

Bitdefender®

e-government
20:10 aneb žijem si jak na zámku,
ať to trvá věčně

Bitdefender GravityZone XDR/EPP

KOLIK LIDÍ POTŘEBUJETE ABYSTE SPLNILI NIS2,
ZoKB A JAK VÁM MŮŽEME POMOCI ?

René Pospíšil – Country Manager CZ/SK

IS4 security
↳ Feel Real Trust

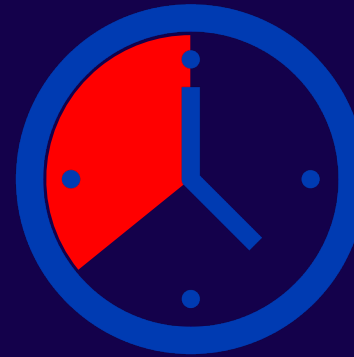
S jakými výzvami se dnes setkáváme?



Je čím dál tím těžší najít, a udržet bezpečnostní specialisty



Mnoho firem a institucí bylo prolomeno nebo se museli potýkat s APT útoky.



Není dostatek času investigovat všechny incidenty a prioritně se soustředit na ty podstatné výstrahy



Nepřehledné množství konzolí a nástrojů napříč různými technologiemi

Více informací o připravované směrnici NIS2:

Připravte se, NIS2 se blíží!



Co je NIS2?

Směrnice NIS2 (Network Information and Security Directive) je rozšířenou verzí původní směrnice NIS.

Jedná se o celoevropský právní předpis o kybernetické bezpečnosti a požadavcích na řízení rizik.

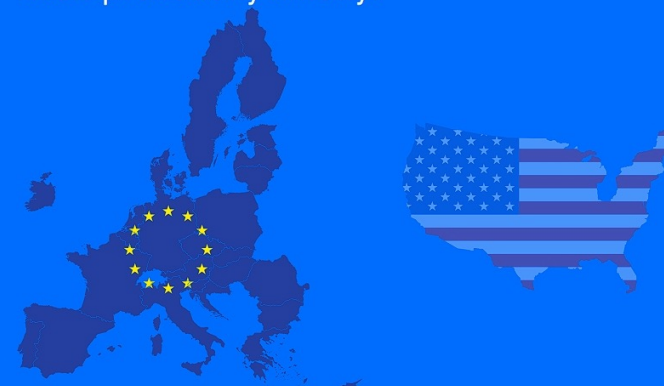
NIS2, která by měla vstoupit v platnost v září 2024, s sebou nese také vyšší finanční zátěž a pokuty pro organizace, které ji nebudou dodržovat.



EU, USA a ostatní státy

Měli bychom se zajímat o NIS2, i když nejsme součástí EU? NIS2 se vztahuje na všechny společnosti, které podnikají v EU*.

*Stále se očekává, že budou ve směrnici NIS2 provedeny změny.





Na koho se NIS2 vztahuje?

"Základní subjekty": společnosti s 250 a více zaměstnanci, a obratem 50 milionů EUR nebo rozvahou 43 milionů EUR.

"Důležité subjekty": společnosti s více než 50 zaměstnanci a ročním obratem nebo bilanční sumou 10 milionů EUR.

NIS1	NIS2
 Zdravotní péče	 Potraviny
 Bankovníctví	 Pošta a kurýrní služby
 Zásobování vodou	 Vesmír
 Poskytovatelé digitálních služeb	 Digitální služby
 Doprava	 Výroba
 Digitální infrastruktura	 Poskytovatelé veřejných sítí nebo služeb elektronických komunikací
 Energetika	 Veřejná správa
	 Odpadní vody a nakládání s odpady

NIS2 rozšiřuje okruh společností, na které se vztahuje, na více průmyslových odvětví, a ukládá specifitější a přísnější požadavky na kybernetickou bezpečnost a řízení rizik, a zároveň zvyšuje finanční sankce za jejich nedodržení.



Možné finanční postihy

Základním subjektům hrozí za nedodržování směrnice pokuta až 10 milionů EUR nebo 2 % celosvětového obratu.

Důležitým subjektům hrozí za nedodržování směrnice pokuta až 7 milionů EUR nebo 1,4 % celosvětového obratu.

U všech subjektů bude vybráno vyšší číslo z obou finančních částek. Organizacím, které nedodržují předpisy, mohou být uloženy další nepeněžní sankce.

To se týká i příkazů k dodržování závazných pokynů, požadavky na oznamování a podávání zpráv dotčeným osobám, a implementace, které z toho mohou vyplývat.



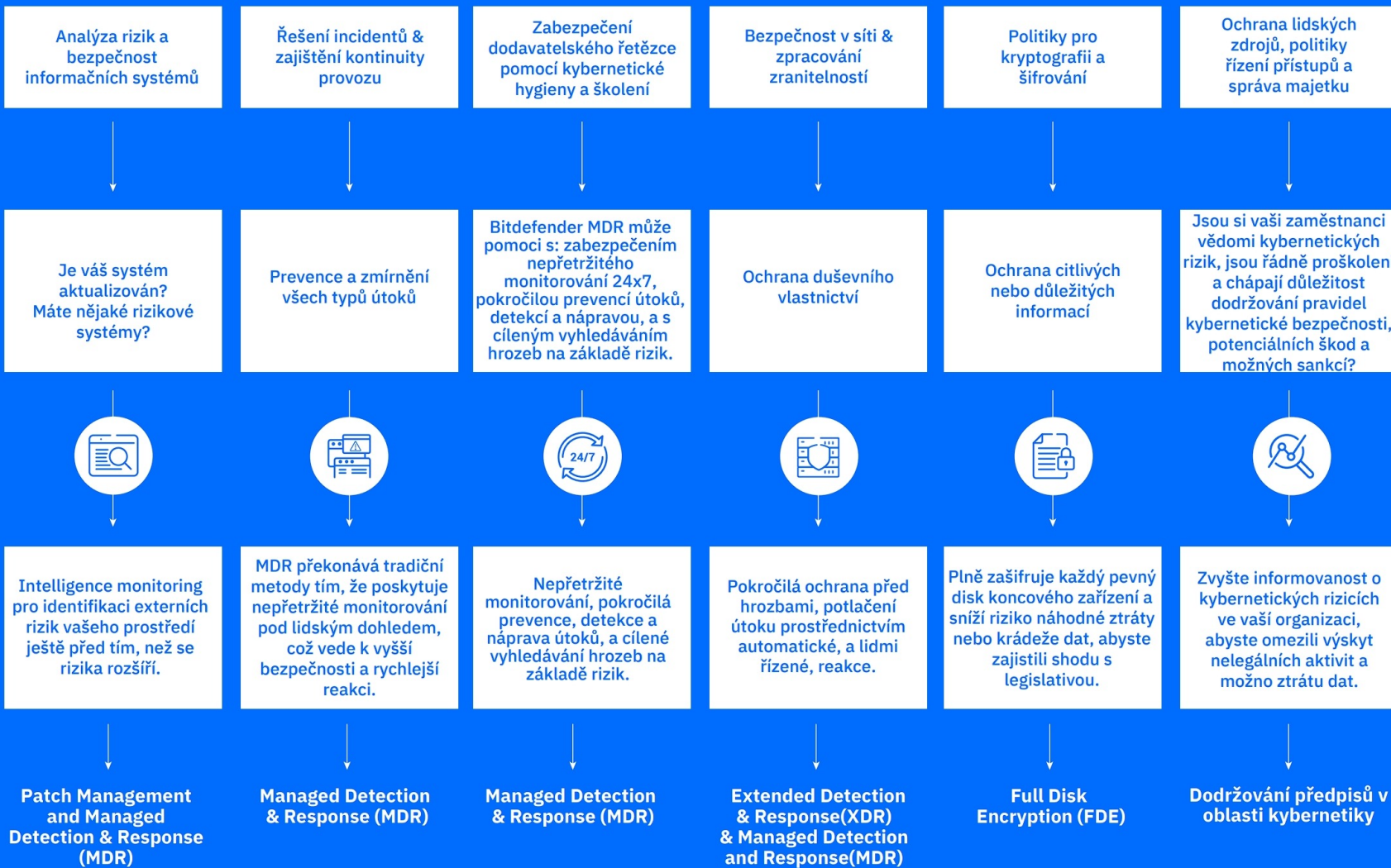


Bud'te připraveni

10 věcí, které by organizace měly posoudit pro zajištění souladu se směrnicí NIS2:

1. Zjistěte, zda se NIS2 vztahuje na vaši organizaci.
2. Identifikujte svá klíčová aktiva.
3. Vypracujte strategii řízení rizik.
4. Zavedte odpovídající bezpečnostní opatření.
5. Implementujte postupy pro odpovídající reakce na incidenty.
6. Provádějte pravidelné testování bezpečnostních systémů.
7. Proveďte školení zaměstnanců.
8. Vezměte v úvahu rizika způsobená externími dodavateli.
9. Uchovávejte si dokumentaci.
10. Dodržujte požadavky v souvislosti s oznamovací povinností.

NIS2 požaduje následující OPATŘENÍ V RÁMCI PŘÍSTUPU KE "VŠEM RIZIKŮM":



Layered security for complete business protection

Modern businesses are more exposed than ever to cyber attacks. Nearly every technology is a potential doorway for cyber-criminals to infiltrate your business. Bitdefender GravityZone provides complete security that monitors and protects the technologies your adversaries are targeting with our patented layered security solution, all fueled by Bitdefender's threat intelligence and research teams.



Visit bitdefender.com to learn more

Principy když stavíte bezpečnost

- Je potřeba stavět na pevných základech
- Otázky které si musíme položit:
- Je stávající platforma, kterou užíváte připravena na dnešní a budoucí hrozby ?
- Jakým vývojem prošla v poslední době ?
- Jak vychází v testech ? Jak dlouho ?
- Pokrývá nové směry ochrany ?
- Obsahuje Analýzu Rizik ?
- Obsahuje File Integrity Monitoring ?
- Obsahuje Patch Management provázaný s Analýzou Rizik ?
- Chrání efektivně Virtualizaci a Cloud i proti bezsouborovým útokům?
- Kolik agentů a kolik konzolí na správu potřebuje ?
- Víte kolik Vás bude stát provoz TCO ?
- Znáte nároky na lidské zdroje ?
- Má lokalizované rozhraní ?
- Má lokální podporu v ČR a SK?



Bitdefender
Založen roku **2001**

1800+ zaměstnanců ...
>60% Vývoj a Výzkum/
engineering

Enterprise HQ v Silicon
Valley (Santa Clara,
California). Vývoj hlavně
v Rumunsku

Enterprise business
roste **+90%** rok od roku

Provozujeme celosvětově
největší bezpečnostní
infrastrukturu chránící
>600 000 000 strojů ve
150 zemích

500 +
MILLION USERS

The image features the text '500 + MILLION USERS' in a bold, sans-serif font. The numbers '500' are significantly larger than the plus sign and the words 'MILLION USERS'. The digits '5', '0', and '0' are filled with a composite image of Earth, showing the blue oceans, green and brown landmasses, and a dark space background with city lights at night. The plus sign is a simple black symbol. The words 'MILLION USERS' are positioned directly below the '500'.

Bitdefender

UZNÁVANÝ INOVATIVNÍ LÍDR

PATENTOVÉ PORTFOLIO: 440+ SCHVÁLENÝCH A DALŠÍ PŘED SCHVÁLENÍM
PRŮKOPNÍK V OBLASTI NASAZENÍ STROJOVÉHO UČENÍ JIŽ OD 2008.

První detekce pomocí strojového učení

2008

První automatizovaná detekce datových toků postavená na strojovém učení

2013

První algoritmus se snížením šumu vytvořený za účelem rozpoznání špatně klasifikovaných vzorců

2011

První použití hloubkového učení za účelem zvýšení účinnosti detekce

2014

První řešení IoT bezpečnosti (Bitdefender Box)

2015

Hypervisor-based memory introspection (HVI)

2016

Nastavitelné strojové učení proti cíleným útokům (HyperDetect)

2017

První výrobce který vytvořil nastavitelné strojové učení bezagentově

2018

První prointegrované řešení EPP s EDR, obsahující Prevenci, Detekci, Odezvu a Bezpečnostní analýzu

2019

Vydání plnohodnotného XDR řešení (stále prointegrovaného s EPP)

