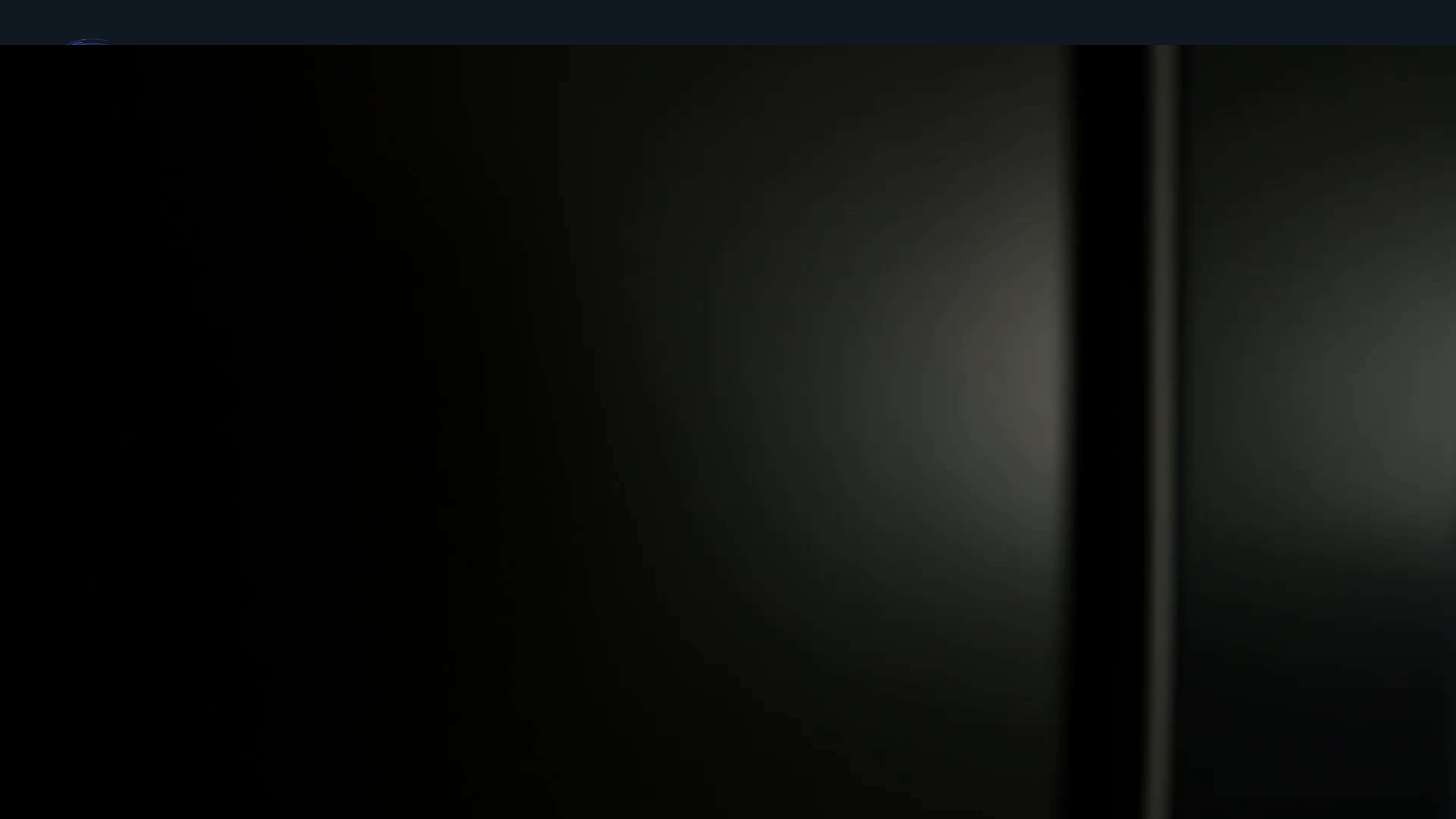
thein.digital



thein.security

Situace.

- Hybridní prostředí
- Nedostatek IT specialistů
- Práce odkudkoliv
- Budeme napadeni?

thein.security

Situace.

- Hybridní prostředí
- Nedostatek IT specialistů
- Práce odkudkoliv

Hrozby – RIZIKA.

1 Pozdní reakce na hrozbu

Útočník se může v prostředí pohybovat dlouhou dobu a nemusí být vůbec odhalen.

2 Velké provozní ztráty

Ochromení IT znamená ochromení činnosti firmy.

