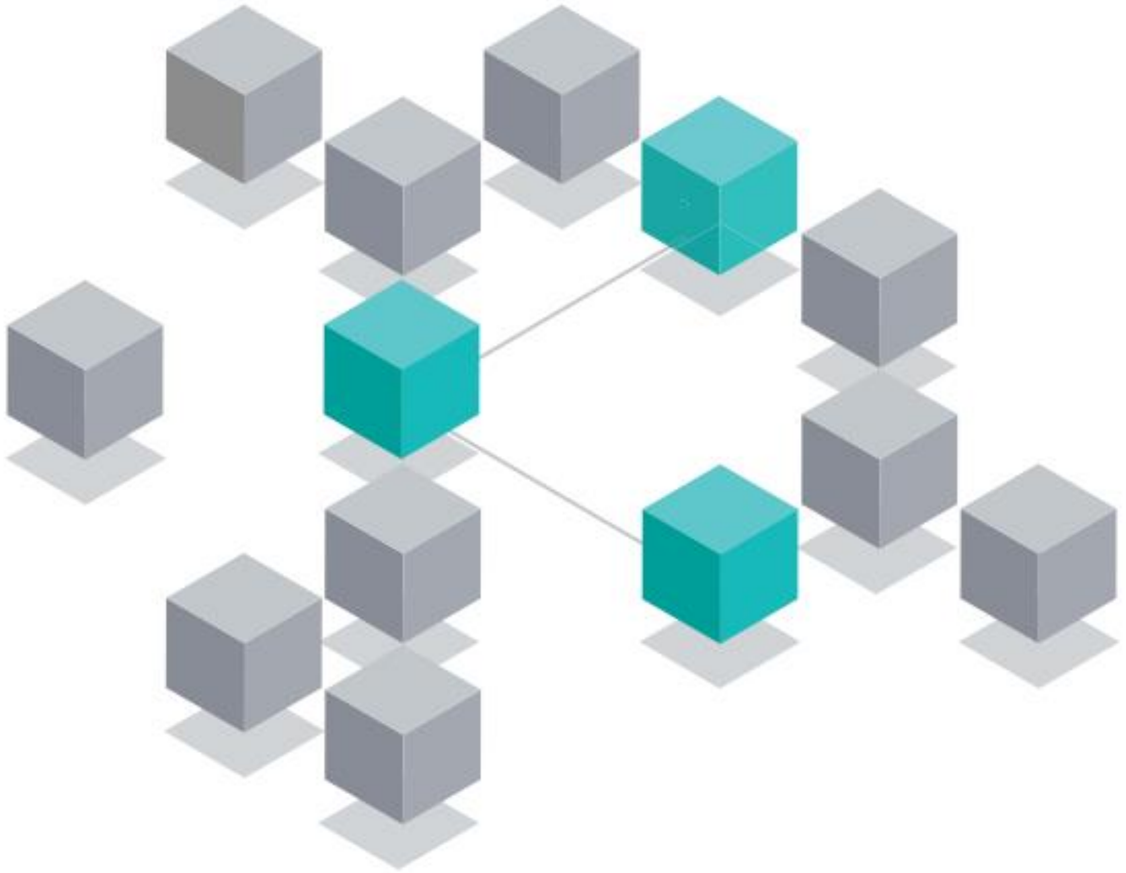
# IBM Security QRadar EDR

Zabezpečení kontinuity provozu

**Miroslav Mašek**

CyberSecurity Consultant
FreeDivision



# QRadar EDR

EDR – endpoint detection and response

Řešení pro detekci hrozeb
na koncových bodech a jejich
okamžité odstranění v reálném čase