2022

BITDEFENDER ŘEŠENÍ LOKALIZOVÁNY DO ČESKÉHO JAZYKA 7. ROKEM



B2C

Produkty určené pro domácnosti a malé firmy



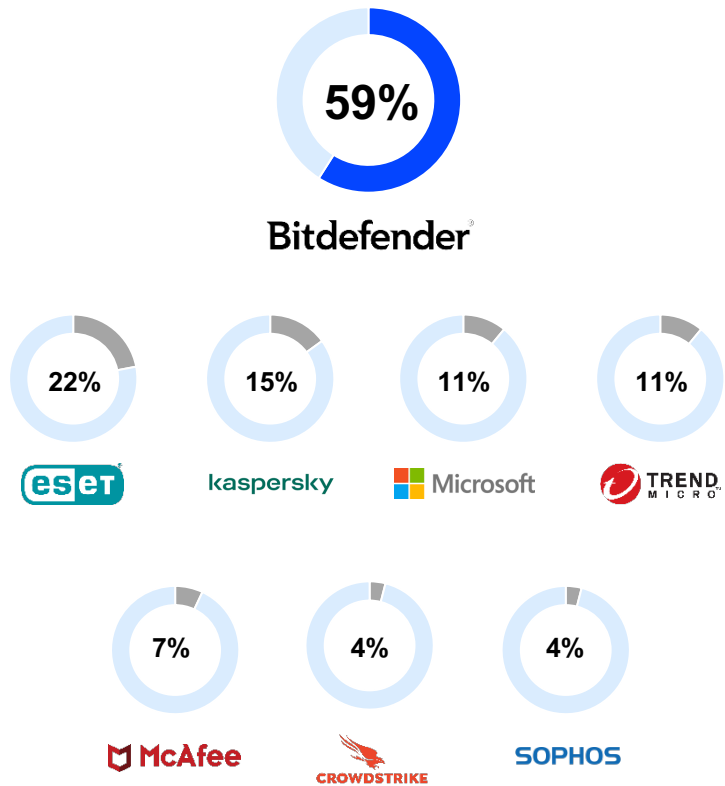
B2B

Produkty pro firemní použití

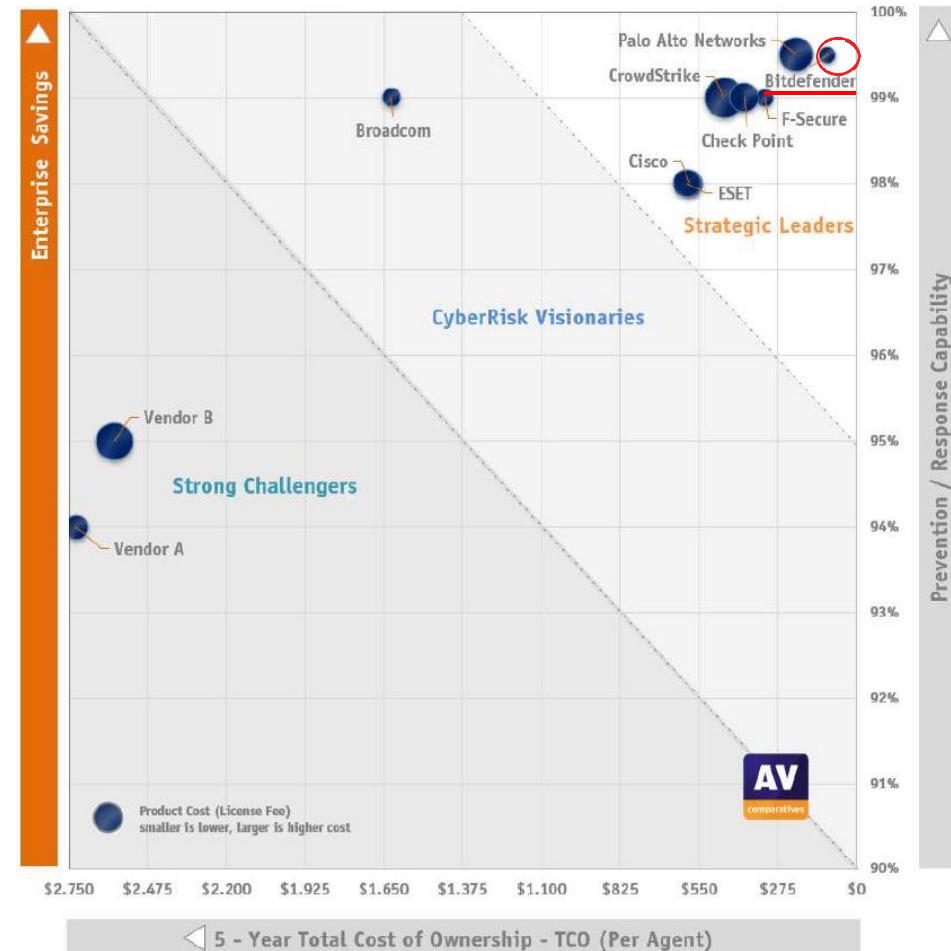


Trvale vysoká efektivita ochrany

#1 Attack prevention rankings from 2018–2021
% (Indexed to 100)¹



Highest Prevention and Response Capability with Lowest 5 Year TCO²

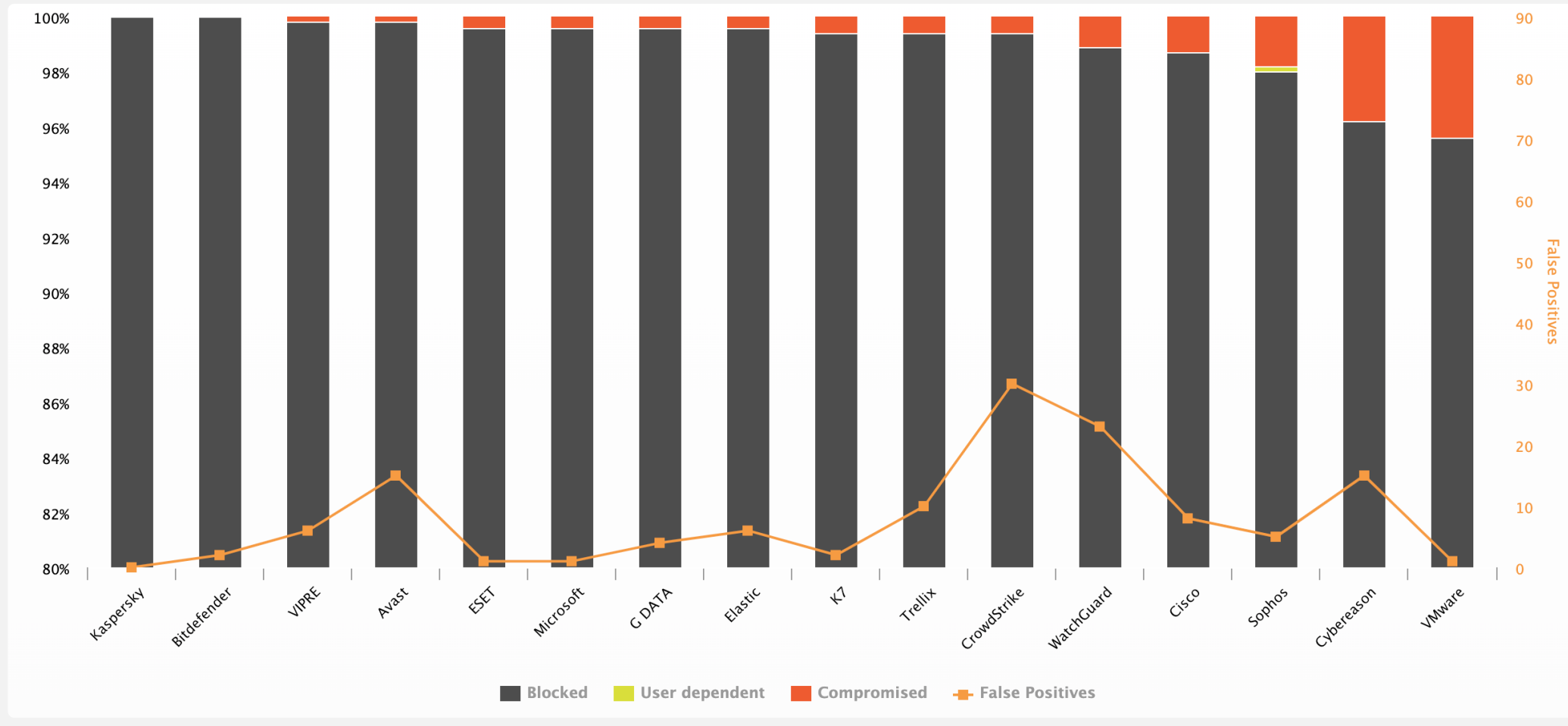


Notes:
1. Represents number of times a given test participant took 1st place in any of the malware detection, **real world & protection** categories tests performed by AV Comparatives
2. **Endpoint Prevention & Response Test 2021, AV Comparatives**

Enterprise Test Charts



Enterprise | Real-World Protection Test | 2023 | Mar-Jun | by protection value | 80 - 100%



Znáte vaše (TCO) provozní náklady EDR+EPP řešení ?

EPR Comparative Report 2021

www.av-comparatives.org

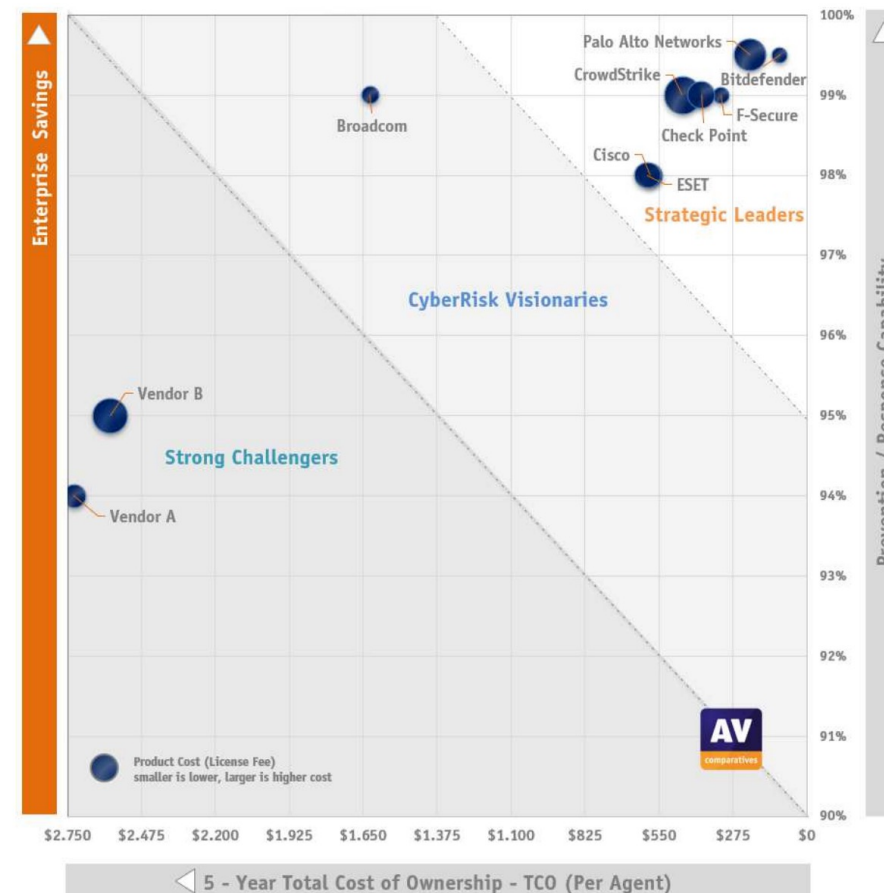
Product	5-Year Product Cost (Per Agent)	Active Response	Passive Response	Combined Prevention/Response Capabilities Y-Axis	5-Year TCO (Per Agent) X-Axis
Bitdefender	\$100	99.0%	100%	99.5%	\$100
Broadcom	\$113	98.0%	100%	99.0%	\$1,734
Check Point	\$180	98.0%	100%	99.0%	\$392
Cisco	\$158	96.0%	100%	98.0%	\$582
CrowdStrike	\$249	98.0%	100%	99.0%	\$461
ESET	\$170	96.0%	100%	98.0%	\$594
F-Secure	\$106	98.0%	100%	99.0%	\$318
Palo Alto Networks	\$210	99.0%	100%	99.5%	\$210
Vendor A	\$153	88.0%	100%	94.0%	\$2,725
Vendor B	\$231	90.0%	100%	95.0%	\$2,591

Figure 2 – CyberRisk Quadrant Key Metrics- based on 5000 agents/clients

5



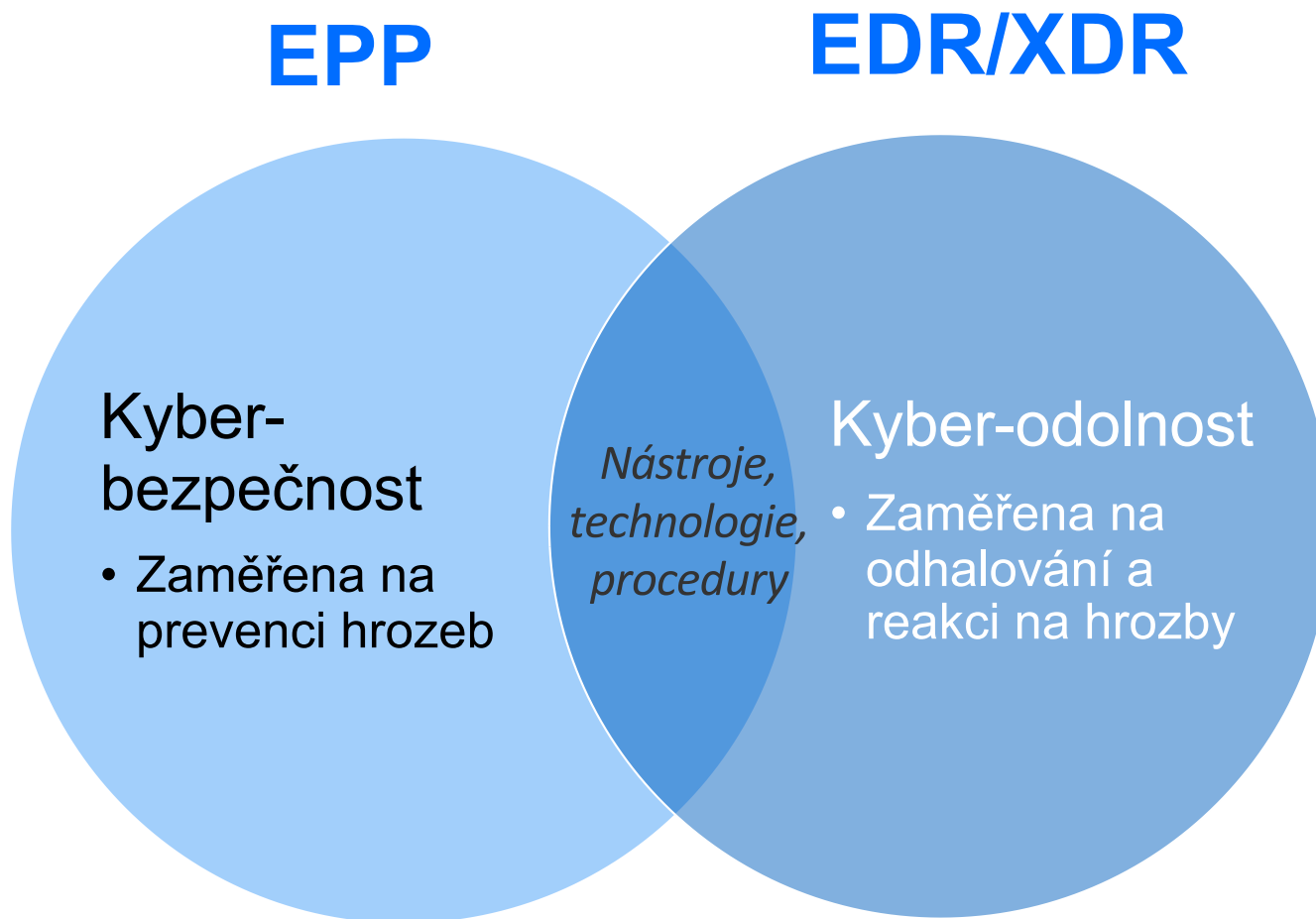
EPR CyberRisk Quadrant™



Reflekující nejen úroveň ochrany ale reálné provozní náklady.
(Kalkulováno pro velikost organizace o 5k zařízeních a 5 let TCO)

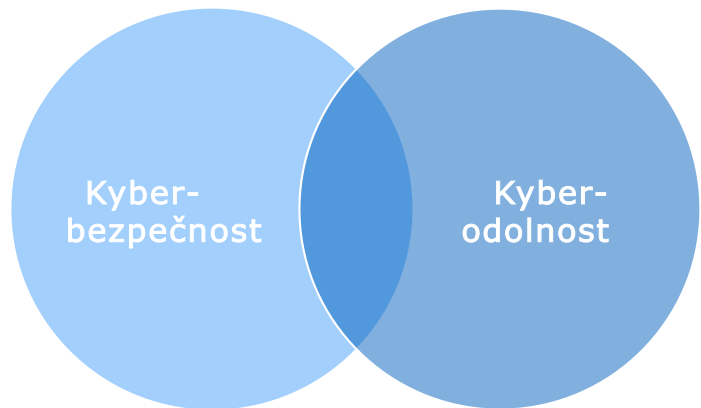
[Stáhnout kompletní zprávu AV-Comparatives](#)

ROLE EPP vs EDR/XDR



EPP

EDR/XDR

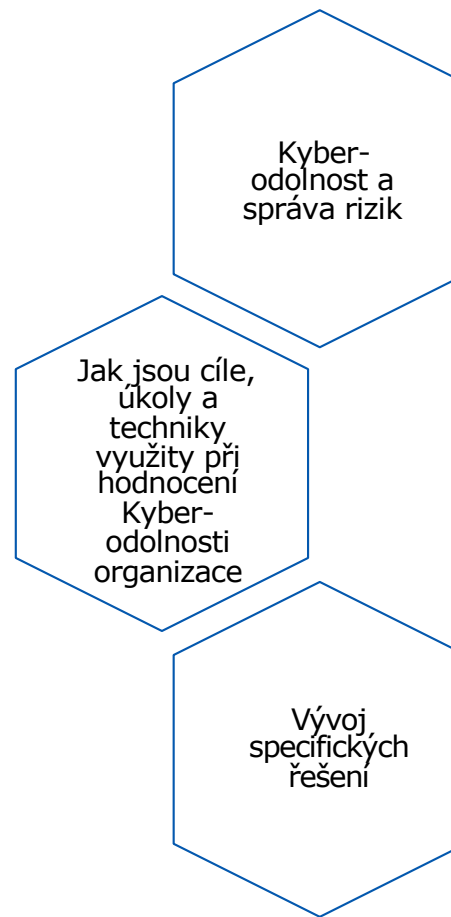


Důležitost kyberodolnosti v roce 2023

SCRAM



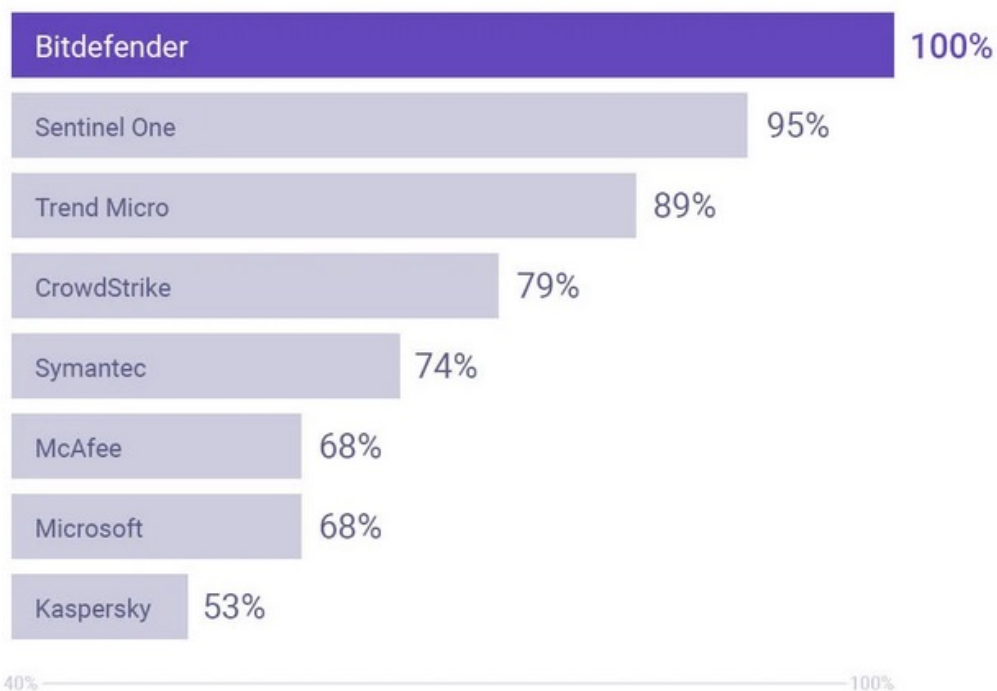
MITRE



EDR, XDR, MDR

Complete MITRE ATT&CK Coverage

for mid-sized organisations & MSPs



Získejte co nejúplnější a nejsmysluplnější pokrytí útočného řetězce

Při hodnocení výsledků ATT&CK je nejlepší začít tím, jak dobře dodavatel pokryl 19-stupňový řetězec útoku, od počátečního napadení až po konečné zvýšení oprávnění.