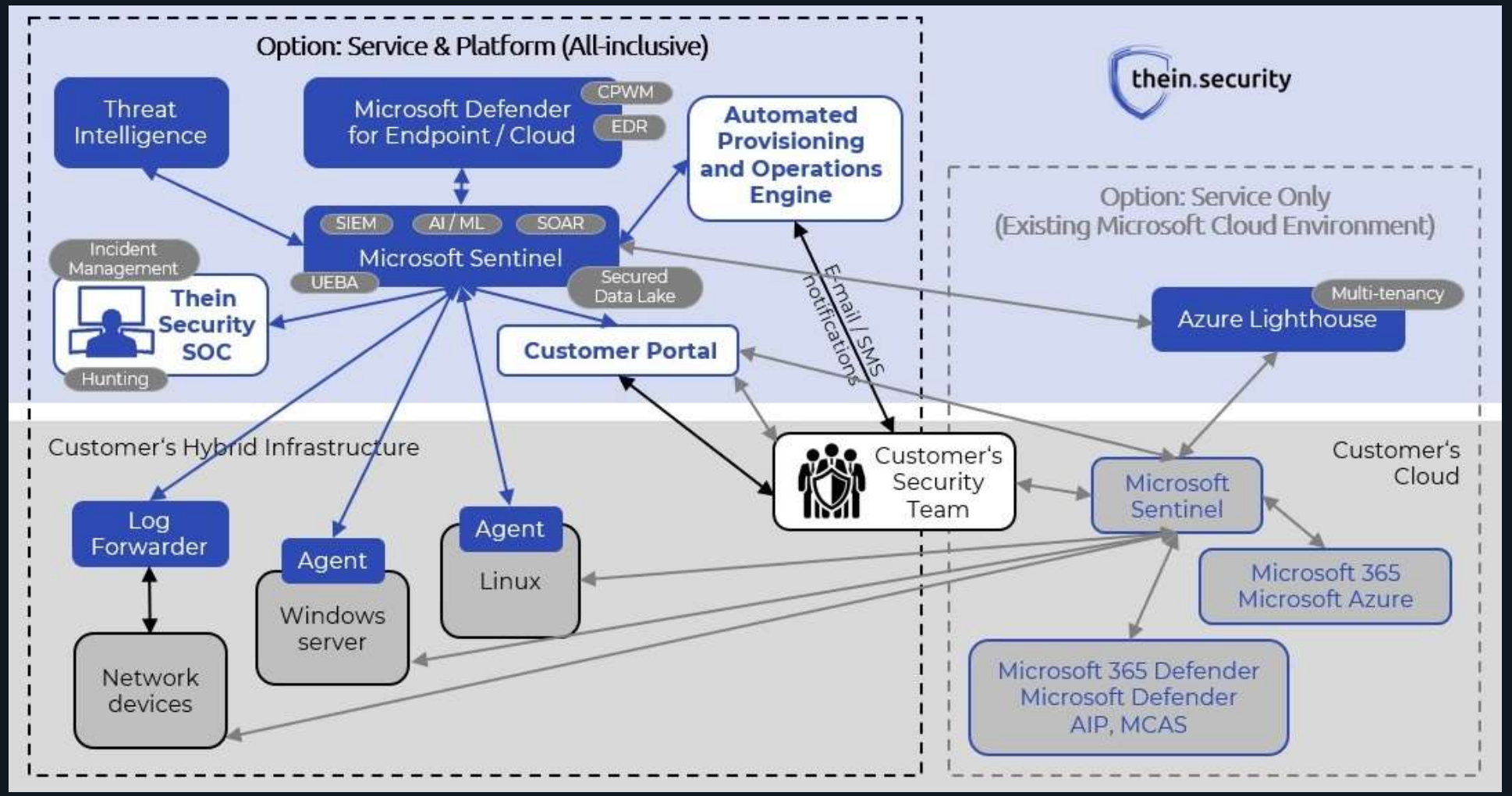
3 Únik citlivých dat

Získat data zpět je nákladné a nemusí se to vůbec podařit.

4 Dopad na značku a reputaci

Ztráta dat poškodí image společnosti v očích zákazníků.