# Proč EDR ?

Anti virus

Basic protection

+

Best-in-class EDR

Behavioral Analysis

Threat Hunting

Risk and Compliance

CERT

IT Audit

Audit

Supply chain attack detection

Heuristics based detection

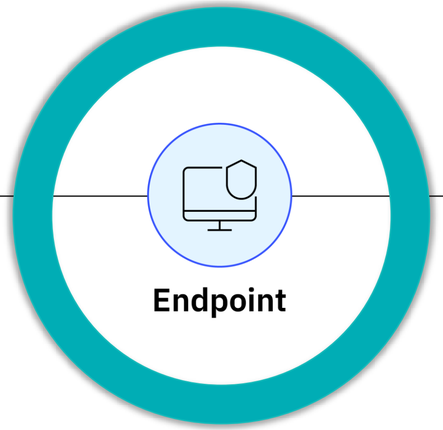
Proactive threat hunting

Block and quarantine

Organizational visibility

Post-breach investigation

Remote endpoint isolation




Real-time console to endpoint

Incident response

Signature (IOC) based detection

Regulatory compliance

Detecting known APT

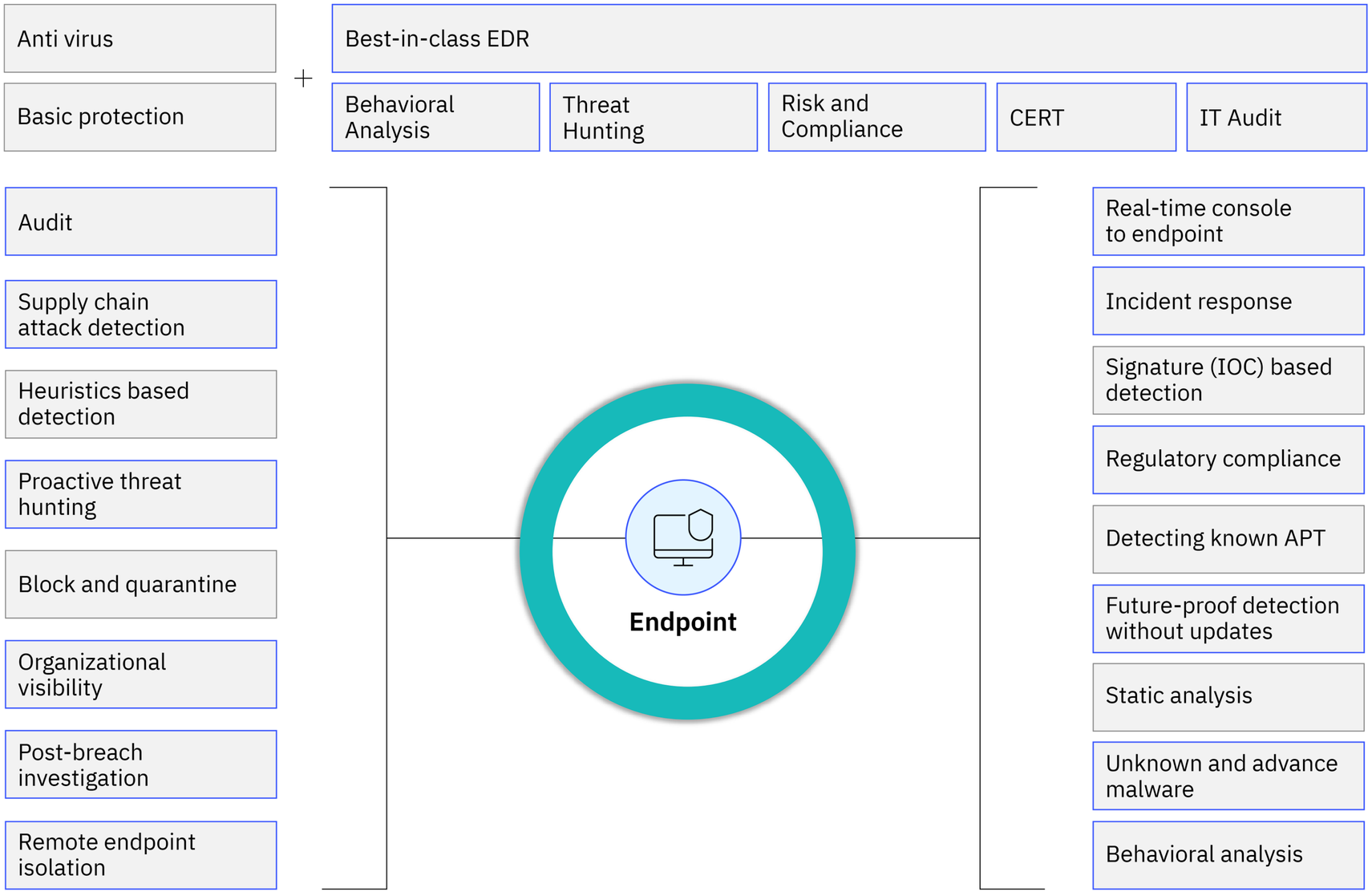
Future-proof detection without updates

Static analysis

Unknown and advance malware

Behavioral analysis

# Proč EDR ?


Anti virus
Basic protection
+
Best-in-class EDR
Behavioral Analysis
Threat Hunting
Risk and Compliance
CERT
IT Audit
Audit
Supply chain attack detection
Heuristics based detection
Proactive threat hunting
Block and quarantine
Organizational visibility
Post-breach investigation
Remote endpoint isolation
Endpoint
Real-time console to endpoint
Incident response
Signature (IOC) based detection
Regulatory compliance
Detecting known APT
Future-proof detection without updates
Static analysis
