Moderní bezpečnostní hrozby: lze se ubránit?

Jan Pinta, CEO

H-Square ICT Solutions s.r.o.

- Bezp
- Jaké
  - Fi
  - IP
  - Ar
- Byli j
- A víte
- Znáte
- A co

Bezpečnostní trendy 2018

Data Center Consolidation

Secure SaaS

Expanding Encrypted Traffic

EU GDPR in May 2018

Public Cloud

Cyber Crime Ransomware

Opravdu se to děje

- Narůstající množství kyberútoků – meziročně o 27,4 % (za posledních 5 let trojnásobně). *
- V roce 2017 čelilo 77 % společností nějaké formě kyberútoku. *
- Nízká cena útoků a jejich vysoká míra úspěšnosti.
- Nebezpečí ztráty dat, odcizení a zveřejnění citlivých informací.
- Útoky jsou vedené na všechny společnosti bez rozdílu.
- Finanční dopady úspěšného útoku bývají mnohonásobně vyšší, než investice vložené do preventivních opatření.

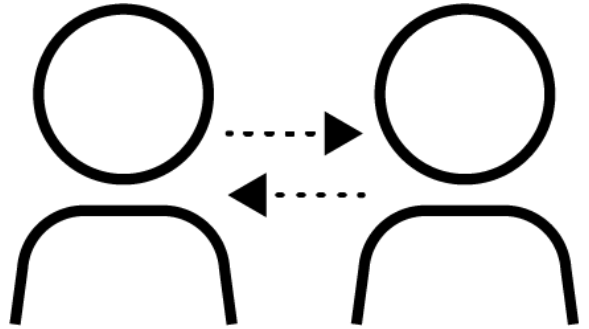
* Zdroj: Accenture, Cost of Cyber Crime Study 2017

Opravdu se to děje

- Příklady (2017):
  - NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs and cost up to $300M.
  - NotPetya ransomware outbreak cost Merck more than $300M per quarter.
  - FedEx estimates ransomware attack cost $280M.
- Lze se bránit?
  - Úroveň používaných bezpečnostních technologií úměrná úrovni útoků.
  - Bezpečnostní strategie a provázanost používaných technologií.
  - Nestrkat hlavu do písku, nezůstávat v roli snadné oběti a poučit se z chyb ostatních.

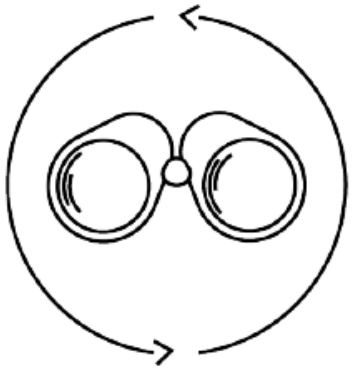
Bylo nebylo…

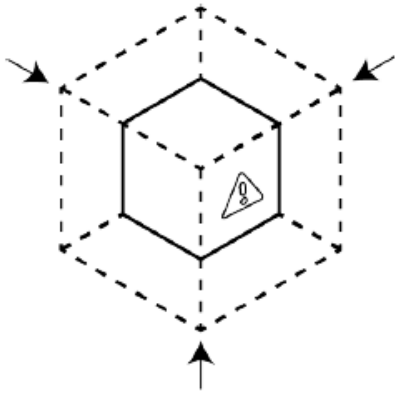
- významná energetická společnost v ČR, provozovatel KI státu
- 2015 – formování požadavků na zvýšení bezpečnosti ICT infrastruktury, plánování a výběr bezpečnostní platformy
- 2016 – potřeba zvýšení síťové bezpečnosti, viditelnosti, moderní ochrany na úrovni aplikací, uživatelů a obsahu, dekrypce SSL provozu
- 2017 – potřeba pokročilé ochrany koncových stanic, účinná obrana proti malware/ransomware, náhrada tradičního AV řešení
- 2018 – ?