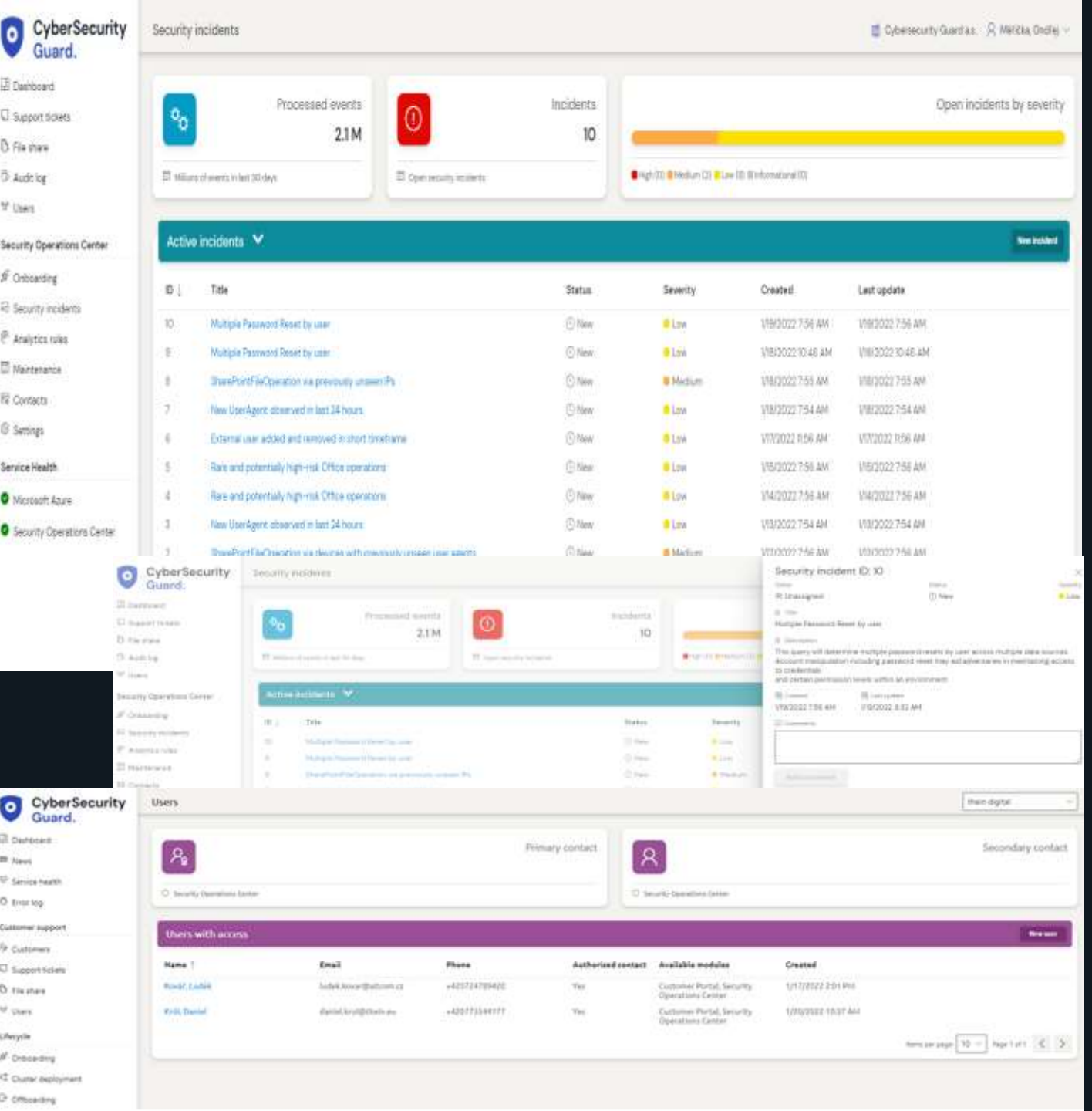
High level architektura



Díky cloud-native platformě založené na Microsoft technologiích a díky námi vyvinutým komponentám monitorujeme čistě cloudové i hybridní IT infrastruktury.

S minimálními implementačními náklady a rychlým nasazením.

Cybersecurity Guard portál



1 Zákaznický portál

2 Incidenty

3 Reporty

4 Smluvní podmínky

thein.security

Čím se lišíme.

- Vytěžujeme Vaše technologie a investice do Microsoft technologií
- Pokrýváme hybridní prostředí, cloud native technologie
- Dohled a řešení incidentů 24 / 7 / 365
- Změna bezpečnostní situace – řízení bezpečnosti.
- **Thein Soc tým pracuje pro Vás**

thein security

Naši mezinárodní partneři.

