky a monitoring provozu
  - » Možnost změny konfigurace služeb

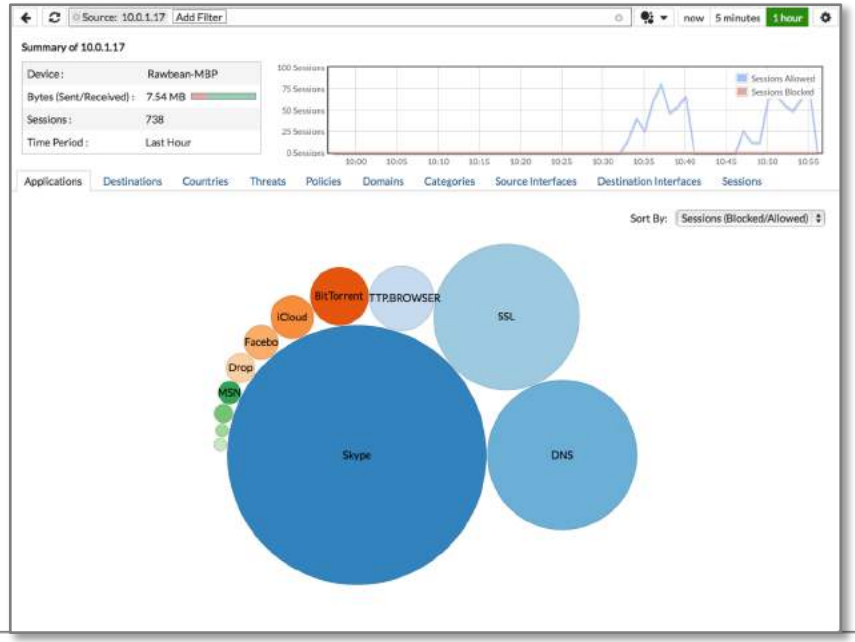
- MSSP umožňuje:
  - » monitorování stavu služeb
  - » nastavení nových zákazníků
  - » řešení problémů (trouble ticketing)

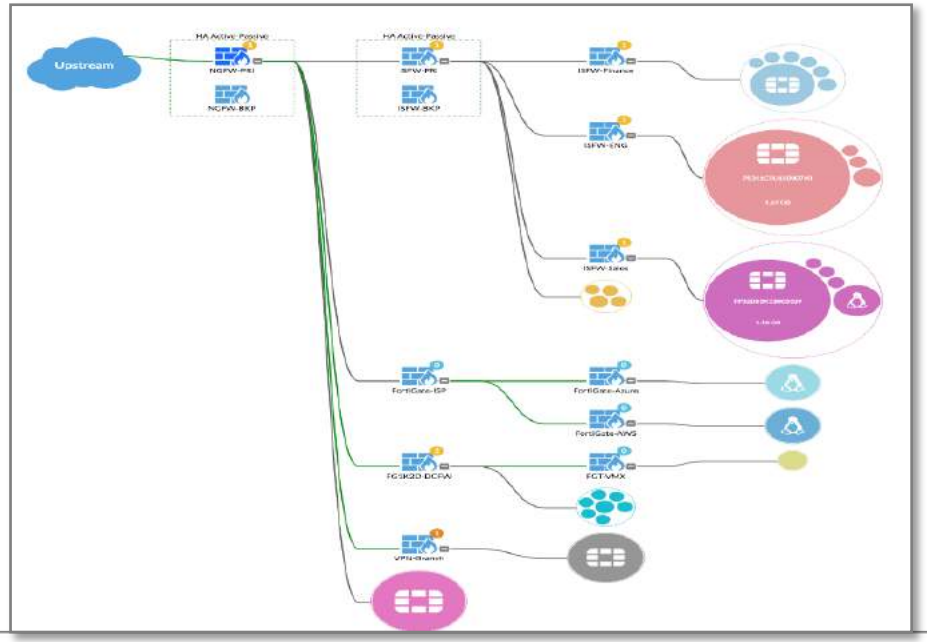


Management


FortiManager
FortiPortal
FortiClient EMS
FortiCloud
FortiCloud MSSP
Orchestrator FDND


FortiGate VM64-KVM Fabric_Core
Security_Fabric_Preview
admin
Dashboard
Main
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
System Information
Licenses
Security Fabric: Security-Fabric
Sessions
Bandwidth - Internet Access (port1)
Security Fabric Score
Advanced Threat Protection Statistics
Session Rate
Memory
Inbound 49.99 kbps
Outbound 10.91 kbps
Current sessions 28
Current usage 65%