Unknown and advance malware
Behavioral analysis

# Unikátní vlastnosti

NANO OS
Monitoring na základě Live-Hypervisor

- Monitoruje operační systém (OS) zvenčí
- Poskytuje kompletní viditelnost a vhled do života aplikací
- Neviditelný pro malware
- Nelze vypnout
- Proprietární detekce high-level škodlivých chování:

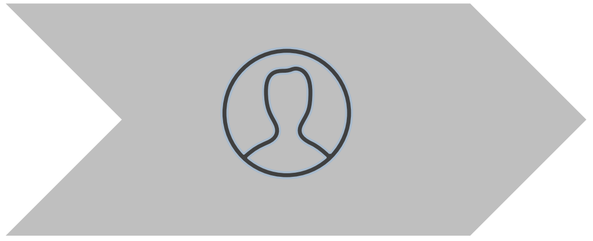
*Keylogging, Dynamic Impersonation, Credential Harvesting, Kernel Exploits, Screen captures*

POKROČILÝ LOV HROZEB
Automatický lov hrozeb řízený AI

- Přes 100 specifických parametrů pro lov hrozeb napříč koncovými zařízeními
- Strategie nápravy včetně vzdáleného vypnutí v reálném čase jedním kliknutím
- Umožňuje uživatelům tvorbu vlastních strategií detekce a postupů

LEHKOST
Bez omezení provozu

- Extrémně nízká zátěž RAM – v průměru 20Mb
- Navržena tak, aby zatížila max. 1% CPU



ÚČINNÁ ANALÝZA
Jednotná platforma pro rychlou kontextualizaci, detekci, odezvu a ochranu

- Nevyžaduje vysoce odborný personál, jednoduchá správa, minimální vklad času/práce
- Vysoká přizpůsobitelnost, tvorba vlastních scénářů detekce a odezvy, možnost multi-tenancy
- Viditelnost v reálném čase, veškeré dotazy v jedné konzoli