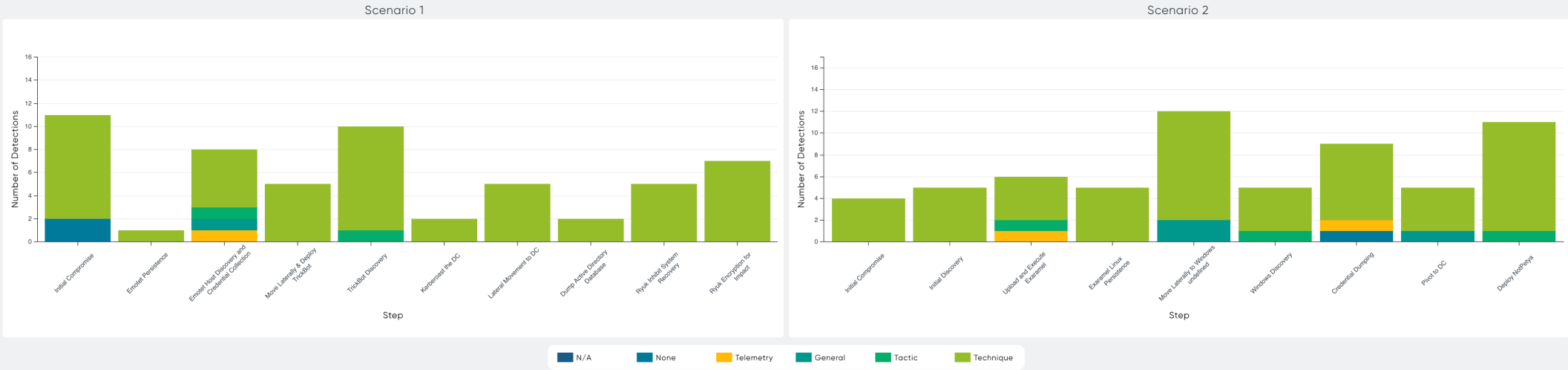
Výsledky ATT&CK jednoznačně ukazují, jak společnost Bitdefender dosáhla maximálního pokrytí celého řetězce útoku, když nevynechala ani jeden krok. Kromě širšího pokrytí Bitdefender také v každém kroku objevuje více detekcí technik, taktik a obecných informací (což jsou nejdůležitější kategorie pro středně velké organizace a MSP, které jsou často omezeny zdroji, dovednostmi a časem) a hledají co nejpřesnější zpracovaná data EDR, nikoli pouze telemetrii.

Uvedený graf zobrazuje zúžený pohled na naši hlavní konkurenci na těchto trzích. [Zde](#) si také můžete prohlédnout úplný graf všech zúčastněných dodavatelů.

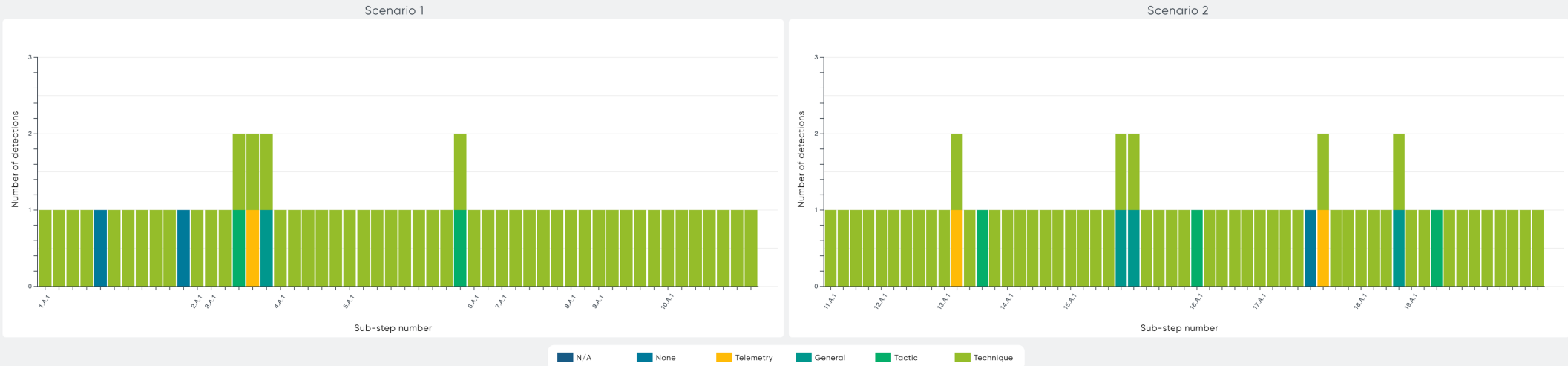
Detailní Výsledky Mitre ATT&CK Evaluations

Results Graphs

Detections Type Distribution By Step



Detections Type Distribution by Sub-step



Obrovská záplava dat je **zdrcující**

Potřeba pro větší a širší náhled do systémů vede organizace k **nákupu mnoho různých nástrojů ochrany**



Identity - IAM



Email Security



Endpoint - EPP/EDR

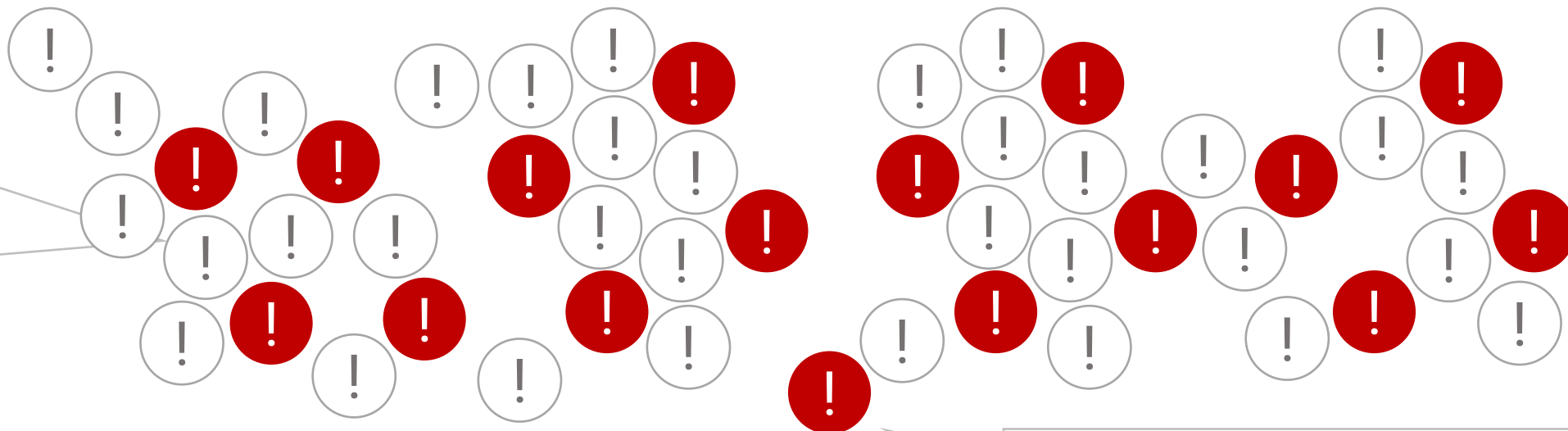


Cloud Security



Network - NDR

Ale **obrovský nárůst logů a analytických dat** z mnoha **neprovázaných zdrojů** je **kontraproduktivní** a vede k ztátě přehledu a obfuskaci opravdových hrozeb

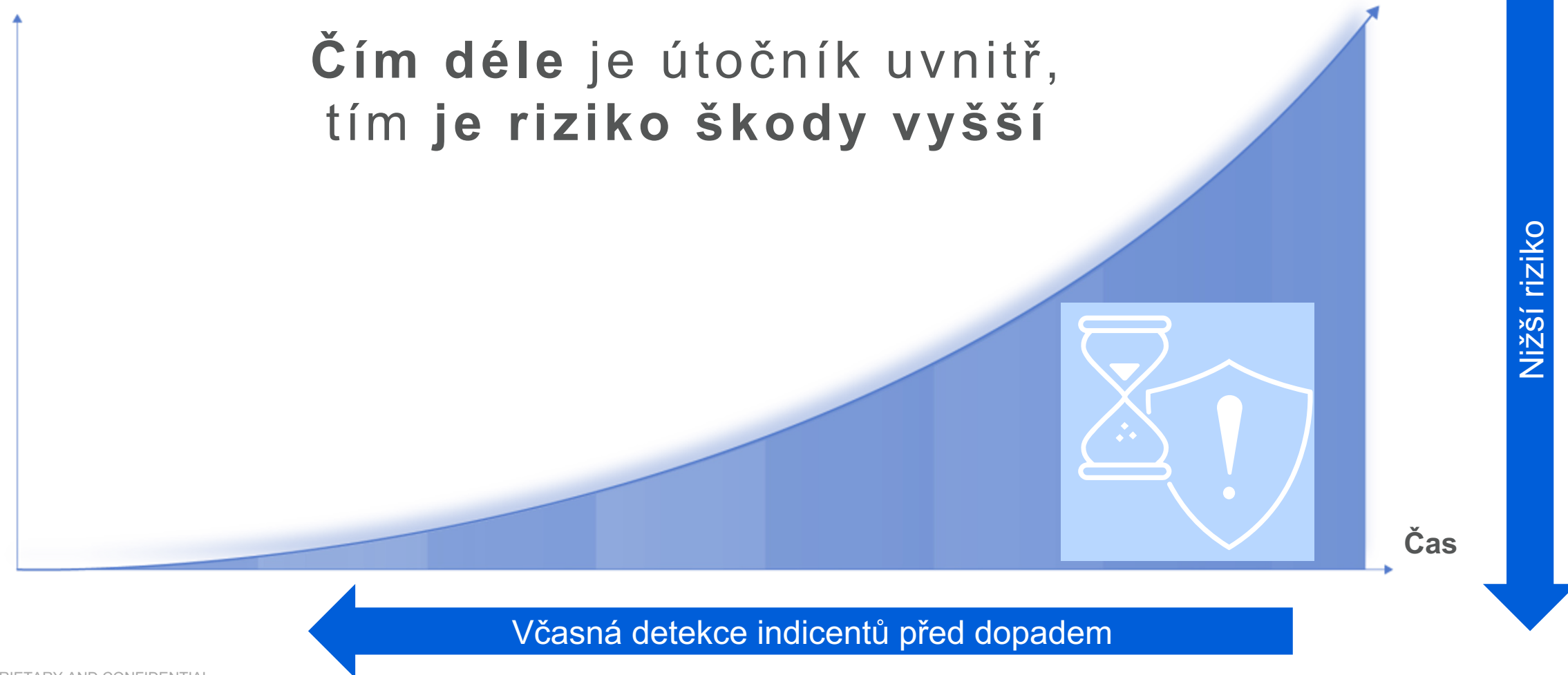


Manuální korelace a analýza těchto dat **brání včasnému odhalení útoků a hrozeb**, a vede k tomu, že **je velmi těžké zabránit průlomům**

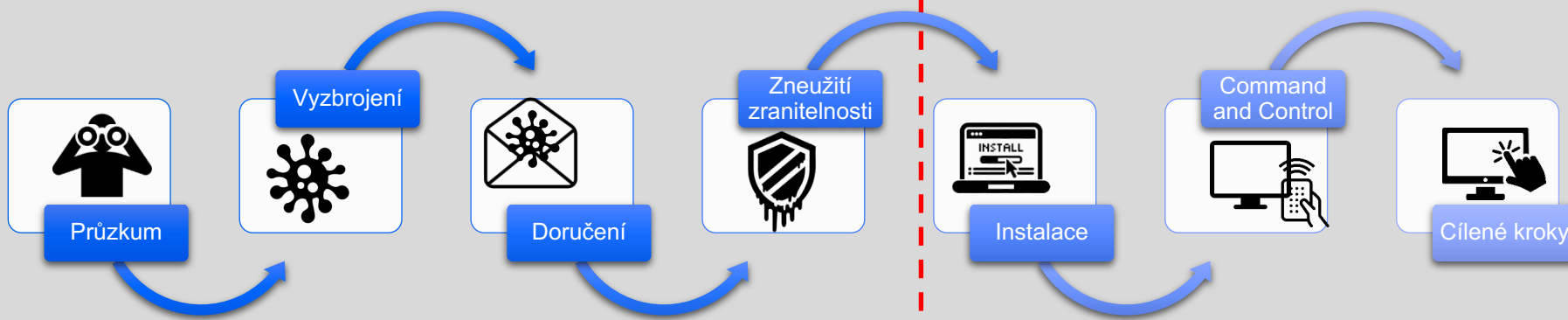
Použitím XDR snížíte čas pro odhalení vyřešení