thein security

NETSCOUT
Guardians of the Connected World

Temná strana DDoS -

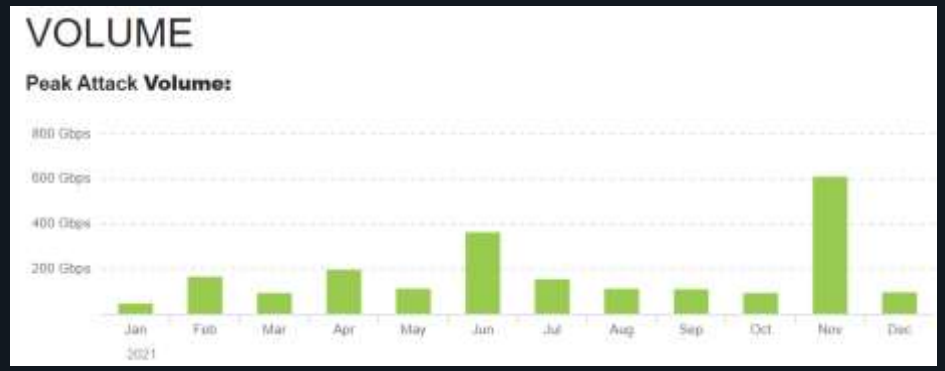
DDoS vydírání a trojitá hrozba

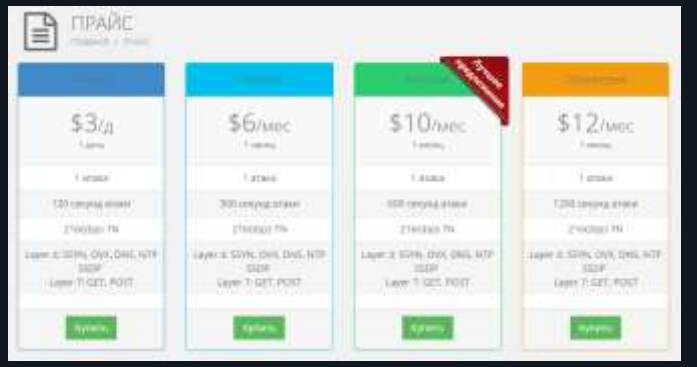
"DDoS vás zasáhne, už to není otázka jestli-
nebo kdy- ale jak na vás zaútočí"

Alexander Tomik, Sales Engineer Central Eastern Europe
Alexander.Tomik@netscout.com

Oldřich Gosman, Security Operation Center
oldrich.gosman@thein.eu

V roce 2021 zasáhlo svět téměř než 10 milionů DDoS útoků – a za jakou cenu?





DDoS Extortion & Triple Threat (Ransomware + data theft + DDoS)

DDoS Extortion (aka RDDoS)

Ačkoli DDoS vydírání není nové, objevují se vysoce profilované kampaně DDoS vyděračských útoků.

- **Lazarus Bear Armada (LBA)**
- **Fancy Lazarus**
- **REvil ransomware group**

Zdá se, že útočníci nyní považují DDoS útoky za zločinné snahy samy o sobě - na rozdíl od jednoho pilíře trojitých vyděračských útoků - což znamená, že je třeba očekávat zkušenější kampaně vydírání DDoS, protože sofistikované skupiny ransomwaru tuto taktiku ovládají.

Ransomware Gangs

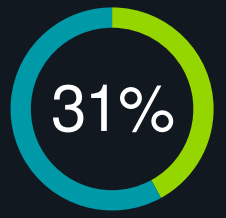
Ve zprávě 1H 2021 Threat Intelligence jsme za,zanmenali že několik různých skupin provádějících operace ransomwaru se také přesunulo na území útoku DDoS, aby vyvinuly větší tlak na oběti, aby zaplatily požadované výkupné.

Pro tuto zprávu vytvořila Palo Alto, partner Threat Intelligence, souhrn ransomwarových gangů, které také používají DDoS k vydírání obětí, aby zaplatily výkupné.

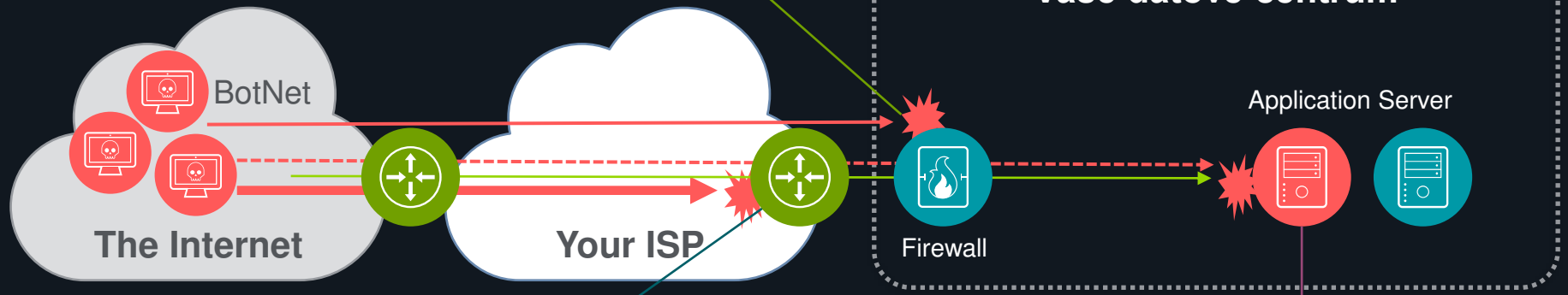
Z výseldků zprávy je patrné, že následující skupiny používají DDoS jako součást svých operací.