# QRadar EDR Architecture

## Endpoint AI & NanoOS

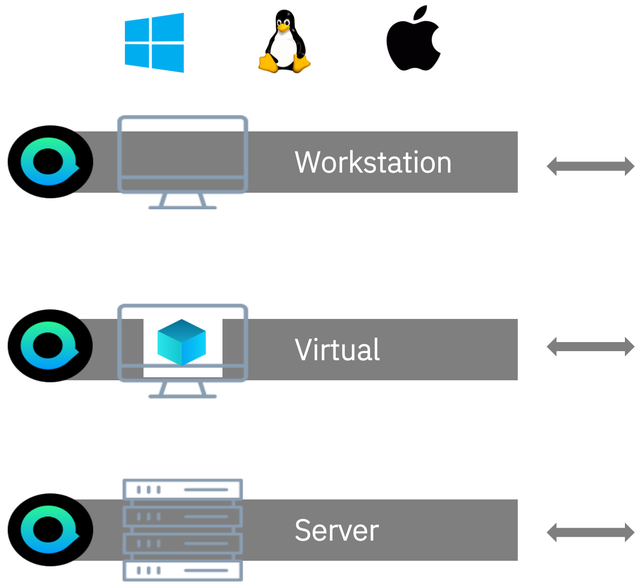
Zachycení v reálném čase

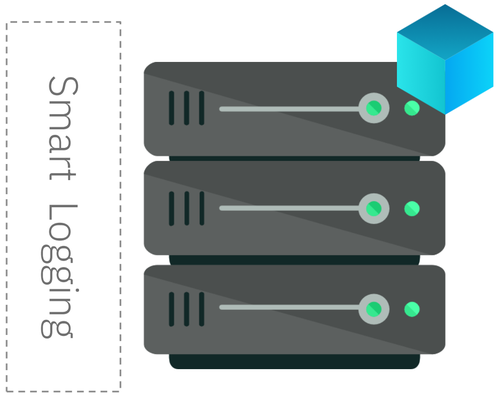
## Infrastrukturální AI

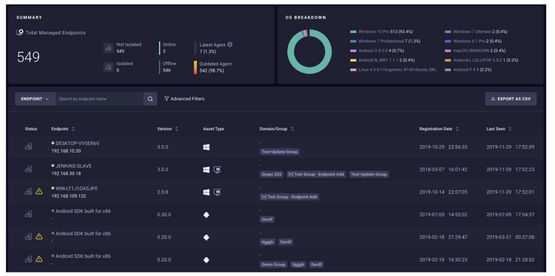
Sběr dat a analýza chování