Source: 10.0.1.17
Add Filter
Summary of 10.0.1.17
Device: Rawbean-MBP
Bytes (Sent/Received): 7.54 MB
Sessions: 738
Time Period: Last Hour
Applications
Destinations
Countries
Threats
Policies
Domains
Categories
Source Interfaces
Destination Interfaces
Sessions
Sort By: Sessions (Blocked/Allowed)
BitTorrent
HTTP.BROWSER
SSL
iCloud
Facebook
Drop
MSN
Skype
DNS


Upstream

OTEVŘENOST - Fabric Alliance Ecosystem

Cloud

- amazon web services
- Microsoft Azure
- ORACLE
- IBM Security
- HPE Helion

SDN

- CISCO
- nuagenetworks
- ADVA Optical Networking
- BROCADE
- openstack
- CLOUDIFY

Endpoint

- Symantec
- McAfee Together is power.
- SentinelOne
- Attivo NETWORKS
- CARBON BLACK ARM YOUR ENDPOINTS
- ziften

Management

- tufin
- algosec
- FIREMON
- servicenow

Vulnerability/SIEM

- WhiteHat SECURITY
- QUALYS Continuous Security
- Hewlett Packard Enterprise

IoT/OT/NAC

- NOZOMI NETWORKS
- ForeScout
- BRADFORD NETWORKS
- Pulse Secure

Identity

- Centrify
- CYBERARK

Technology

- intel
- VERISIGN
- ribbon communications

Automatizace a koordinace

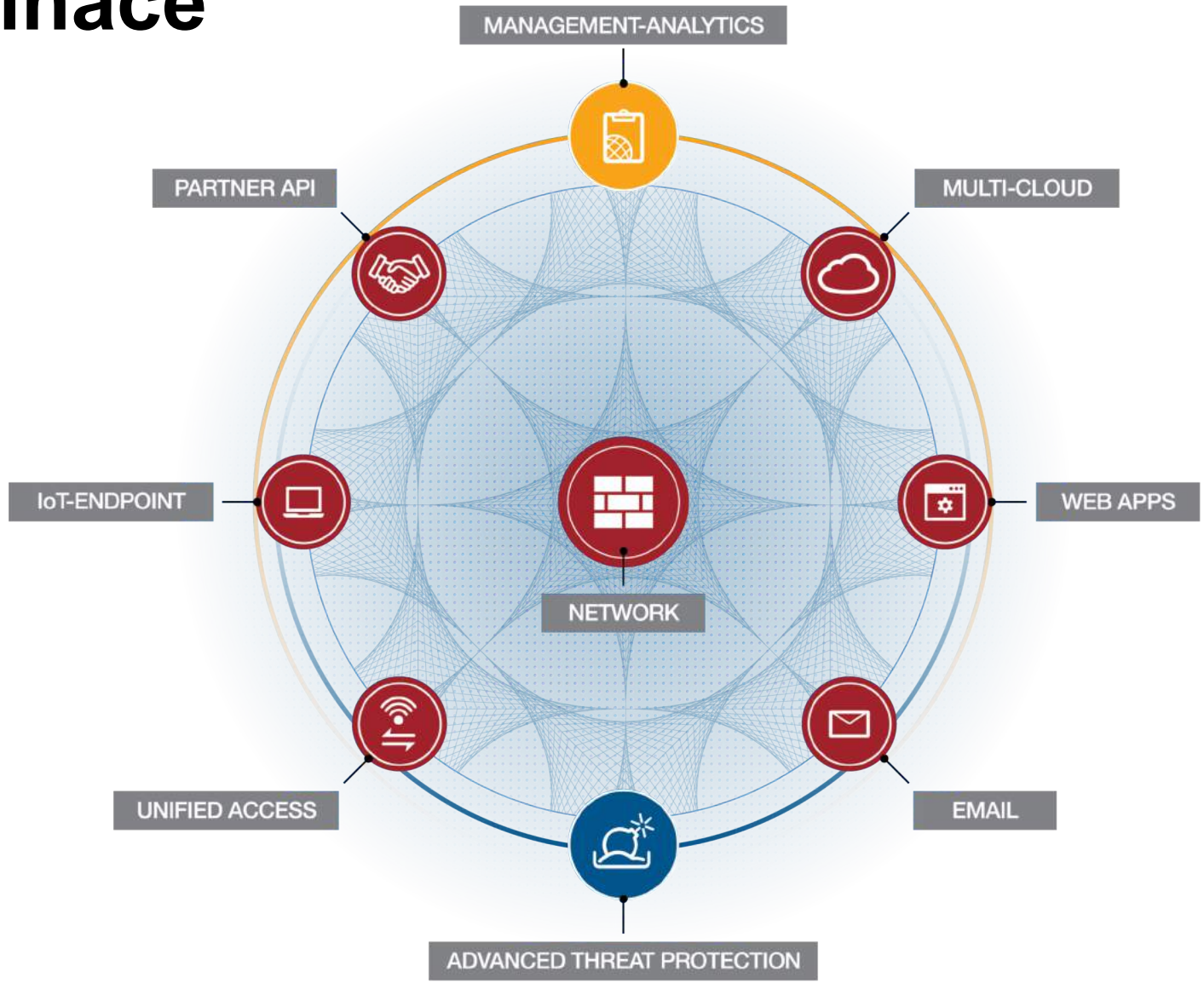
A Security Architecture that provides:

BROAD Visibility & Protection of the Digital Attack Surface

INTEGRATED Detection of Advanced Threats

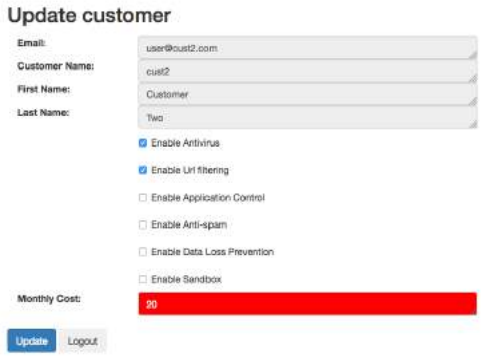
AUTOMATED Response & Continuous Trust Assessment

Delivered as:



MSP PLATFORMA – SPRÁVA A SLUŽBY

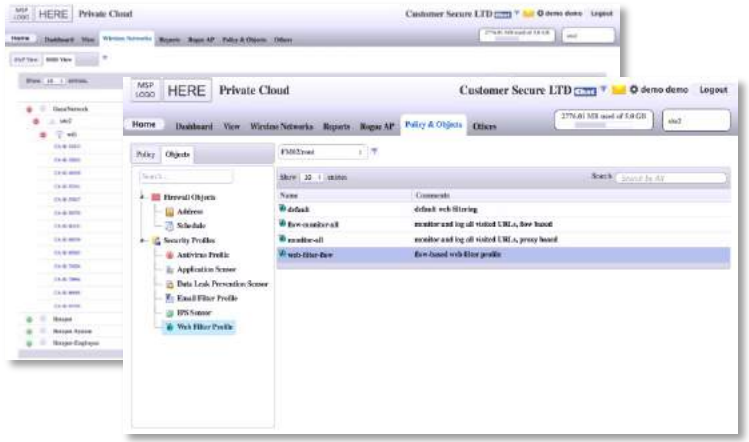
- **Management a analytika**
  - » FortiSIEM, FortiManager, FortiAnalyzer
- **Autentifikace přístupu**
  - » FortiAuthentificator
- **Základní bezpečnostní služby**
  - » NGFW (Firewall, IPS, VPN, Anti-Vir, Antispam, Anti-Malware, Web filtr, Application Control)
- **Doplňující účelová řešení**
  - » 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



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

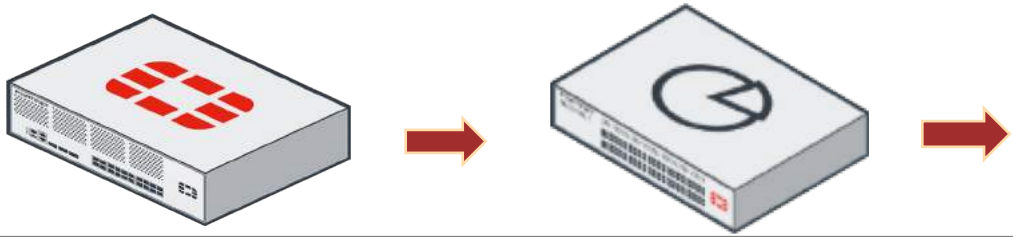
Obchodní podpora

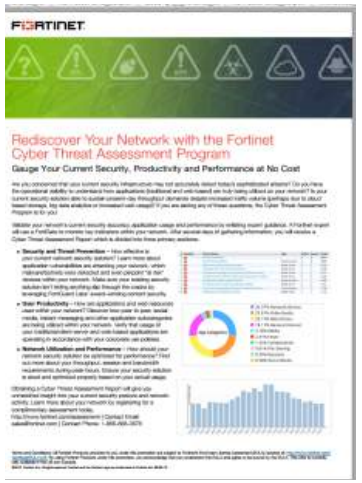
CTAP - Bezplatný test sítě

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

Pohled do vaší sítě pokrývající klíčové oblasti:

» ***Bezpečnostní hrozby*** *– odhalíme slabá místa, malware, botnety, atd.*
» ***Produktivita*** *– přehled o uživatelích 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'

Martin Fišer
mfiser@fortinet.com
602 303 265