Riziko

Čím déle je útočník uvnitř,
tím je riziko škody vyšší



ENDPOINT DETECTION & RESPONSE



EPP: PREVENTENCE

EDR: DETECTION & RESPONSE

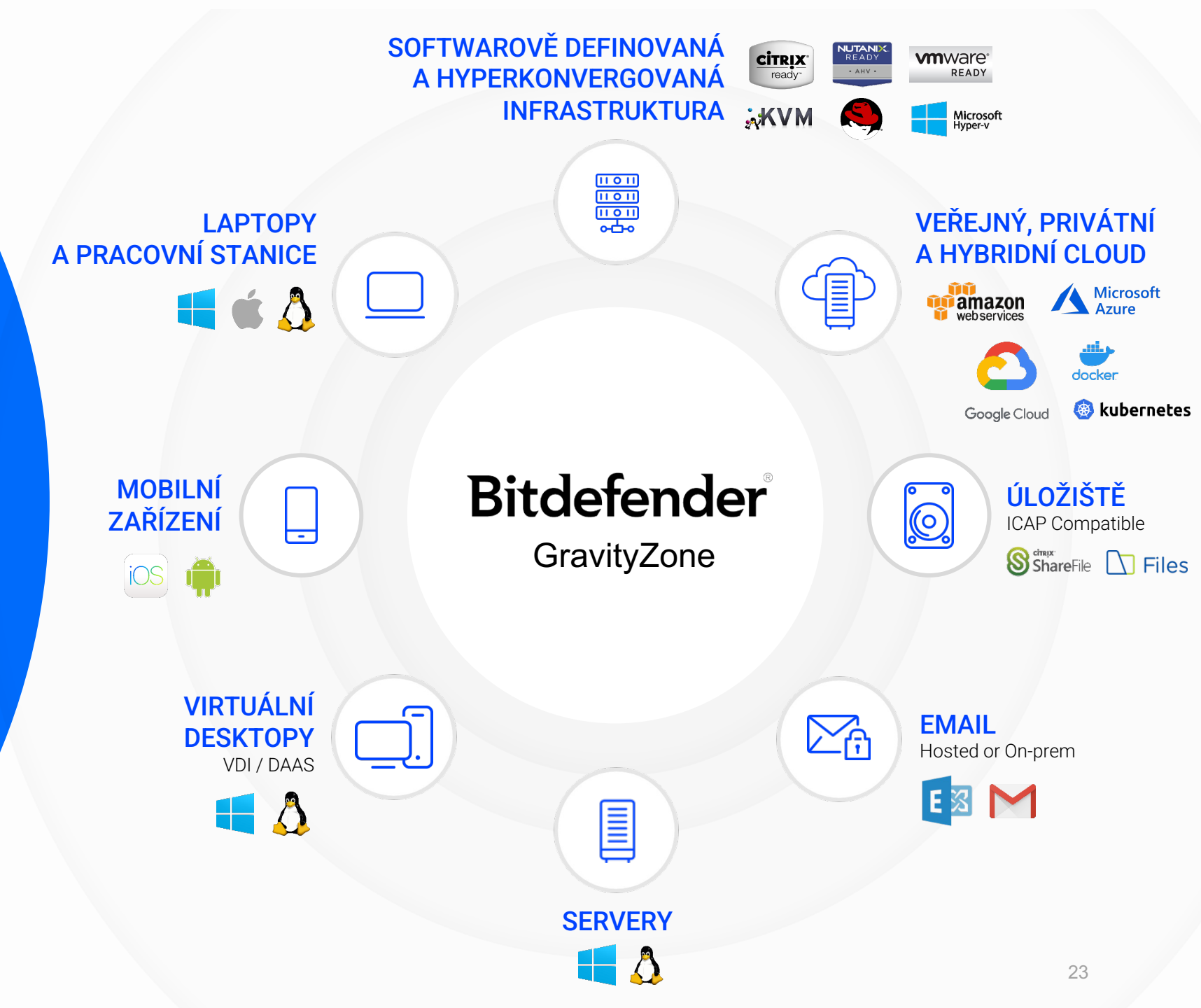


- Incident
- Určení priority
- Zamezení šíření
- Remediacce
- Hlášení

Bitdefender GravityZone

PLATFORMA PODNIKOVÉHO ZABEZPEČENÍ PRO NEJLEPŠÍ PREVENCI NARUŠENÍ

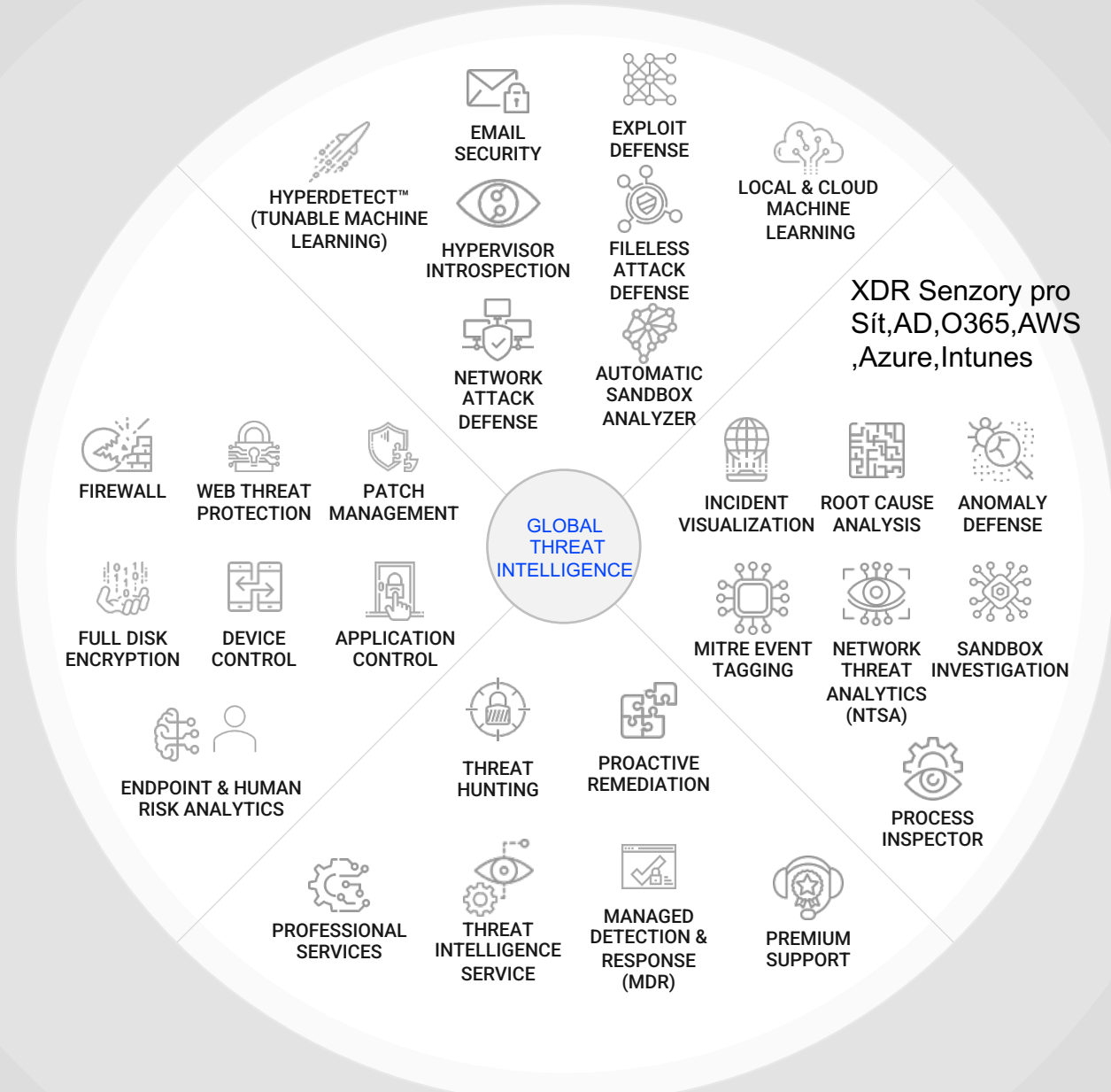
Jednotná prevence, detekce, reakce a zabezpečení napříč koncovými body, sítí a cloudem



35 vrstev ochrany

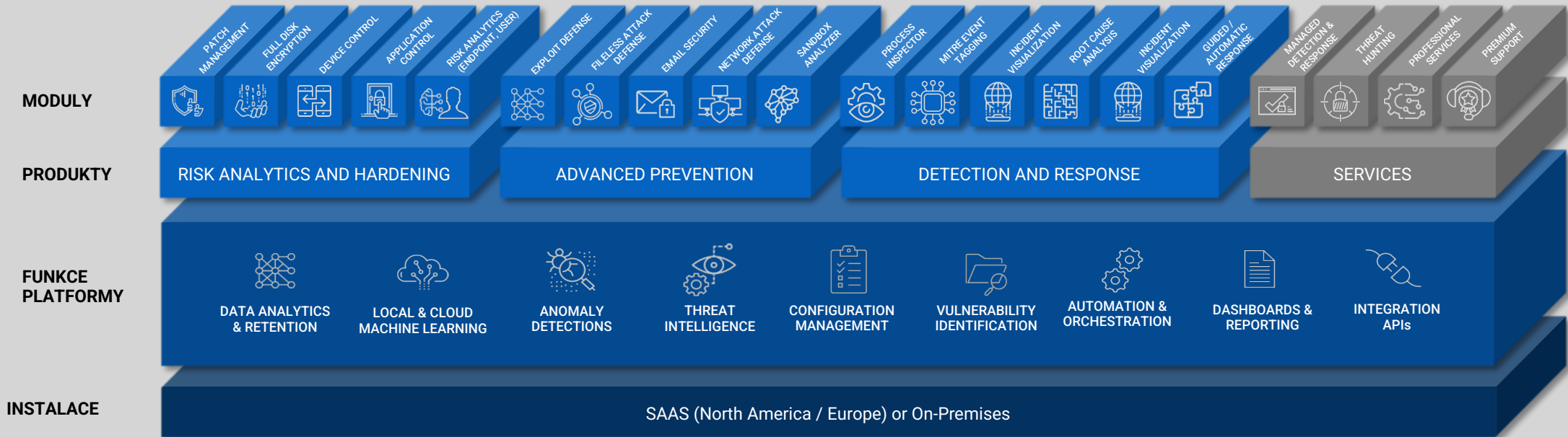
TECHNOLOGIE & SLUŽBY

ANALÝZA RIZIK & VYTVRZOVÁNÍ



SLUŽBY

Bitdefender GravityZone



Endpoints

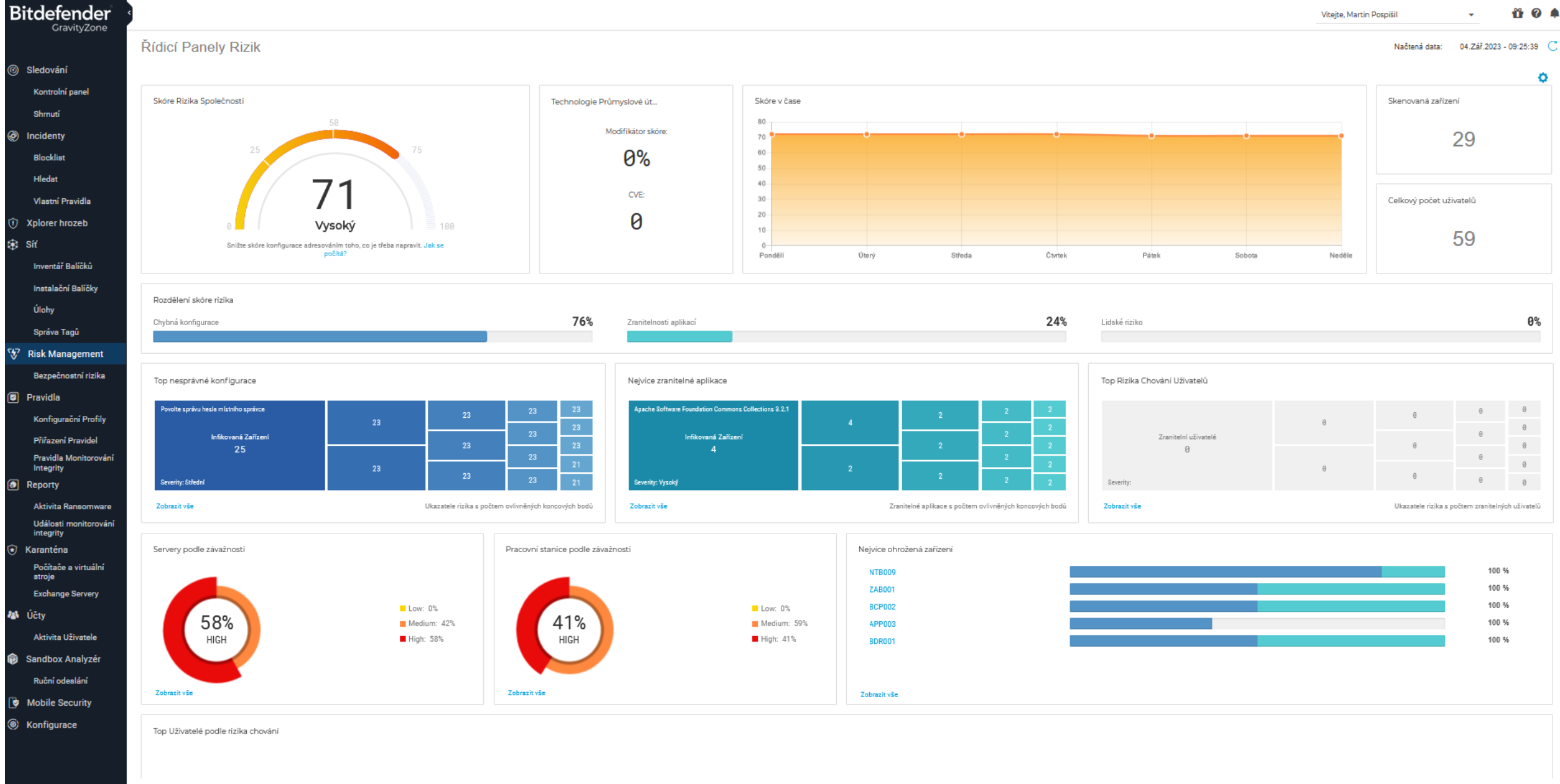


Cloud Workloads



Connected Devices

Řídicí panel - Analýza rizik a analýza chování uživatelů



Hlavní výhody GravityZone Risk Managementu

- **Úplný přehled o zabezpečení rizik** -skenování rizik spojených s chybnou konfigurací operačního systému, zranitelností aplikací a chováním uživatelů, které mohou ohrozit chod organizace.
- **Komplexní dashboard** - umožňuje bezpečnostním týmům rychle identifikovat a kontrolovat rizikové uživatele a zařízení, a odstraňuje tak problémy a zmatky spojené se správou bezpečnostních rizik.
- **Plánovaná skenování rizik** - umožňuje bezpečnostním týmům udržovat si přehled vznikajících bezpečnostních rizicích. Jakmile se objeví nová bezpečnostní rizika, bezpečnostní týmy o nich budou mít přehled a budou je moci rychle odstranit.
- **Oprava bezpečnostních rizik přímo z konzoly GravityZone** - mnoho chybných konfigurací operačního systému lze snadno opravit přímo z dashboardu pro správu rizik. Po přidání doplňku GravityZone Patch Management mohou bezpečnostní týmy jediným kliknutím záplatovat zranitelné aplikace ve všech dotčených systémech.
- Díky kontrole systémů, z hlediska několika indikátorů rizik, může **GravityZone Risk Management** pomoci identifikovat a zmírnit potenciálně slabá místa zabezpečení, způsobená **chybnou konfigurací operačního systému, zranitelnými aplikacemi a chováním uživatelů.**
- **Prověřování rizik lze spouštět** jednotlivě na libovolném systému z konzoly GravityZone, nebo **pravidelně prostřednictvím pravidel nakonfigurovaných v politice.**
- Po dokončení skenování rizik se stanoví celkové skóre rizik na základě identifikovaných kritérií a vybraného modifikátoru zdraví pro dané odvětví.
- **Bezpečnostní týmy mohou rychle identifikovat systémy a uživatele, kteří jsou nejvíce ohroženi.**

GravityZone Patch Management

automatické instalace podle priorit určených na základě automatického vyhodnocení analýzy rizik

(jednotná konzole)

Šetří lidské zdroje a provozní náklady



GravityZone Patch Management

Bezpečnostní a jiné než bezpečnostní záplaty.

I když je phishing hlavní příčinou narušení bezpečnosti, stejně důležitá je správa a záplatování interních systémů. Analytická společnost Gartner předpovídá, že "do konce roku 2020 bude 99 % zneužívaných zranitelností i nadále patřit mezi ty, které jsou známé odborníkům na bezpečnost a IT".

Přídavný modul Patch Management, plně integrovaný do platformy GravityZone, umožňuje organizacím udržovat operační systémy a softwarové aplikace aktuální a poskytuje komplexní přehled o stavu záplat v celé instalační základně systému Windows. Modul záplatování poskytuje aktualizace pro celou flotilu pracovních stanic, fyzických serverů nebo virtuálních serverů.

Modul GravityZone Patch Management obsahuje několik funkcí, například skenování záplat na vyžádání / plánované skenování záplat, automatické / ruční záplatování nebo hlášení chybějících záplat.

Podniky, které záplatují své koncové body, posílí svou bezpečnostní pozici a soulad s předpisy a zároveň zvýší provozní efektivitu.