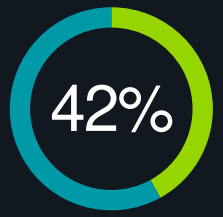
Nejnovější trendy DDoS útoků - Složitost

Fakt: Moderní DDoS útoky jsou složité: tvoří je dynamický multivektor

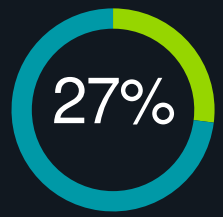


TCP State-Exhaustion Attacks
- Selhání stavových zařízení (Load Balancers, Firewalls, IPS)
- 2x nárůst (oproti 16 % v předchozím roce)
- U 54 % došlo k selhání
-





Volumetric Attacks
- Velké (až 1,7 Tb)
- Saturuje linky
- 91% podniků zažilo nasycení linek

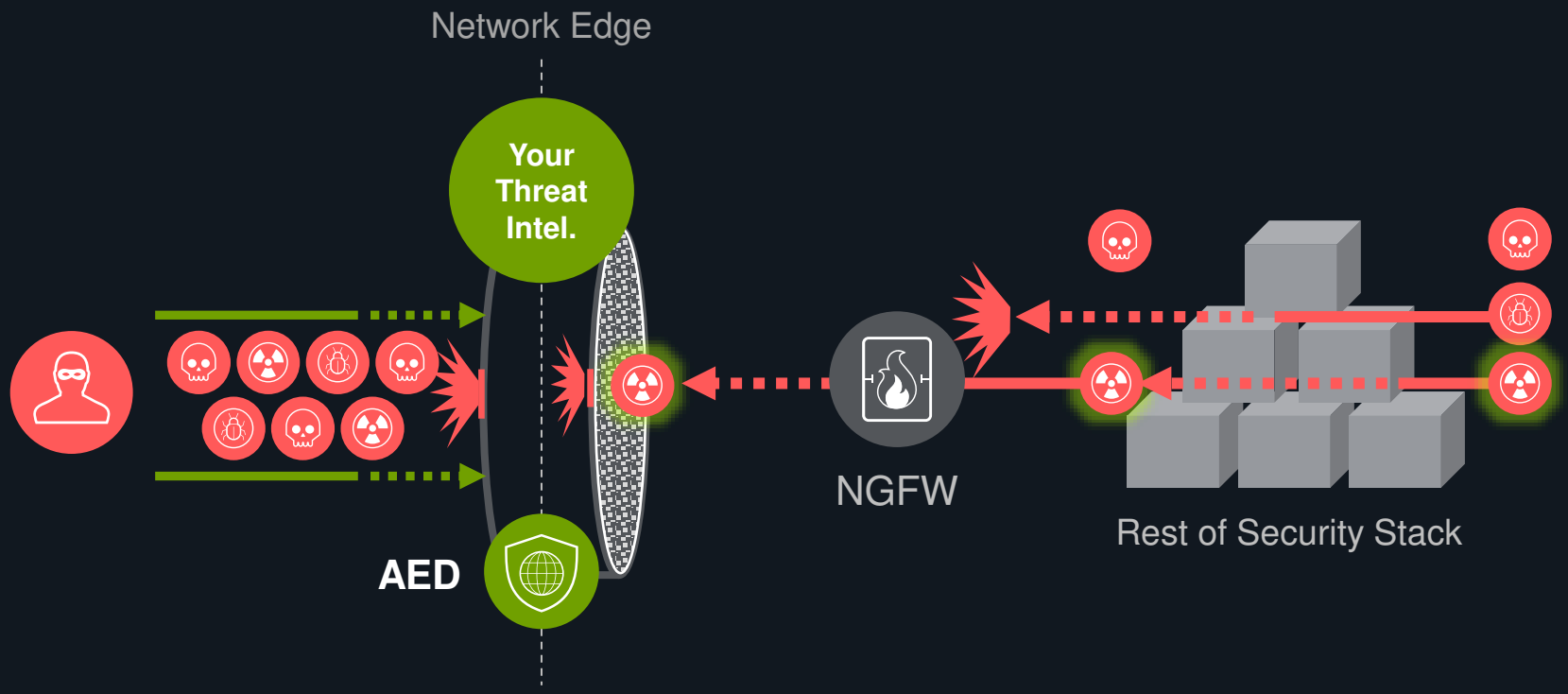


Application Layer Attacks
- Malé a pomalé, stealth útoky
- Zhroucení aplikačních serverů