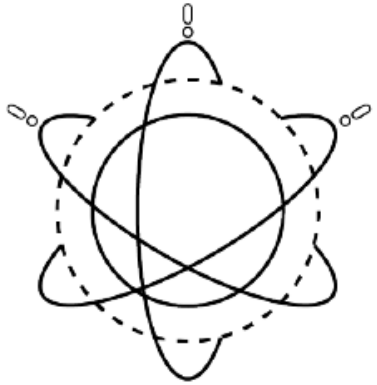


H-SQUARE ICT SOLUTIONS

2015 – Volba bezpečnostní platformy



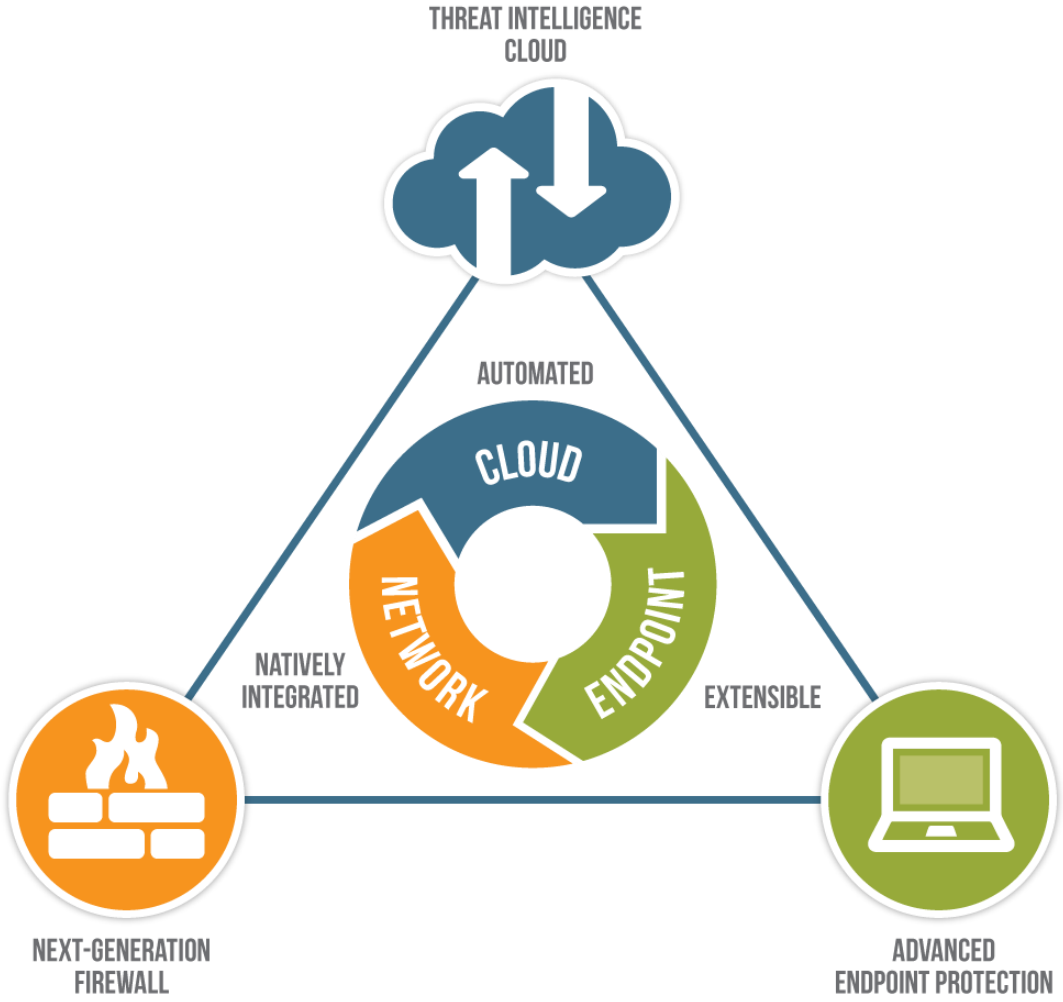




ÚPLNÁ VIDITELNOST	ZMENŠENÍ PLOCHY PRO ÚTOK	ZAMEZENÍ VŠEM ZNÁMÝM HROZBÁM	ZJIŠTĚNÍ A ZASTAVENÍ NEZNÁMÝCH HROZEB
• Síť i koncové body • Všechny aplikace, včetně cloud a SaaS • Všichni uživatelé a zařízení, ve všech umístěních • Mobilní uživatelé • Šifrovaný provoz	• Povolení žádoucích aplikací • Zastavení "špatných" aplikací • Omezení funkcí aplikací • Omezení rizikových stránek a obsahu	• Zneužití zranitelností • Škodlivý kód • Command & control • Škodlivé a phishingové weby • Špatné domény • Ukradená hesla a údaje	• Neznámý škodlivý kód • Zero-day zneužití zranitelností • Nové chování útoků