Vlastnosti & výhody

- Aktualizace operačního systému a největší množiny softwarových aplikací
- Automatické a ruční aktualizace
- Podrobné informace o aktualizacích - CVE, ID bulletinu, závažnost záplaty, kategorie záplaty
- Možnost nastavení různých plánů pro bezpečnostní a jiné než bezpečnostní aktualizace
- Rychlé nasazení chybějících aktualizací
- Možnost distribuovat aktualizace ze serveru relay, což snižuje síťový provoz.
- Specifické zprávy o aktualizacích, které pomáhají společně prokázat dodržování předpisů
- Automatické upozornění správce IT na chybějící bezpečnostní/nebezpečnostní aktualizace.

FILE INTEGRITY MONITORING

Základní informace

- Hlavní funkcí modulu je sledování 3 hlavních prvků integrity souborů
 - Confidentiality - důvěrnost
 - Integrity - integrita
 - Availability - dostupnost
- FIM identifikuje například
 - Vytváření souborů
 - Jejich úpravy
 - Přesuny souborů
 - Mazání souborů



**PCI-DSS Payment
Card Industry Data
Security Standard**



**SOX - Sarbanes-
Oxley Act**



HIPAA



ISO 27001



NIST CSF



GDPR

FILE INTEGRITY MONITORING

Bitdefender
GravityZone

- Monitoring
 - Dashboard
 - Executive Summary
- Incidents
 - Blocklist
 - Search
 - Custom Rules
- Threats Xplorer
- Network
 - Patch Inventory
 - Packages
 - Tasks
 - Tags Management
- Risk Management
 - Security Risks
- Policies
 - Configuration Profiles
 - Assignment Rules
 - Integrity Monitoring Rules**
- Reports

Integrity Monitoring Rules

CONFIGURATION <

RULES

- All rules
- Default OS rules
- Default application rules
- Custom rules

RULE SETS (3)

- Win2019
- Win10
- Linux

All rules

ACTIONS ▾

Rule name 🔍 Entity type ▾ Severity ▾ More ▾

<input type="checkbox"/>	Rule name	Description	Entity type	OS	Severity	Rule type
<input type="checkbox"/>	[RHEL-v8] System Configuration Files	Monitors /etc files, archives some contents	Multiple	Linux	● High	Default
<input type="checkbox"/>	[MS-Windows-2008-DM] Files and Directories	-	Multiple	Windows	● High	Default
<input type="checkbox"/>	[MS-Windows-2012-DM] Files and Directories	-	Multiple	Windows	● High	Default
<input type="checkbox"/>	[MS-Windows-2016] Files and Directories	-	Multiple	Windows	● High	Default
<input type="checkbox"/>	[MS-Windows-7] Files and Directories	-	Multiple	Windows	● High	Default
<input type="checkbox"/>	[Oracle-Solaris-v10] System Configuration Files	Monitors /etc files, archives some content	Multiple	Linux	● High	Default
<input type="checkbox"/>	[Oracle-Solaris-v10] Variable System Files	Monitors /var and /tmp directories (permissions only)	Multiple	Linux	● High	Default
<input type="checkbox"/>	[RHEL-v7] System Configuration Files	Monitors /etc files, archives some contents	Multiple	Linux	● High	Default
<input type="checkbox"/>	[SUSE] System Configuration Files	Monitors /etc files, archives some contents	Multiple	Linux	● High	Default
<input type="checkbox"/>	[Amazon Linux v2] System Configuration Files	Monitors /etc files, archives some contents	Multiple	Linux	● High	Default

Hlavní vlastnosti



Nesledujte jen soubory

Sledujte nejen soubory, kontrolujte více entit v systému

- Soubory
- Adresáře
- Klíče a hodnoty v registrech
- Instalované aplikace
- Eskalace uživatelských práv



Řízení rizik a změn

- Identifikujte změny v souborech pro indikaci událostí a incidentů integrity
- Vše v reálném čase
- Řešte schválené a neschválené změny
- Identifikujte významné změny konfigurace ve chvíli, kdy k nim dochází



Efektivita správy

- Automatická doporučení aplikovatelná podle pravidel umožňují reakci na základě událostí
- Redukce vynaloženého času při konfiguraci monitoringu
- Prioritizace upozornění zajistí lepší přehled o důležitých událostech

POKROČLÁ, ÚČINNÁ a PŘESNÁ DETEKCE - Hyperdetect

HyperDetect

This feature is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage. It can be customized to suit your organization's security requirements.

Protection Level

Ochrana proti relevantním hrozbám

Možnost nastavení úrovně agresivity detekce

	<input type="radio"/> Permissive	<input type="radio"/> Normal	<input type="radio"/> Aggressive
<input checked="" type="checkbox"/> Targeted Attack	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> Suspicious files and network traffic	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Exploits	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> Ransomware	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> Grayware	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Actions **Získejte plnou viditelnost a zapněte si automatické akce**

Files: Extend reporting on higher levels

Network traffic: Extend reporting on higher levels

Deny
Disinfect
Delete
Move files to quarantine
Report Only

Chrání proti:

- Ransomware
- Exploitům
- Útokům bez souboru
- Skript. útokům

Dodává plnou vizibilitu ohledně podezřelých aktivit

OBSAHUJE VÍCE JAK 80 000 speciálně vycvičených vzorců chování pro rozpoznání cílených útoků. Nejefektivnější detekce pomocí strojového učení (AI)

Pojistka proti zašifrování Ransomware remediacce

umožňuje automaticky obnovit zašifrovaná data z chráněného oddílu na disku ...

Ochrání tak proti útokům vedeným z nechráněných stanic v síti...

Bitdefender Ransomware Mitigation

Ransomware je již dlouhou dobu lukrativním byznysem, který kyberzločincům vynáší miliardy na zaplacených výkupných. Nyní, když už je ziskovost ransomwaru prokázána, hledají zločinecké organizace nové a nové způsoby, jak na svých investicích ještě více vydělat, což povede k čím dál více sofistikovaným útokům na firmy a organizace.

Jak Bitdefender GravityZone poráží ransomware?

Jako adaptivní vrstvené bezpečnostní řešení poskytuje Bitdefender GravityZone několik funkcí proti ransomwaru, přičemž všechny jeho vrstvy spolupracují při prevenci, detekci a nápravě.

Více blokovacích vrstev	Koncový bod a síť, před provedením a při spuštění, na bázi souborů a bez souborů
Více detekčních vrstev	Kontrola procesů, monitorování registrů, kontrola kódu, hyperdetekce
Více vrstev obnovy	Účinný rollback z místního počítače, vzdáleného systému nebo bezpečnostního incidentu
Adaptivní obranné mechanismy	Pokročilý Anti-Exploit, adaptivní heuristika, konfigurovatelné strojové učení
Technologie pro minimalizaci rizik	Automatické opravování zranitelností, chybné konfigurace systému, chování uživatelů
Zálohy odolné proti neoprávněné manipulaci	Nepoužívá se zranitelná stínová kopie, ransomware nemůže odstranit zálohy.
Vzdálené blokování ransomwaru	Blokuje vzdálené a síťové útoky ransomwaru, a zařazuje IP adresy útočníků na černou listinu.
Čištění v rámci celé organizace	Vzdálené ukončování procesů, snadná globální karanténa a odstraňování souborů

Doporučený nástroj k ověření kvality detekce ochrany proti Ransomware

Dynamická simulace Ransomware útoků

Stáhněte si Ransomware simulator zde

<https://www.knowbe4.com/ransomware-simulator>

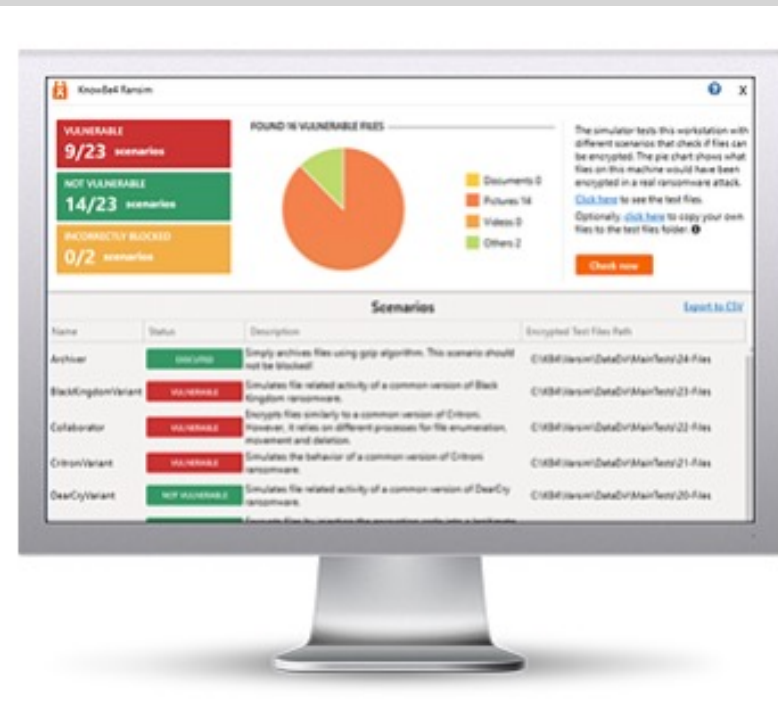
Povolte spuštění samotného nástroje tím že ho dáte do whitelistu (nutné pouze u těch vendorů co se bojí výsledků..)

Poznámka:

- 100% neškodná simulace opravdových ransomware a cryptomining útoků
- Nepoužívá žádné vaše data
- Testuje 23 typů nakažlivých scénářů útoků
- Stačí stáhnout a spustit
- Výsledky získáte do pár minut

PŘIJDTE SI OTESTOVAT NA NAŠEM BITDEFENDER STÁNKU PRVNÍCH 5 získá extra dárek ...

KnowBe4
Human error. Conquered.



Šifrování pevných disků

umožňuje centrální správu šifrování pro Windows (BitLocker) a MacOS (FileVault)

důležité pro notebooky a GDPR ochranu dat ...

Jednoduchá správa a obnova hesel



GravityZone Full Disk Encryption

Původní, osvědčený šifrovací doplněk pro zabezpečení firemních dat.

Data jsou v digitální ekonomice nejdůležitějším aktivem. Ochrana důvěrných dat, splnění požadavků na dodržování předpisů a prevence nákladných úniků dat, jsou klíčovými pilíři strategie ochrany podnikových dat.

GravityZone Full Disk Encryption je řešení, které pomáhá společnostem dodržovat předpisy týkající se dat, a předcházet ztrátě citlivých informací v případě ztráty nebo odcizení zařízení.

GravityZone Full Disk Encryption šifruje bootovací i ne bootovací svazky, na pevných discích, ve stolních počítačích a notebookech, a poskytuje jednoduchou vzdálenou správu šifrovacích klíčů.

Toto řešení poskytuje centralizovanou správu nástrojů BitLocker (v systému Windows), FileVault a nástroje příkazového řádku diskutil (obojí v systému macOS), přičemž využívá výhod nativního šifrování zařízení a zajišťuje optimální kompatibilitu a výkon. Vyměnitelné disky nejsou šifrovány.

Vlastnosti & výhody

- Nativní, osvědčené šifrování, které využívá šifrovací mechanismy poskytované systémy Windows a Mac
- Jedna konzola pro ochranu koncových bodů a správu šifrování
- Specifické zprávy o šifrování, které pomáhají společnostem prokázat shodu s předpisy
- Vynucení ověřování před spuštěním systému

FULL DISK ENCRYPTION

The screenshot shows the Bitdefender GravityZone interface. On the left is a dark sidebar with the Bitdefender GravityZone logo and a navigation menu. The menu items include: Tag Management, Risk Management, Security Risks, Policies (highlighted), Configuration Profiles, Assignment Rules, Integrity Monitoring Rules, Reports, Ransomware Activity, Integrity Monitoring Events, Quarantine, and Computers and VMs. The main content area is divided into two columns. The left column contains a list of modules: General, Antimalware, Sandbox Analyzer, Firewall, Network Protection, Patch Management, Device Control, Integrity Monitoring, Relay, Exchange Protection, and Encryption (highlighted). Below the Encryption module is a sub-menu with 'General'. The right column displays the 'Encryption Management' settings. It features a checked checkbox for 'Encryption Management' and a descriptive paragraph: 'Enable this module to start managing endpoint encryption from Control Center. Disabling it will leave volumes in their current state and will allow users to manage encryption locally.' Below this are two radio button options: 'Decrypt' (unselected) and 'Encrypt' (selected). Under 'Encrypt', there is a checked checkbox for 'If Trusted Platform Module (TPM) is active, do not ask for pre-boot password.' There is also an unchecked checkbox for 'Exclusions' with an information icon. At the bottom, there is a table with two columns: 'Type' and 'Excluded items'. The 'Type' column has a dropdown menu currently showing 'Entity'.

Bitdefender GravityZone

Tag Management

Risk Management

Security Risks

Policies

Configuration Profiles

Assignment Rules

Integrity Monitoring Rules

Reports

Ransomware Activity

Integrity Monitoring Events

Quarantine

Computers and VMs

- General +
- Antimalware +
- Sandbox Analyzer +
- Firewall +
- Network Protection +
- Patch Management
- Device Control +
- Integrity Monitoring +
- Relay +
- Exchange Protection +
- Encryption -**

Encryption Management

Enable this module to start managing endpoint encryption from Control Center. Disabling it will leave volumes in their current state and will allow users to manage encryption locally.

Decrypt
Select this option to decrypt volumes.

Encrypt
Select this option to encrypt volumes. Users will be prompted to enter a password that will be required

If Trusted Platform Module (TPM) is active, do not ask for pre-boot password.

Exclusions ⓘ

Type	Excluded items
<input type="text" value="Entity"/>	Entity

Nová ochrana OS Linux a Kontejnerů

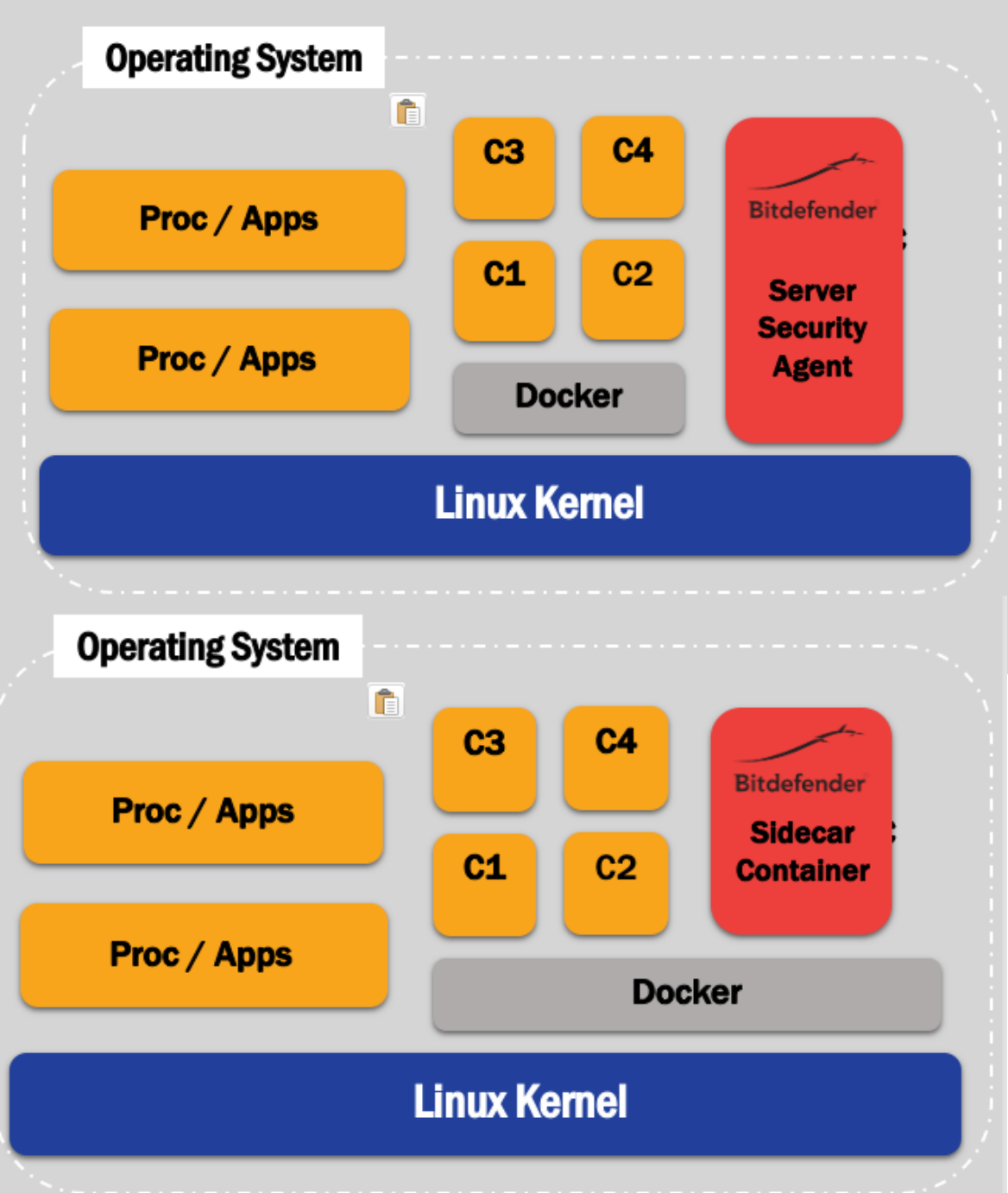
“zbavte se závislosti na jádru”