Source: Arbor Networks 14h Annual Worldwide Infrastructure Security Report

Arbor Edge Defense (AED)

První a poslední linie inteligentní, automatizované obrany perimetru



PRVNÍ OBRANNÁ LINIE

- Příchozí DDoS útoky
- Nejen volumetrické
- Sondování / průzkumné / útoky hrubou silou

POSLEDNÍ OBRANNÁ LINIE

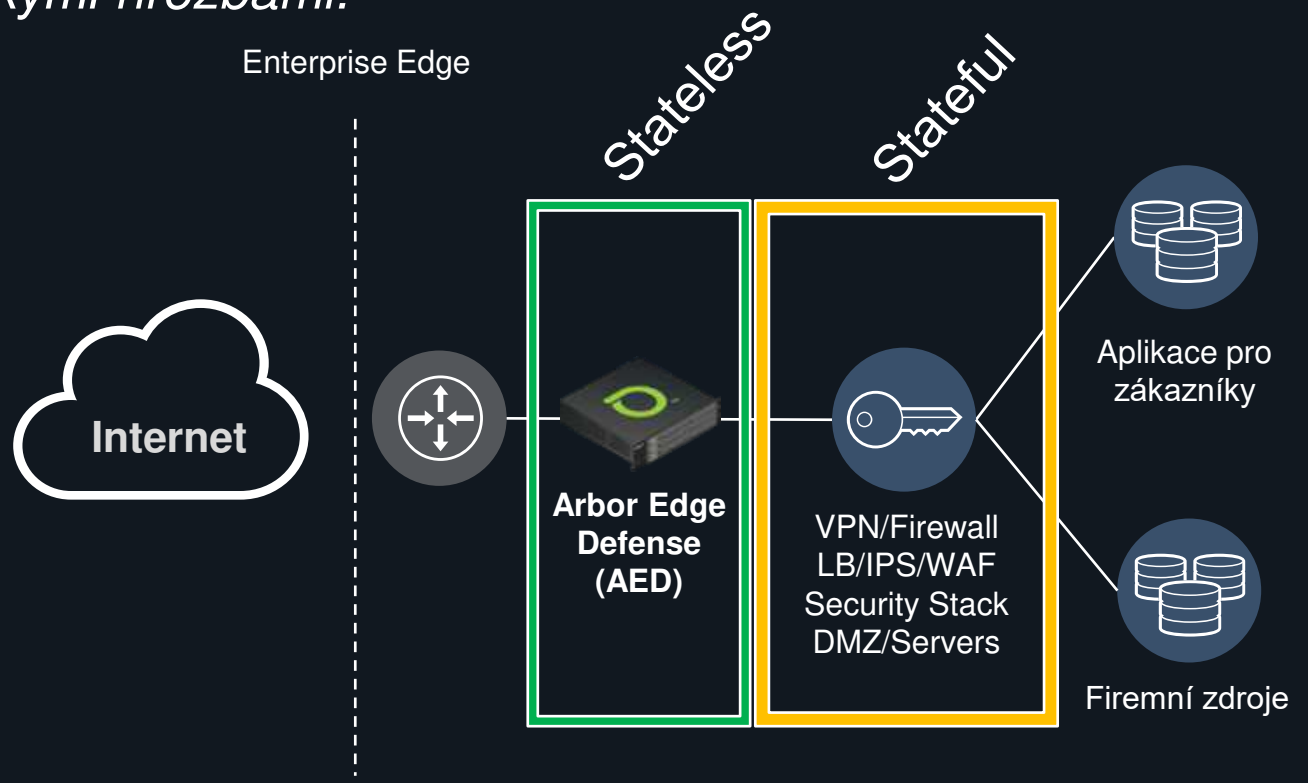
- Zablokuje odchozí komunikaci od ohrožených interních hostů.
- Nad rámec tradičního DDoS: AIF, 3rd Party IoC

Uvedení Arbor Edge Defense (AED)

Ochrana podnikového perimetru: První a poslední linie inteligentní, automatizované, bezstavové, perimetrické obrany. Poskytuje bezstavovou ochranu před vyčerpáním stavu a aplikační vrstvou DDoS. Poskytuje viditelnost a kontrolu nad celým připojením k internetu a zároveň využívá inteligenci ATLAS pro pokročilou ochranu před kybernetickými hrozbami.