## Jednotná konzole

Optimalizovaný postup nápravy



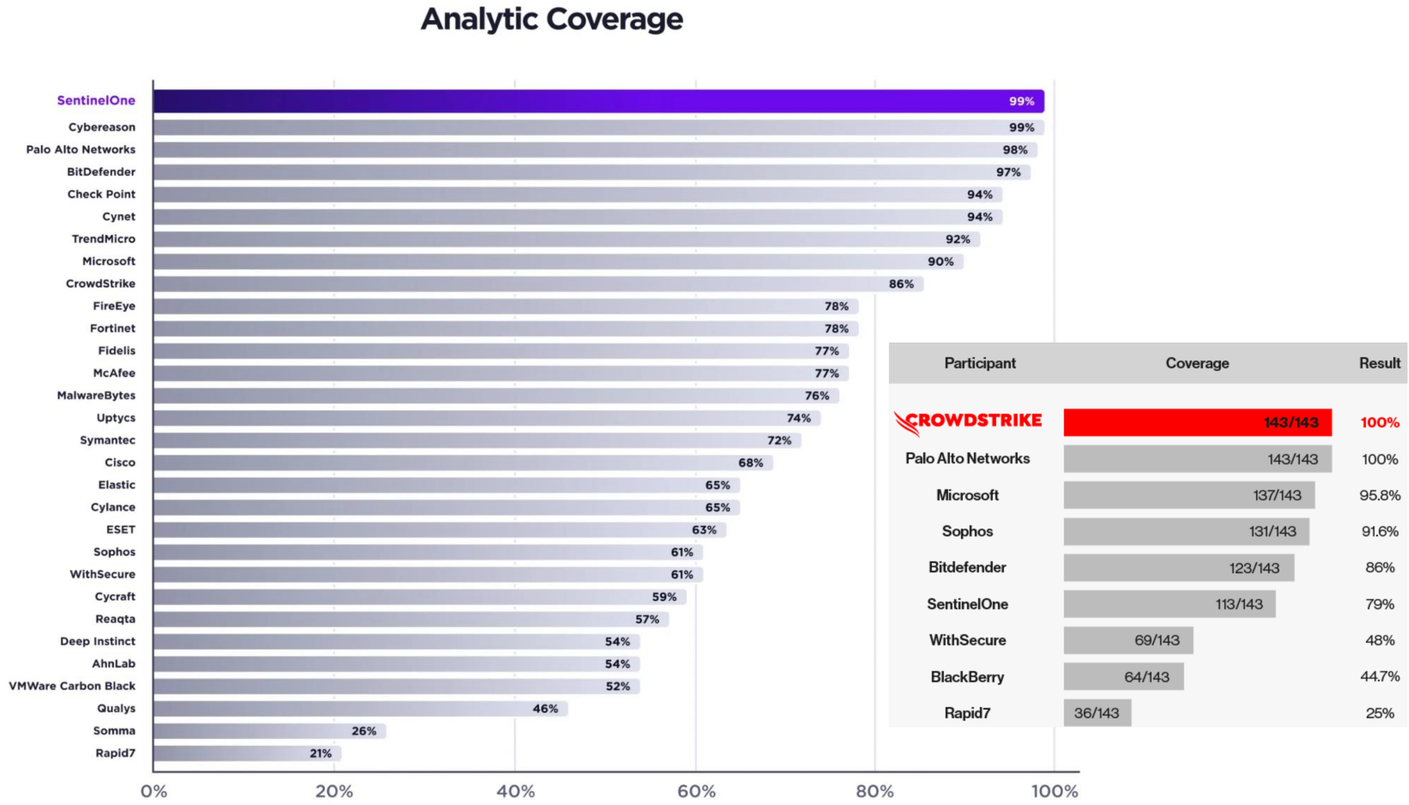




ENDPOINT AGENT

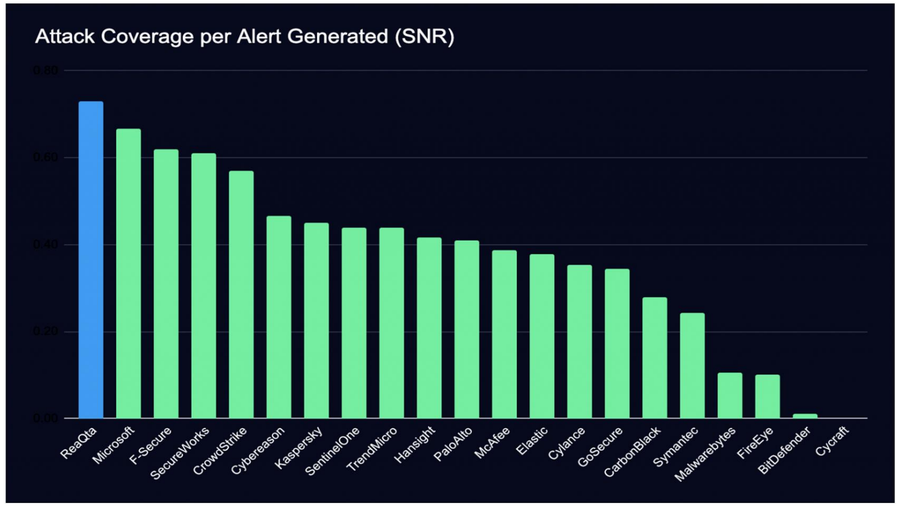
HIVE BRAIN

DASHBOARD

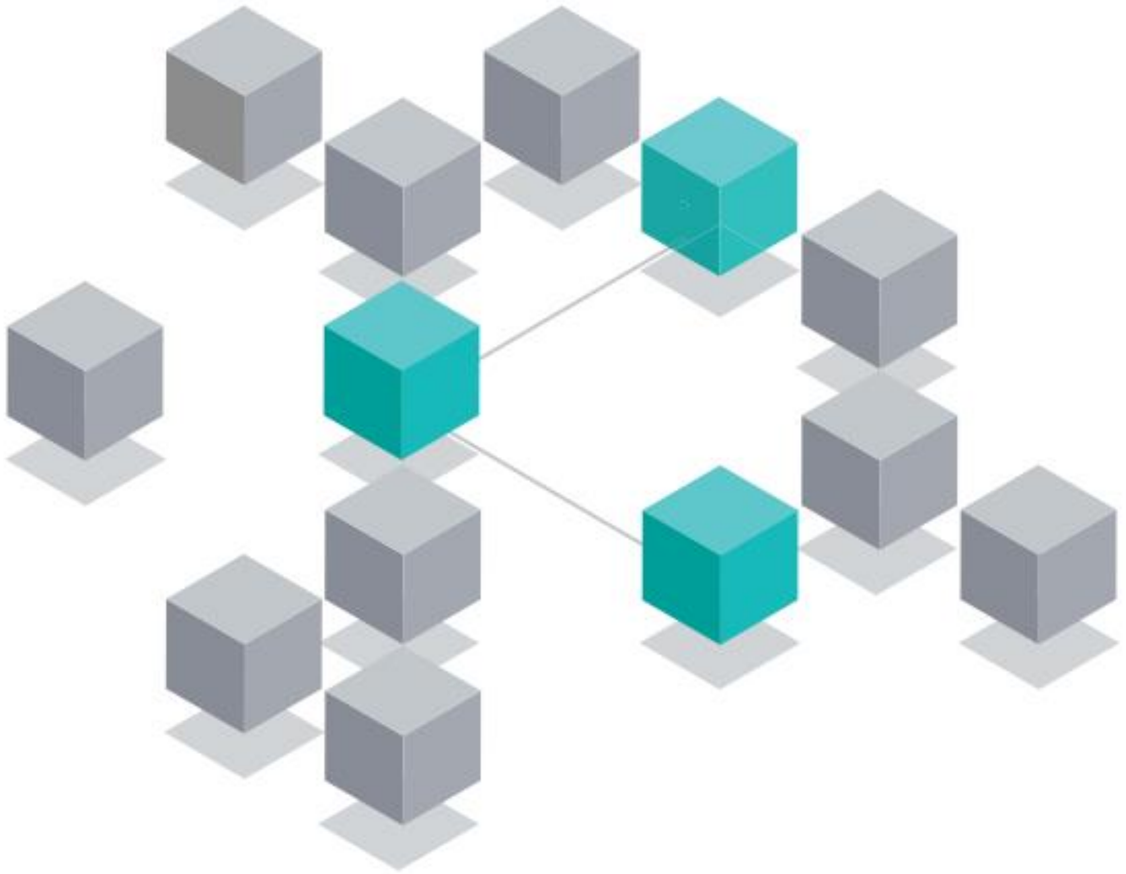
# Jak číst MITRE?