1. Model nasazení: Guest Agent

- Vhodný pro prostředí s možností přímého přístupu na hosta “direct guest access” (IaaS)
- Běží nezávisle na jádru jako “in-guest agent”
 - Monitoruje běžící kontejnery
 - Monitoruje operační systém hosta
 - Je kompatibilní s “OCI compliant runtimes”

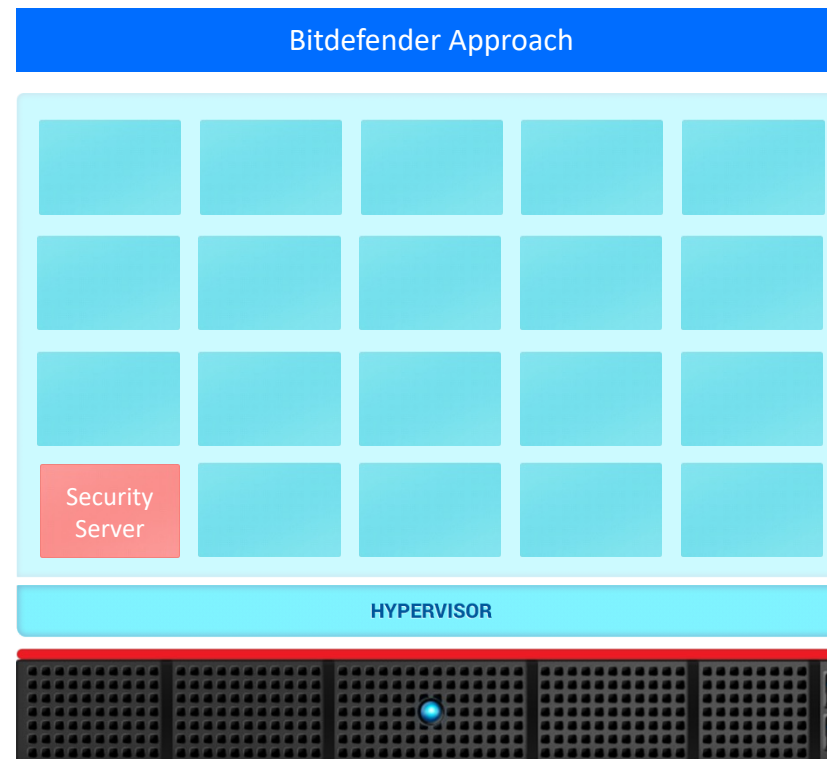
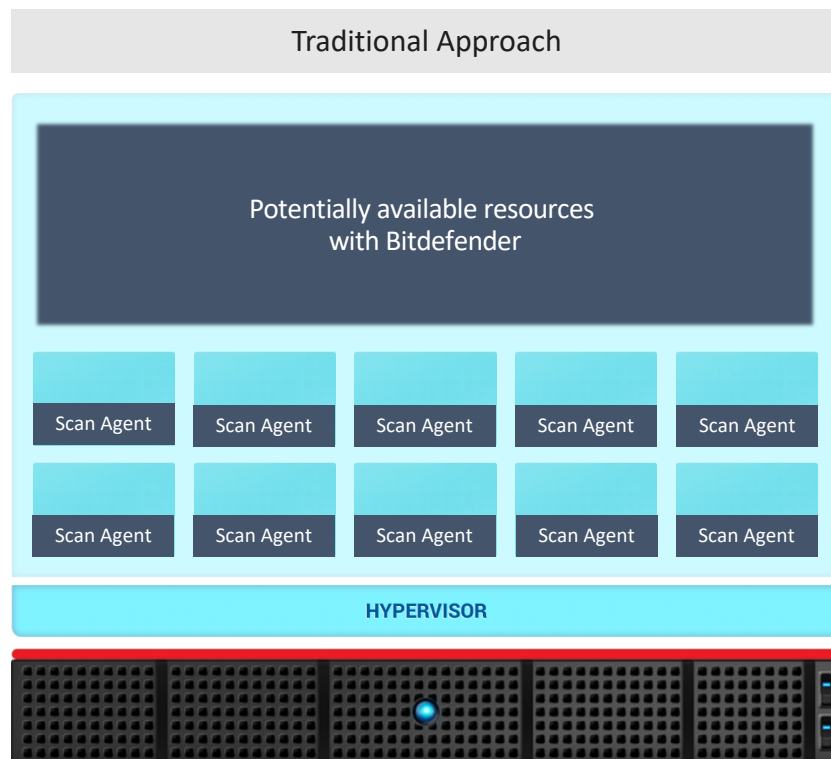
2. Model nasazení: Sidecar Container

- Vhodný pro prostředí která neumožňují přímý přístup na hosta
- Nasazení PaaS
 - Cloud-nativní distros
- Běží jako privilegovaný kontejner
 - Monitoruje sousedící kontejnery
 - Monitoruje guest OS
- Běží na “OCI compliant runtimes”



OCHRANA VIRTUALIZACE

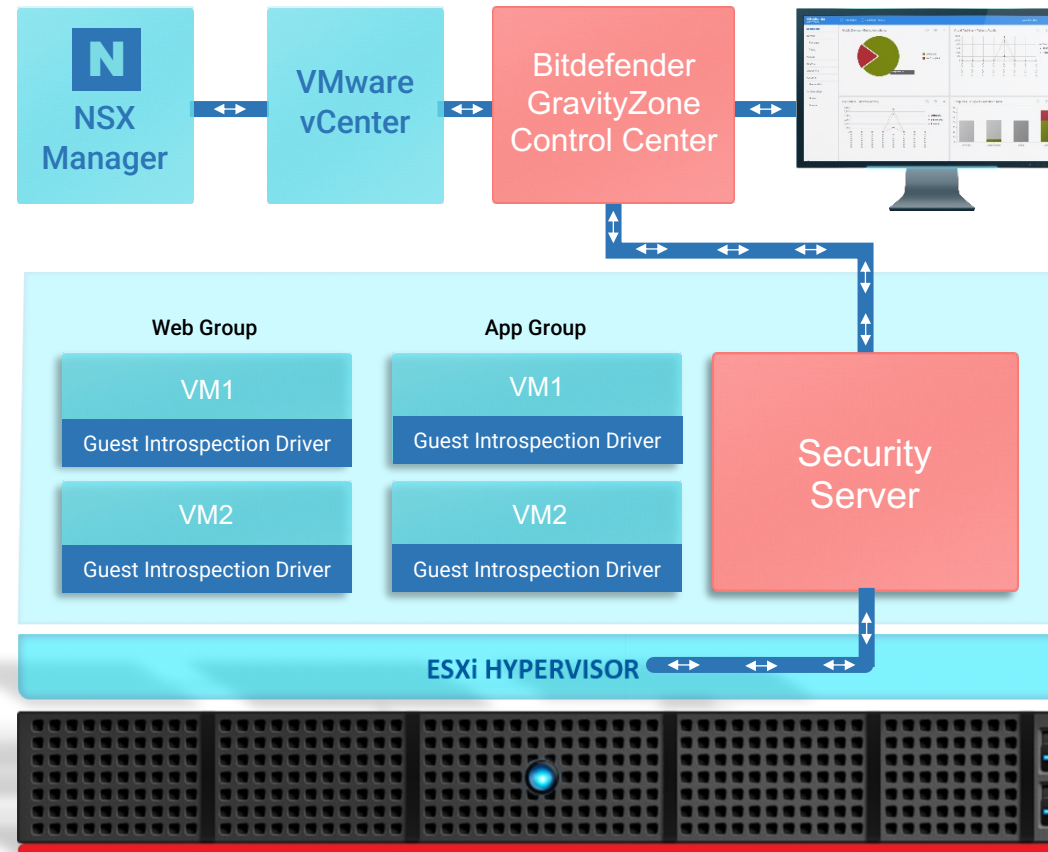
TRADIČNÍ PŘÍSTUP VS. PŘÍSTUP BITDEFENDERU



BEZPEČNOST VIRTUALIZACE

Prostředí VMware s NSX-V / NSX-T

Bitdefender®



Přístup přes NSX sice umíme ale nedoporučujeme používat !

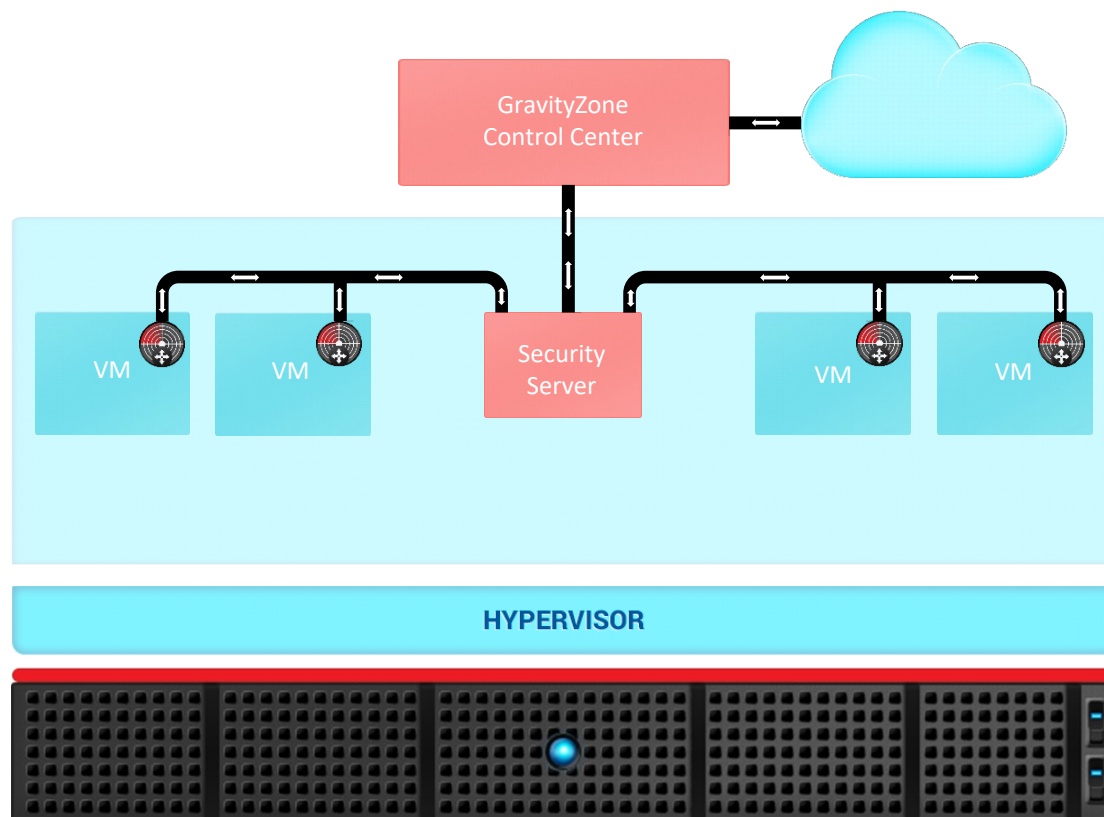
Místo toho doporučujeme ochranu pomocí Bitdefender BEST lehkými klienty s Centrálním Skenováním pomocí security serveru ...

Přístup přes NSX má tyto omezení:

- Pouze **sken souborového systému**
- Nemá přístup do paměti virtualizovaného stroje **tudíž nelze takto chránit proti bezsouborovým útokům**
- host driver **neumožňuje vysokou dostupnost**

SECURITY FOR VIRTUALIZED ENVIRONMENTS

MULTIPLATFORMNÍ ARCHITEKTURA



Pro všechny virtualizační platformy doporučujeme tento způsob ochrany pomocí lehkých klientů. Skenovací proces se přenáší Security Server Appliance.

Jelikož tento způsob funguje přes TCP/IP, tak není závislý na Hypervizoru.

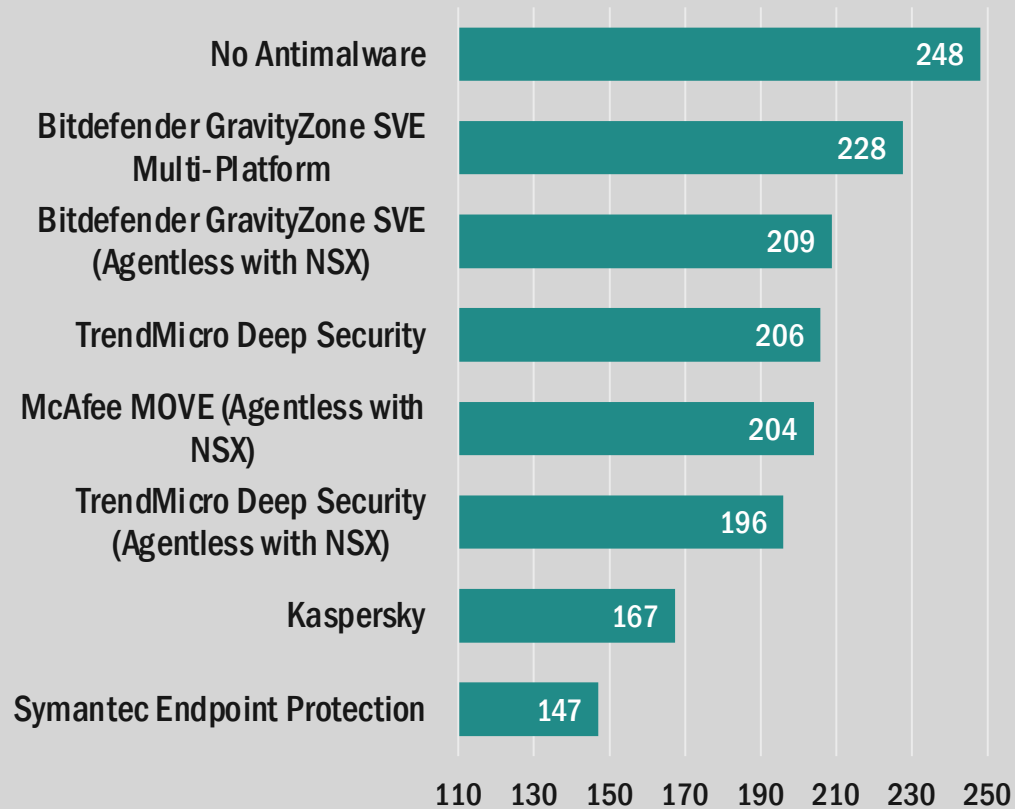


BEST s Centrálním Skenem

Bitdefender

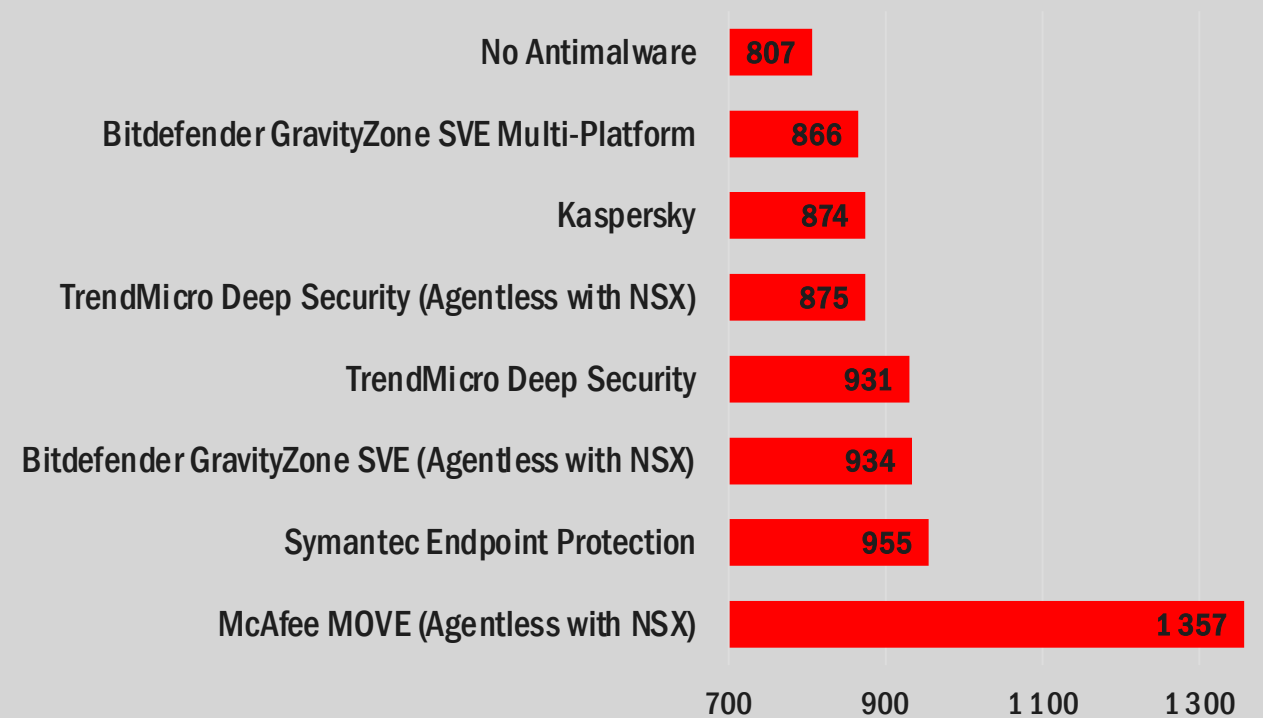
Snížení nároků na infrastrukturu = úspora nákladů