Arbor Edge Defense

- Viditelnost paketů na perimetru
- Inline a transparentní pro síť
- Monitorování / detekce / ochrana v reálném čase
- Vyladěno pro podnikovou infrastrukturu
- Profesionální znalosti a zaměření na zákazníka a firemní infrastrukturu
- Chrání dostupnost všech podnikových služeb před sofistikovanými DDoS útoky
- Klíčový bod ochrany perimetru



Proč NETSCOUT ARBOR?

Lídr v oboru produktů a služeb ochrany před útoky DDoS.

20

Již řadu let Arbor dodává inovativní technologie a produkty pro zabezpečení a viditelnost sítě

1/3 = Objem internetového provozu monitorovaného projektem ATLAS

Arbor Networks je součástí NETSCOUT od roku 2015.

Kontakty pro vás.

Oldřich Gosman

+420 731 241 074

Www.theinsecurity.eu

Alexander Tomík

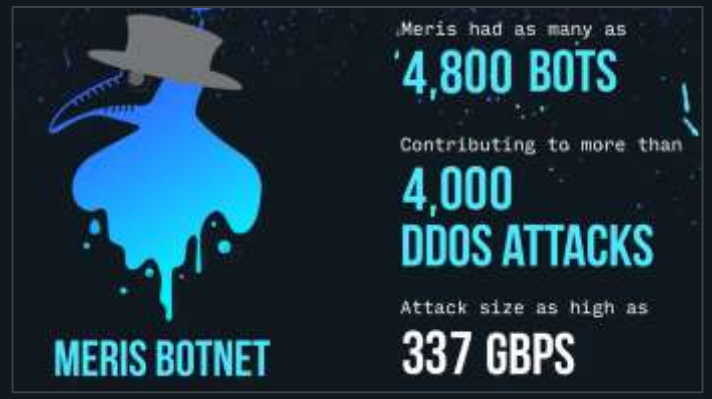
+43 664 240 92 51

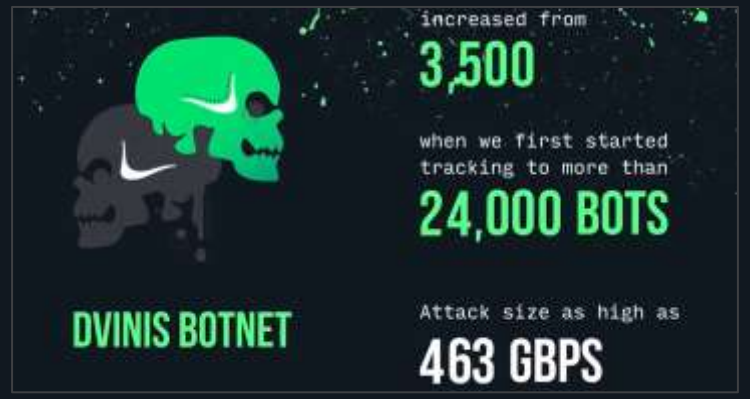
www.netscout.com

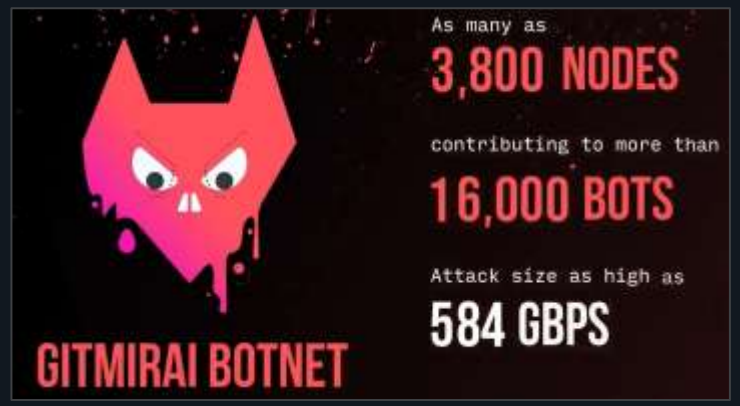
Děkujeme.

www.theinsecurity.eu

The Rise of Server-Class Botnet Armies







Mēris Botnet Snapshot

First Seen:
June 2021

Current Active Nodes: ~2,000
Peak Active Nodes: ~4,800
Attacks to Date: ~4,000
Maximum Attack Size: ~337 Gbps
Average Attack Size: ~7 Gbps