| Participant | Coverage | Result |
|---|---|---|
| CROWDSTRIKE | 143/143 | 100% |
| Palo Alto Networks | 143/143 | 100% |
| Microsoft | 137/143 | 95.8% |
| Sophos | 131/143 | 91.6% |
| Bitdefender | 123/143 | 86% |
| SentinelOne | 113/143 | 79% |
| WithSecure | 69/143 | 48% |
| BlackBerry | 64/143 | 44.7% |
| Rapid7 | 36/143 | 25% |

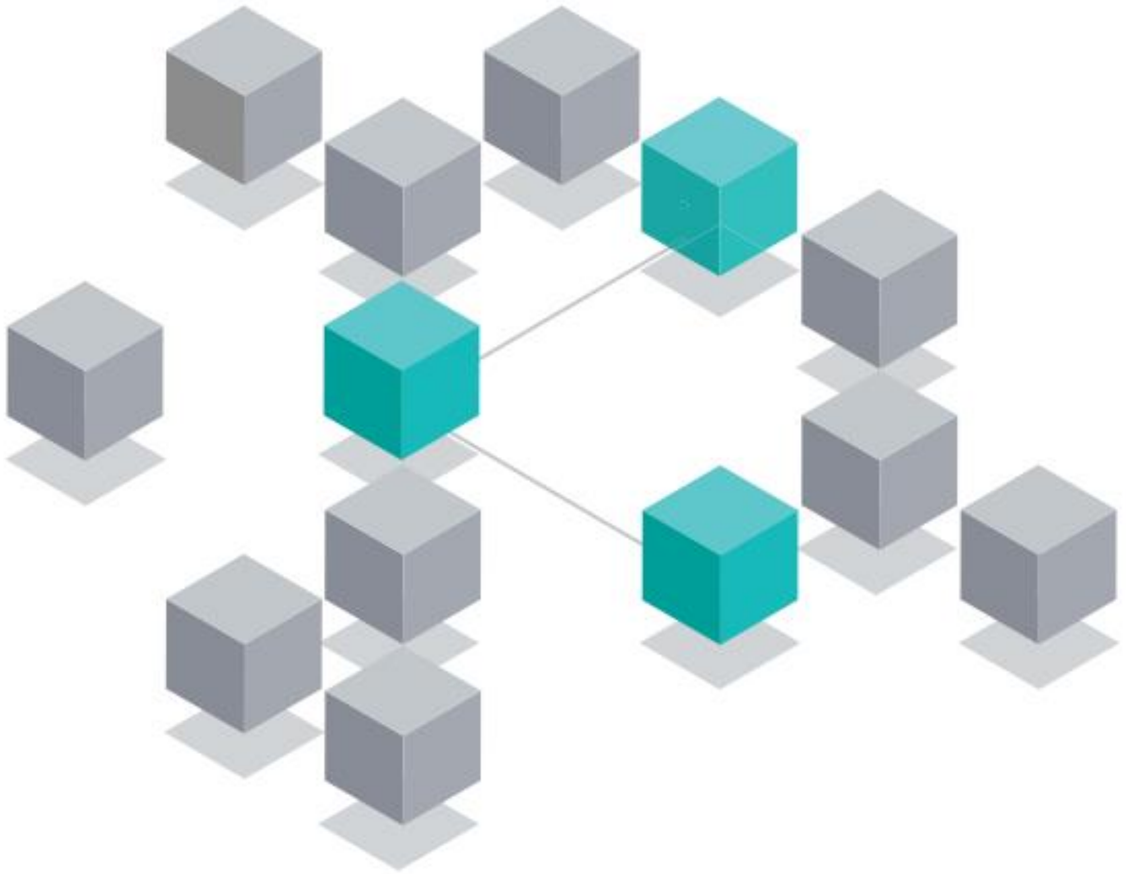


# Živá ukázka



# Proč EDR od FreeDivison?

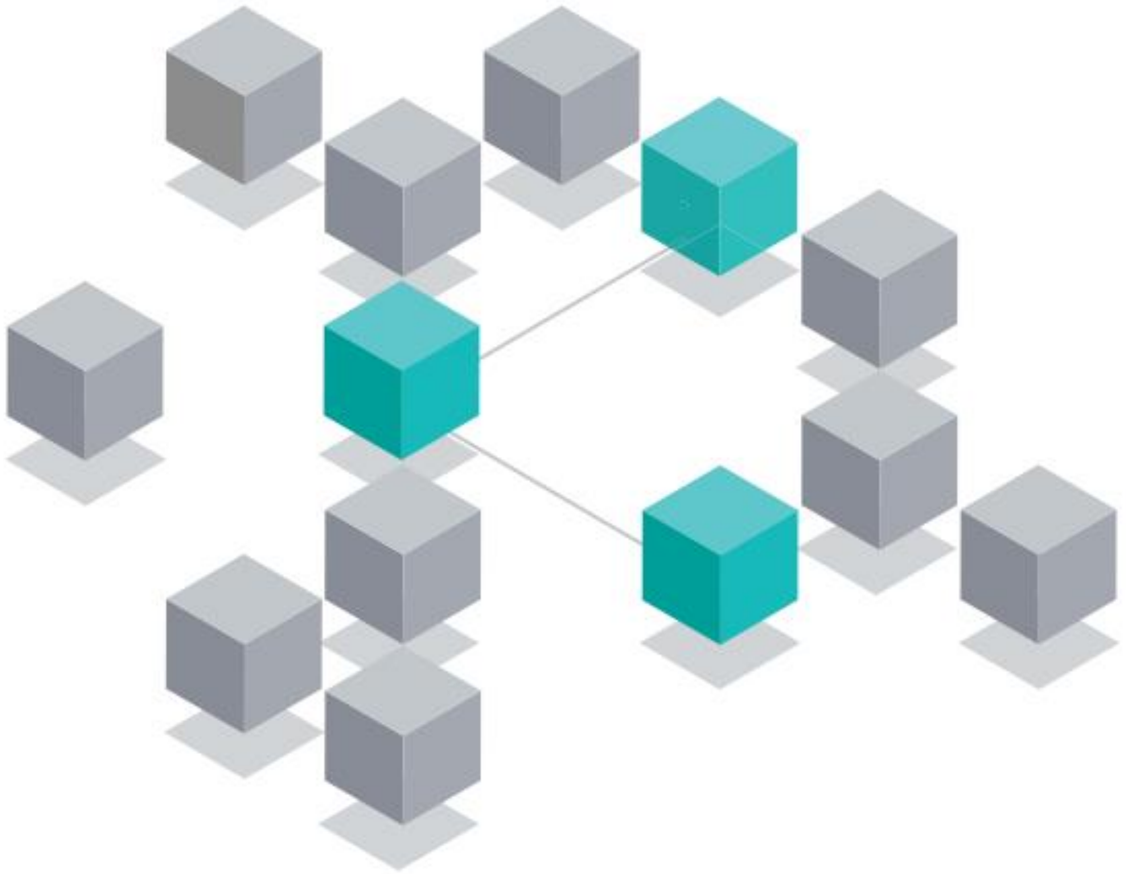
- Cloud FreeDivision
- Možnost služby dohledu = MDR
- Bezkonkurenční cena pro ČR
- Profesionální tým podpory
- Multi-tenantní řešení
- Možnost POC zdarma