Maximální počet konkurentních VDI Sessions per Host

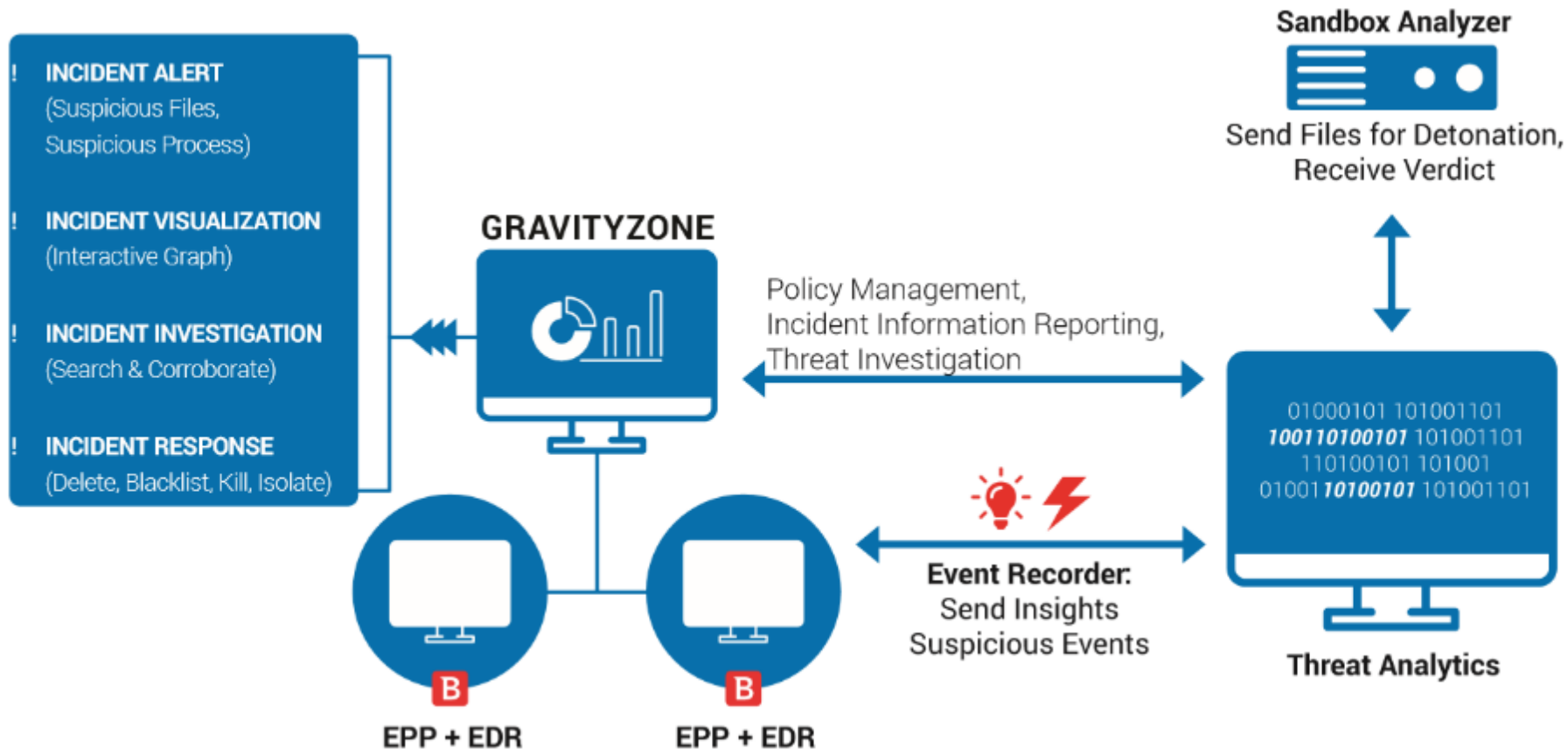


AŽ O 36% RYCHLEJŠÍ ODEZVA APLIKACÍ

Čas odpovědi nestresovaného systému (v Milliseconds)



XEDR – PRO Vizibilitu a RYCHLOU NÁPRAVU

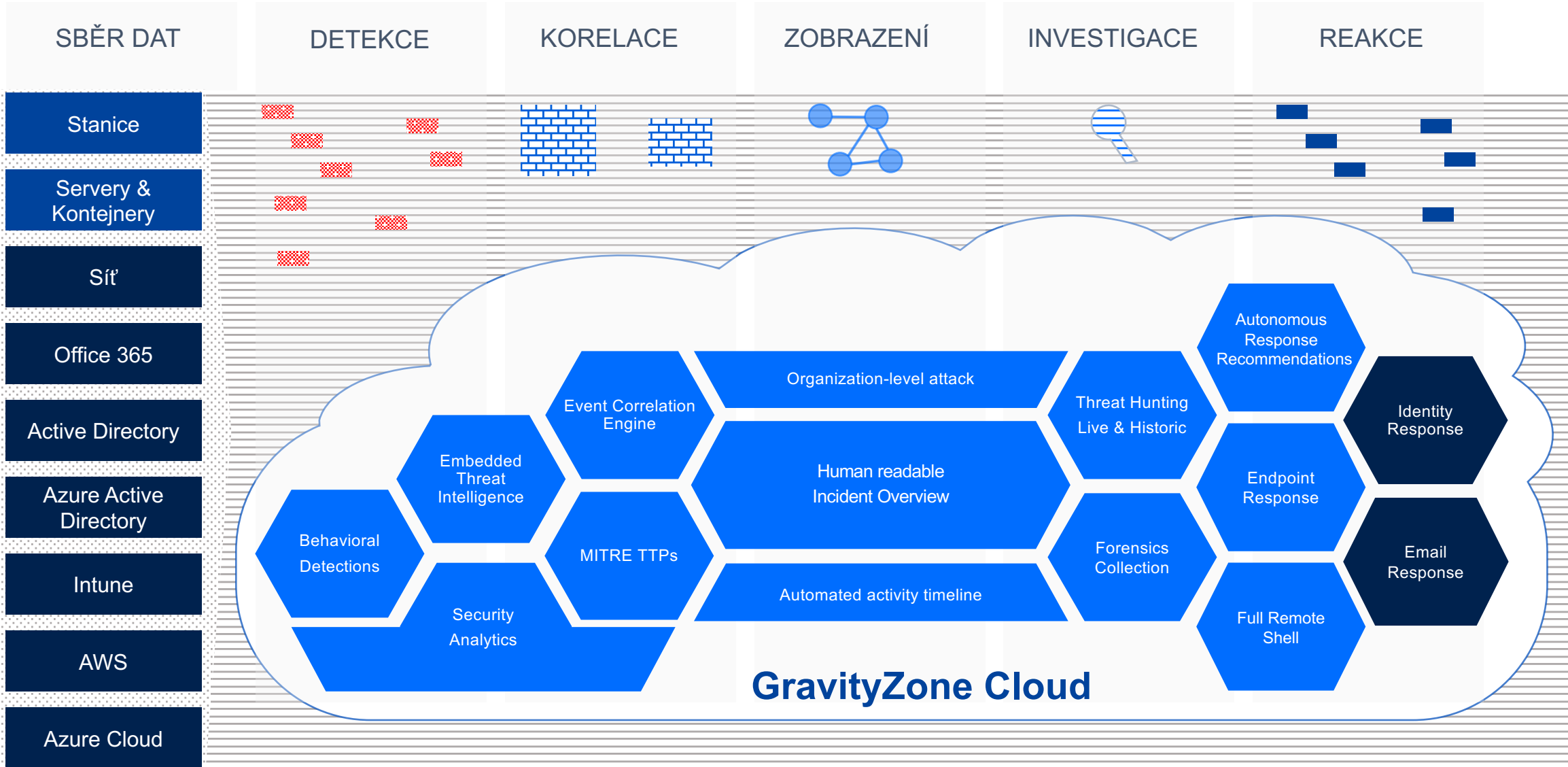


Minimalizuje čas vystavení se nákaze a zastavuje průlomy.

Umožňuje automatickou detekci, jednoduchou investigaci a rychlé vyléčení na jednom místě

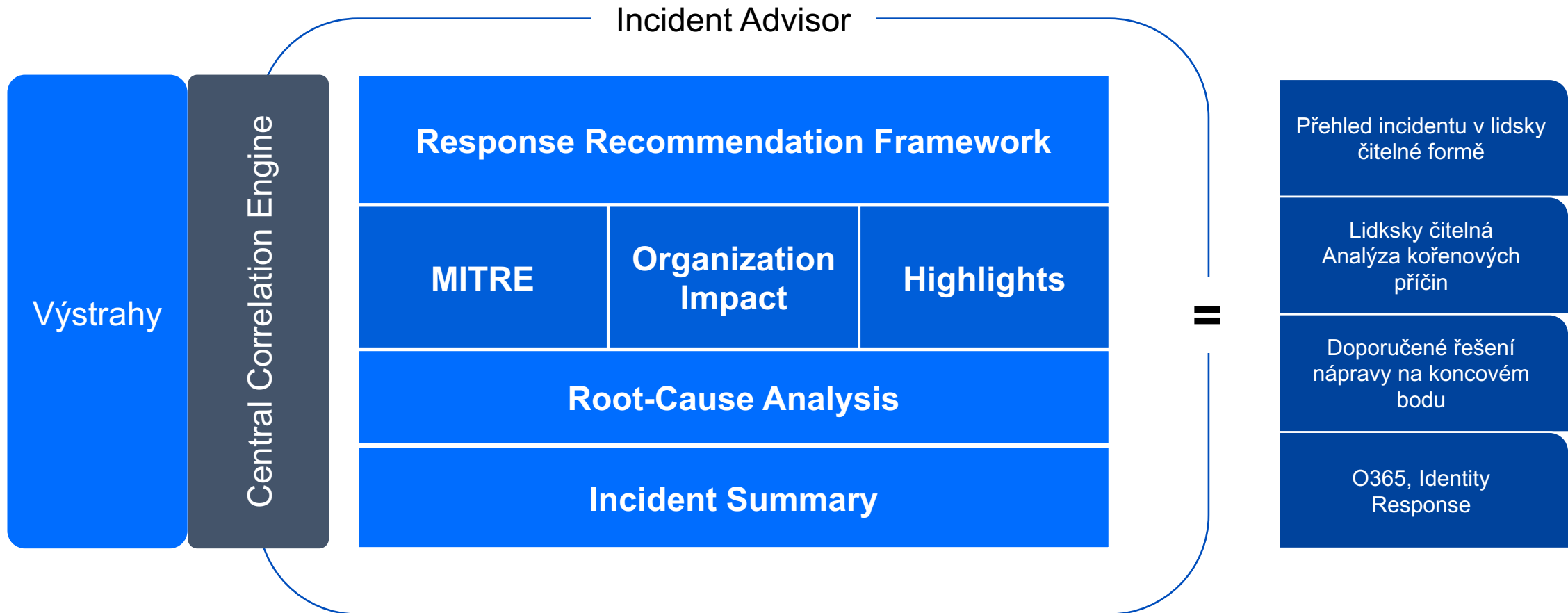
Snižuje požadavky na lidské zdroje a jejich znalosti a schopnosti provádět brzké detekce a nápravná opatření

PŘEHLED



POMOCNÍK S INCIDENTY

Incident Advisor



GravityZone XDR – Incident Advisor

B Welcome, Security Analyst

INCIDENT #582 Status Open

Back Overview Graph Alerts Response

83/100 Incident Severity Score

Created: 01 Feb 2022, 13:13:48
Last updated: 01 Feb 2022, 13:19:31
Type of attack: Exfiltration, Exploit, SpearPhishing

ORGANIZATION IMPACT

6 2 3 9

SUMMARY

A potential network breach originating from 2 users has been detected as part of 5 alerts affecting the following: 2 managed assets and 2 users.

Lateral Movement originating from managed asset: BOB-PC and user: alice has been detected in your network as part of 12 alerts affecting the following: unmanaged asset: FILESERVER2.cloudoffice.local 5 managed assets and user: bob. Multiple attempts to gain or maintain the persistence of a possible malicious objects were detected in 3 alerts on managed asset: CFO-PC and user: administrator@cloudoffice.local. These 3 managed assets were the source of malicious actions detected in 57 alerts affecting 5 managed assets and 2 external ips. Sensitive data may have been exfiltrated to external ip: 100.0.1.111 based on 3 alerts originating from managed asset: CEO-PC.

ROOT CAUSE

The attacker gained access to the network because a malicious email was received on O365 user: alice on managed asset: ALICE-PC.cloudoffice.local from external address: gesteban.cloud@gmail.com resulting in a connection to an external ip 100.0.1.111.