Dvinis Botnet Snapshot

First Seen:
September 2021

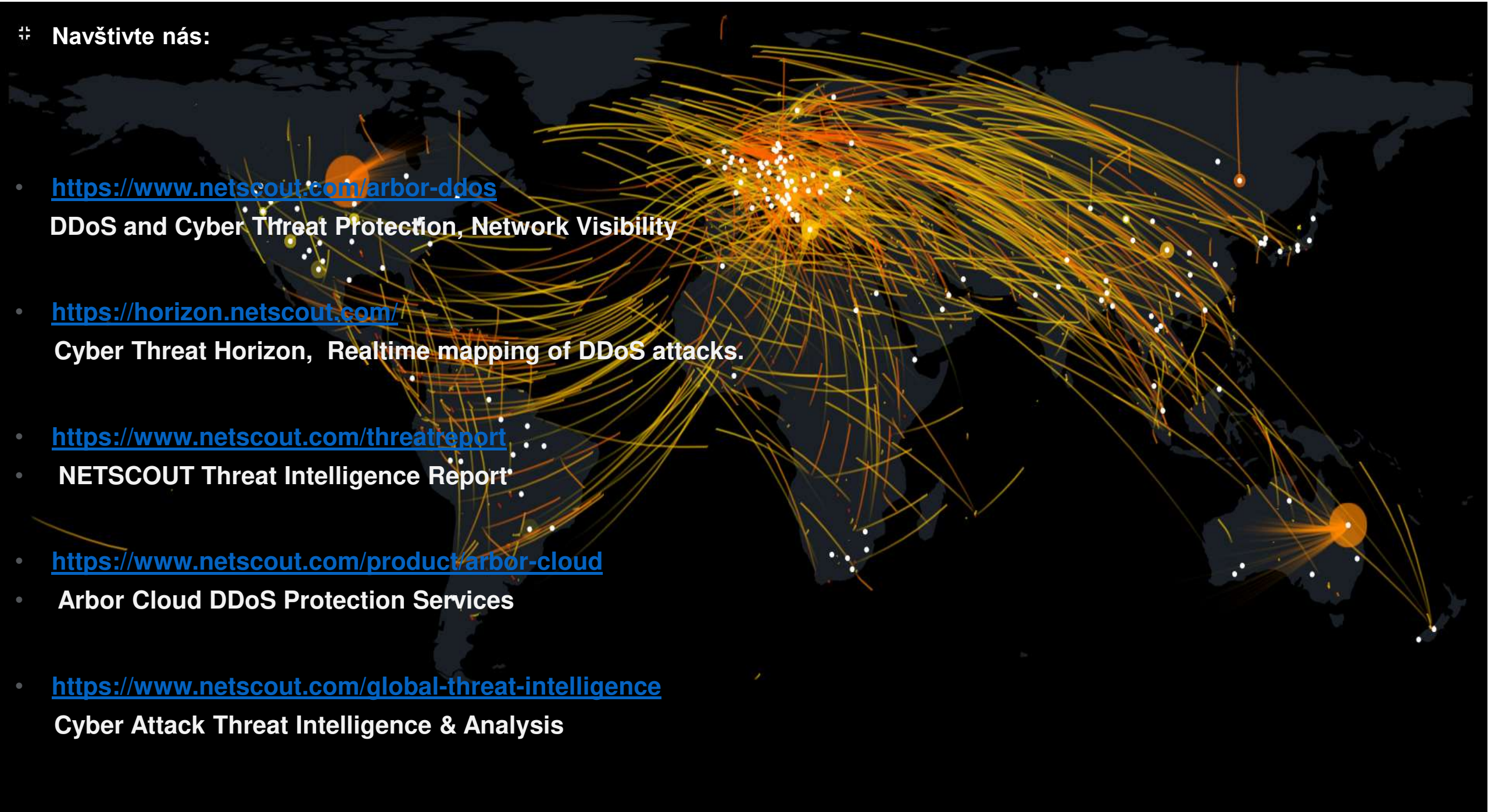
Current Active Nodes: ~24,000
Peak Active Nodes: ~24,000
Attacks to Date: ~29,000
Maximum Attack Size: ~463 Gbps
Average Attack Size: ~3 Gbps

GitMirai Botnet Snapshot

First Seen:
November 2021

Current Active Nodes: ~3,800
Peak Active Nodes: ~3,800
Attacks to Date: ~16,000
Maximum Attack Size: ~514 Gbps
Average Attack Size: ~5.4 Gbps

Navštivte nás:



- https://www.netscout.com/arbor-ddos
  DDoS and Cyber Threat Protection, Network Visibility

- https://horizon.netscout.com/
  Cyber Threat Horizon, Realtime mapping of DDoS attacks.

- https://www.netscout.com/threatreport
- NETSCOUT Threat Intelligence Report

- https://www.netscout.com/product/arbor-cloud
- Arbor Cloud DDoS Protection Services

- https://www.netscout.com/global-threat-intelligence
  Cyber Attack Threat Intelligence & Analysis