# Průběh POC

- Do 100 licencí
- Příprava prostředí – do 30 minut
- Kickoff – předání přístupů a instalace
- Workshopy – s technickým týmem
- Délka testování – 21 dní

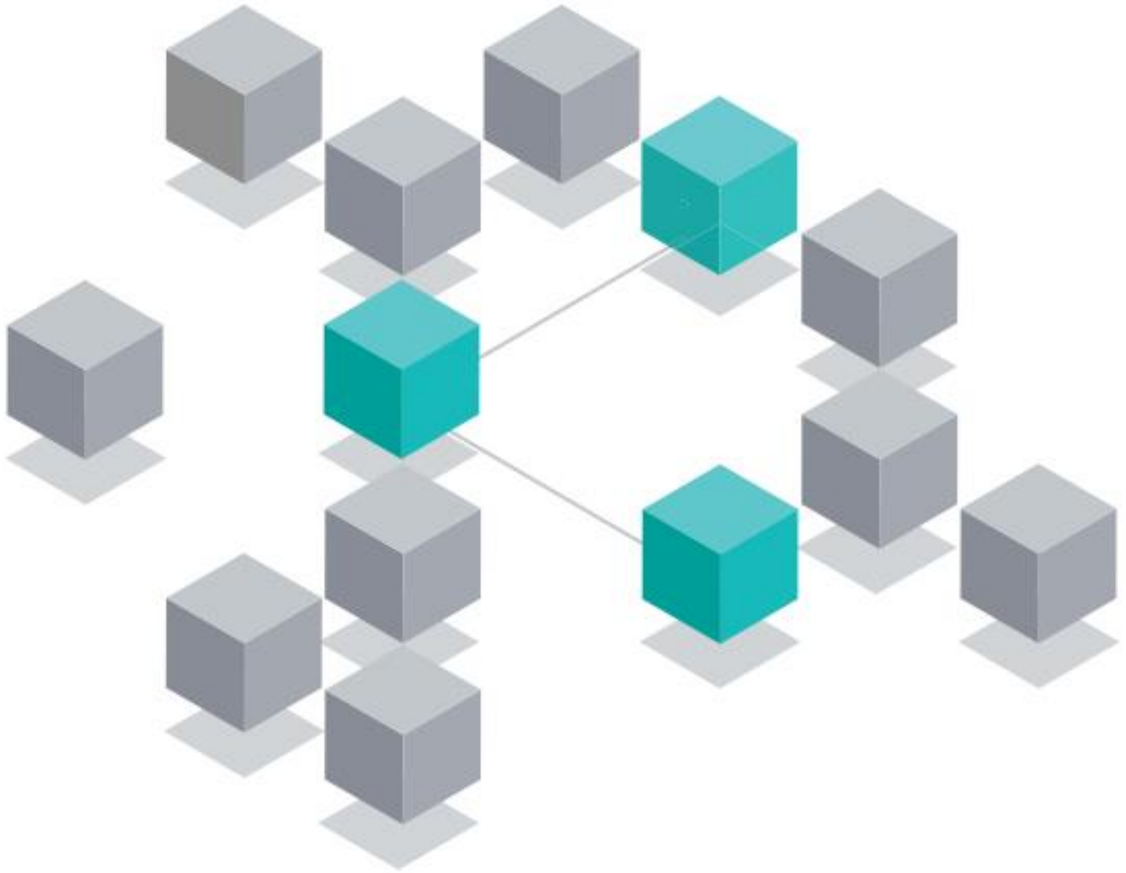
- Možnost zpracování výstupu



# Obchodní model - licencování

- Pouze formou pronájmu
  - 12 nebo 36 měsíců
    - platba po roce
- Licencováno per OS
- Licence za admin přístup do konzole
- Možnost dokoupení MDR

- FD Cloud vs On-Prem – 35 % rozdíl
  - Funkcionalita Cloud x On-prem 1:1



# IBM Security QRadar EDR

Zabezpečení kontinuity provozu

Miroslav Mašek
CyberSecurity Consultant
FreeDivision