H-SQUARE ICT SOLUTIONS

2015 – Volba bezpečnostní platformy



H-SQUARE ICT SOLUTIONS

2015 – Volba bezpečnostní platformy

2016 – Next Generation Firewall

Požadavky

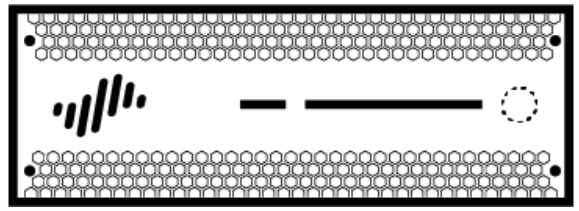
- náhrada perimetrových firewallů
- náhrada původních IPS sond
- jednotná platforma pro HQ, pobočky i DC
- náhrada proxy serveru + kontrola přístupů vázaná na identitu
- dekrypce odchozích SSL spojení
- vysoká škálovatelnost
- centrální management

H-SQUARE ICT SOLUTIONS

2016 – Next Generation Firewall

Palo Alto Networks NGFW

- nasazeny desítky HA párů PAN NGFW
- různé modelové řady dle požadovaných parametrů při zachování jednotné platformy a managementu
- migrace původních stavových pravidel do next generation podoby
- dekrypce vybraného SSL provozu
- minimální odstávky v řádu desítek sekund
- nasazení centrálního managementu Panorama



2017 – Pokročilá ochrana koncových bodů

Požadavky

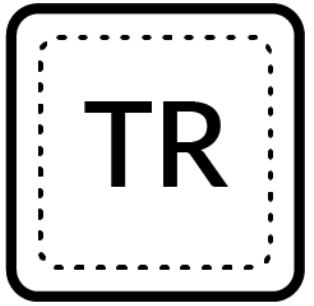
- vyřešit nedostačující ochranu cca 1500 koncových bodů
- nalézt řešení, které ideálně nahradí tradiční AV/HIPS technologii
- ochrana před známými i neznámými hrozbami, moderními útoky, malware, fileless, ransomware a zranitelnostmi
- co nejširší podpora operačních systémů a platforem (PC, servery, VM)
- jediný agent, s co nejnižšími nároky na výkon
- snadná integrace a provázanost
- centrální správa

H-SQUARE ICT SOLUTIONS

2017 – Pokročilá ochrana koncových bodů

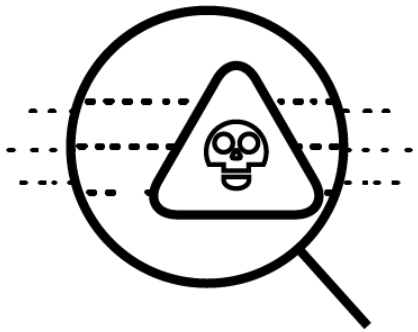
Traps – Advanced Endpoint Protection

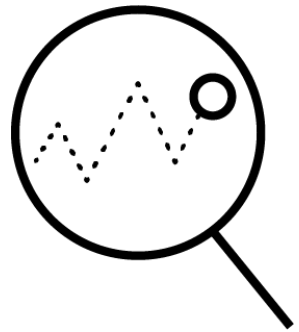
- kombinace více metod pro blokování malware a zranitelností, známých i neznámých hrozeb, včetně zero-day útoků, ransomware
- plnohodnotná náhrada tradičních AV řešení
- podpora Windows, Windows Server, MacOS, Linux, VM (ESX, Hyper-V, Citrix, Oracle) + ochrana OS po ukončení podpory
- minimální nároky < 0.1% CPU, 50 MB RAM, 250 MB HDD
- žádné skenování, signatury, virové databáze
- vysoká škálovatelnost, centrální správa, snadný deployment



2018 - Co dál?