ATT&CK TACTICS AND TECHNIQUES

Initial Access	T1566 Phishing
	T1078 Valid Accounts
	T1190 Exploit Public-Facing Application
Execution	T1204 User Execution
	T1059 Command and Scripting Interpreter
Persistence	T1137 Office Application Startup
	T1078 Valid Accounts

HIGHLIGHTS

- Suspicious Email Received** | Initial Access
Severity: Low
An email containing suspicious attachments has been received.
Detected by Endpoint on 01 Feb 2022 at 13:12:59
1 1
+ 4 OTHER INITIAL ACCESS ALERTS
- Exploit NRPC CVE-2020-1472 ZeroLogon** | Lateral Movement
Severity: High
Network Attack Defense has detected a crafted login attempt that exploits an elevation of privilege vulnerability via Netlogon Remote Protocol.
Detected by Endpoint on 01 Feb 2022 at 13:15:41
1 1
+ 11 OTHER LATERAL MOVEMENT ALERTS
- KerberosBruteForce** | Persistence
Severity: Medium
Possible brute force attack on a service server that uses kerberos login.
Detected by Endpoint on 01 Feb 2022 at 13:16:13
1 1
+ 2 OTHER PERSISTENCE ALERTS
- Generic.Exploit.Shellcode.2.7E50AF52** | Execution
Severity: High
Shell code used for post exploitation has been loaded into memory

RESPONSE

ACTION NEEDED (49) EXECUTED (3)

CONTAINMENT

- 3 Users to block
- 8 Hosts to isolate

[VIEW DETAILS](#)

MITIGATION

- 1 IP address to block
- 2 File hashes to block
- 1 Security solution to instal on unmanaged asset
- 1 Email address to block

[VIEW DETAILS](#)

REMEDIATION

- 1 Email to delete
- 8 AM scans to run
- 8 System repairs to run

[VIEW DETAILS](#)

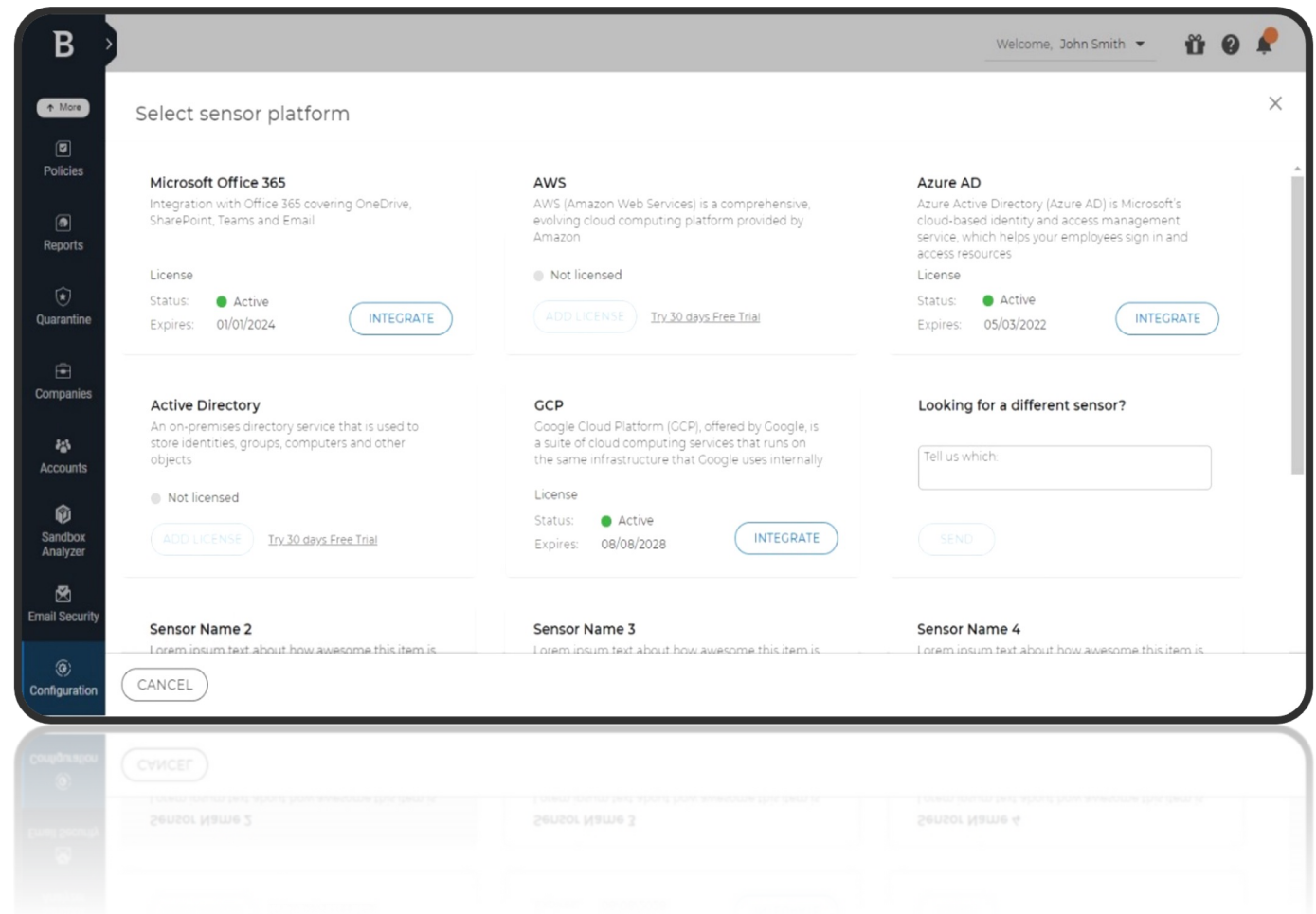
HAPPENING

GravityZone XDR – Incident Graph

The screenshot displays the GravityZone XDR Incident Graph interface. At the top, a navigation bar includes a 'Back' button, 'Overview', 'Graph' (selected), 'Alerts', and 'Response' tabs. The top right corner shows 'Welcome, Security Analyst' and an incident summary: 'INCIDENT #582' with a status of 'Investigating'. A left sidebar contains a navigation menu with categories like Monitoring, Incidents, Threats Xplorer, Network, Risk Management, Policies, Reports, Quarantine, Accounts, Sandbox Analyzer, and Configuration. The main area is titled 'Activity' and is grouped by 'Kill Chain'. It is divided into three main sections: 'INITIAL ACCESS', 'EXECUTION', and 'EXIT POINTS'. The 'INITIAL ACCESS' section shows an email address 'gesteban.cloud@...' leading to 'ALICE-PC.cloudof...'. The 'EXECUTION' section shows a sequence of events: 'Suspicious Email Received' (2 alerts), 'SuspiciousEmailsReceivedInTransition' (13 alerts), 'SuspiciousEmailsReceivedInTransition' (15 alerts), and 'SuspiciousEmailsReceivedInTransition' (18 alerts). The 'EXIT POINTS' section shows an IP address '100.0.1.111' leading to 'BOB-PC.cloudoffi...'. The graph also shows various alerts and actions such as 'Exploit NRPC CVE-2020-1472...', 'KerberosBruteForce', 'SuspiciousLogin', and 'Attack Bruteforce SSH'. The interface includes search and zoom controls at the top right and a filter icon at the bottom right.

ZDROJE DAT PRO XDR

- **Microsoft Office365**
 - OneDrive
 - SharePoint
 - MS Teams
 - Email
- **Google Cloud Platform**
 - Google Workspace
- **Identity**
 - On-premise AD
 - Azure AD
 - MS Intune
- **Cloud**
 - AWS
 - Azure
- **Network**
 - Bitdefender Network Sensor



INVESTIGACE

■ Vyhledávání

- Pokročilé filtrování
- Rozšířený pohled na data
- Více datových zdrojů
- Smart views

■ Hledání v reálném čase

- Live Search napříč endpointy
- OS: Windows, Linux, Mac

■ Balíček investigace

- Získávání forenzních informací
- OS: Windows, Linux, Mac

■ Plnohodnotný Remote Shell

- Přímá investigace a reakce napříč endpointy
- OS: Windows, Linux, Mac

The screenshot displays the Bitdefender Security Center interface. The search bar contains the query: `process.parent_path: *explorer.exe AND process.path: *cmd.exe`. The search results are displayed in a table with the following columns: Date, Source, Event, Detection name, Type, Score, Timestamp, MITRE tactics, and MITRE techniques. The results show a series of events from August 18, 2021, to August 25, 2021, all originating from source `hr-ro_0987` and involving the `ctc_raw_pr...` process. The events are categorized as 'Raw event' or 'Alert' with a score of 1. The MITRE tactics listed are 'Execution' and the MITRE techniques are 'Command and s...'. The interface also shows a sidebar with navigation options like Dashboard, Incidents, Threats Explorer, Network, Risk Management, Policies, Reports, Quarantine, and Companies.

Date	Source	Event	Detection name	Type	Score	Timestamp	MITRE tactics	MITRE techniq...
25 Aug 2021, 10:27	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
24 Aug 2021, 01:18	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Alert	1	16305074...	Execution	Command and s...
23 Aug 2021, 02:51	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
22 Aug 2021, 11:34	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Alert	1	16305074...	Execution	Command and s...
21 Aug 2021, 06:57	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
20 Aug 2021, 11:23	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
19 Aug 2021, 02:12	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
19 Aug 2021, 02:12	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
18 Aug 2021, 16:11	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...

DETEKCE A REAKCE

■ Pomocník s incidenty

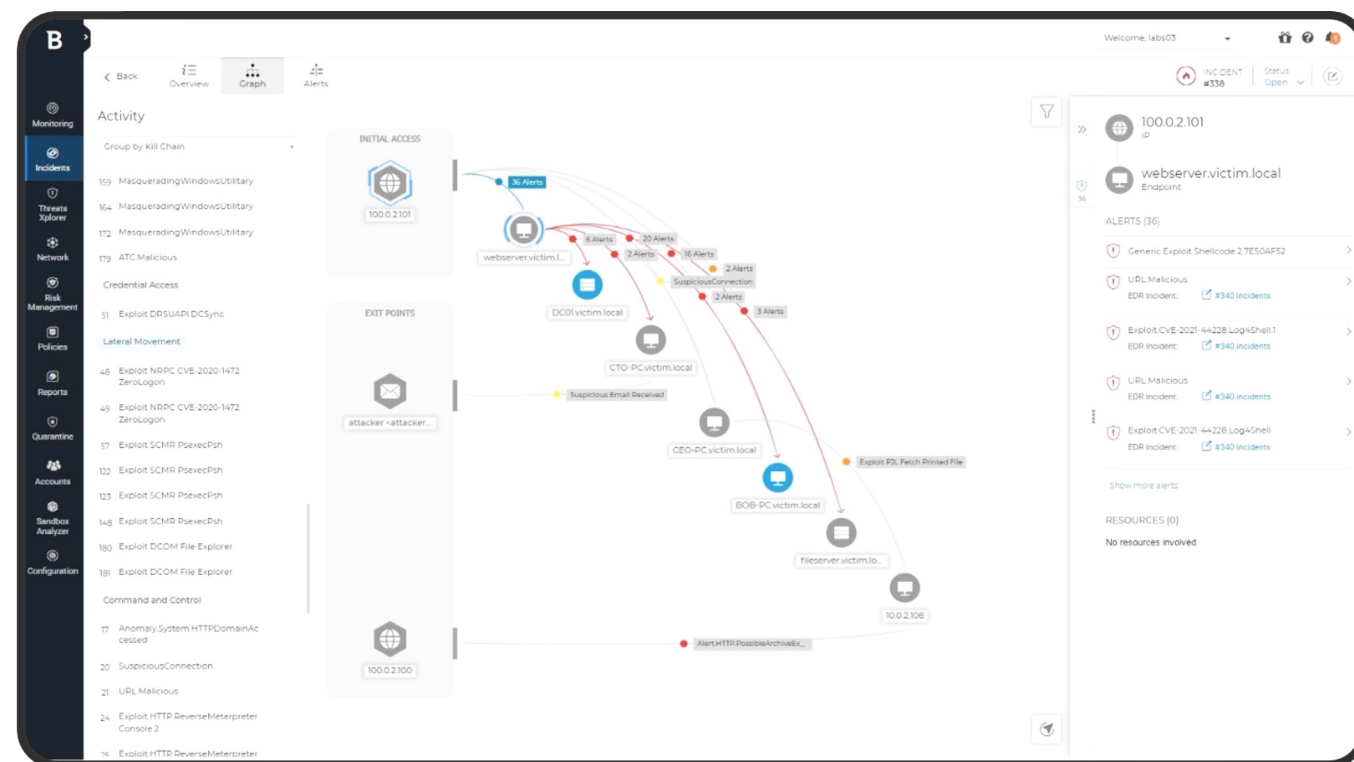
- Shrnutí
- Root Cause
- Organization Impact
- Highlights

■ Reakce

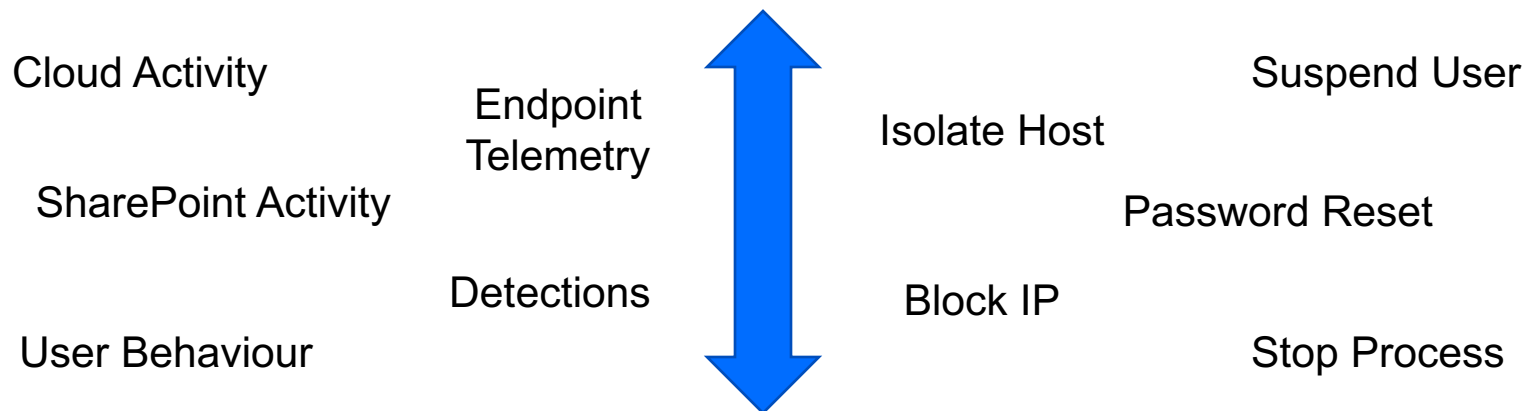
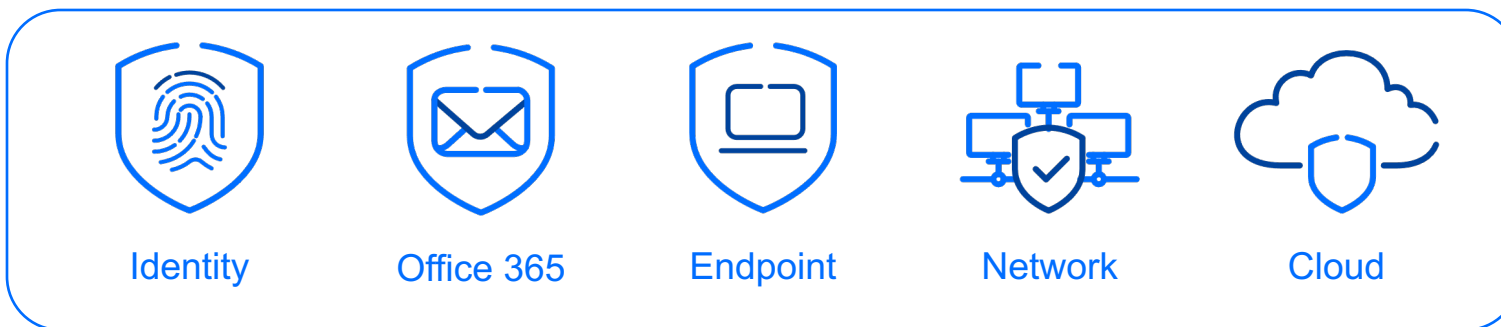
- Doporučení
- Endpoint
- Office365
- Identity
- Seznam spuštěných akcí

■ Grafické zobrazení

- Initial Access
- Exit Points
- Multiple Resource types
- Alerts on Transitions



GravityZone XDR vytvořeno pro MDR



Bitdefender MDR

IS4 SECURITY

Vendor
Representative
Company



Společnost IS4 security s.r.o. působí jako lokální zastoupení několika značek pro Českou Republiku a Slovensko

Za Bitdefender zajišťujeme kompletní servis:

- před/po prodejní technickou podporu v českém jazyce

[+420 245 501 801](tel:+420245501801)

<https://support.bitdef.cz/>

helpdesk@bitdef.cz

- lokalizaci produktů B2C i B2B do češtiny
- obchodní i technická školení
- pomoc s výběrem vhodného produktu pro prostředí vašeho zákazníka

info@bitdef.cz