- Ochrana VM prostředí
- Ochrana cloudových služeb a SaaS aplikací
- Behaviorální analýza datových toků
- Pokročilá identifikace útočníků, forenzní analýza útoků

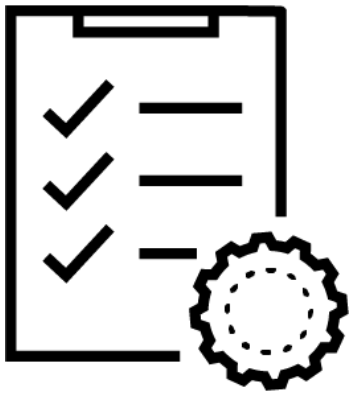




H-SQUARE ICT SOLUTIONS

Splněné cíle

- Definování jasné bezpečnostní strategie
- Zaměření na integritu a provázanost řešení
- Úplná viditelnost napříč infrastrukturou
- Ochrana proti známým i neznámým hrozbám
- Zjednodušení správy a budoucího rozvoje
- Snížení počtu incidentů a odhalení zranitelností
- Významné zvýšení bezpečnosti



GDPR compliance

- Bezpečné zpracování a uchování dat
  - ✓ Next Generation Security Platform poskytuje zabezpečení na úrovni aplikací, sítě, koncových bodů i cloudu
- Prevence úniku citlivých dat
  - ✓ Automatizovaná a aktivní preventivní ochrana
- Zjištění a nahlášení úniku citlivých dat
  - ✓ Panorama, ESM, Magnifier, reporting

H-SQUARE ICT SOLUTIONS

Kdo jsme?

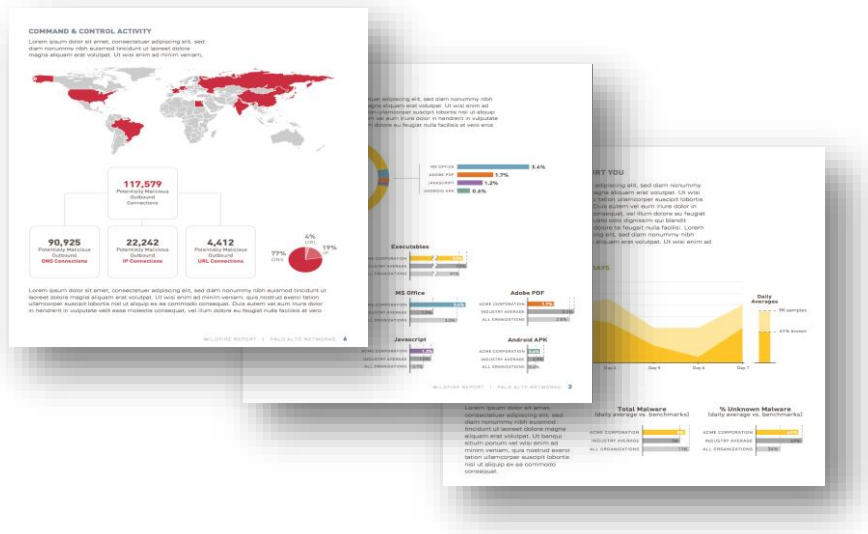
H-Square ICT Solutions s.r.o.

- Platinový partner předního světového výrobce bezpečnostních technologií Palo Alto Networks + Traps Specialized Partner
- Zaměření na bezpečnost nové generace, komplexní ochranu podnikové ICT infrastruktury proti moderním hrozbám a útokům
- Zkušený tým odborníků, nejvyšší úroveň certifikací
- Rozumíme tomu, co děláme
- Baví nás to
- Bude to bavit i Vás?

H-SQUARE ICT SOLUTIONS

Zkuste to!

- **Security Lifecycle Review**
  - risk assessment a identifikace hrozeb a zranitelností v datovém provozu
  - umístění pasivní NGFW sondy
  - zpracování reportu a vysvětlení nálezů
- **Ultimate Test Drive**
  - Hands-on labs (cca 3 hod.)
  - NGFW + Traps
- **Demo / Proof-of-Concept u vás**



Děkuji za pozornost

H-SQUARE
ICT SOLUTIONS

www.h-square.cz | info@h-square.cz