Bitdefender

Jak snížit (TCO) provozní náklady bezpečnostního produktu na minimum?

Rene Pospisil, Bitdefender Country Manager CZ/SK

Bitdefender

Zpravodajství o pokročilých hrozbách

Průběžně integrováno do prevenčních technologií, analytických služeb a MDR operací

30 miliard Množství odhalených hrozeb na stovkách milionů senzorů (celosvětově) každý den

400+ Hrozeb odhaleno každou minutu

19 Zveřejněno dešifrovacích nástrojů po útoku Ransomwarem

Miliardy $ Pomohli jsme orgánům činným v trestním řízení dopadnout organizace, u nichž se dopad jejich činnosti odhaduje řádově v miliardách USD

825 Elitních bezpečnostních výzkumníků, lovců hrozeb a bezpečnostních analytiků. Spolupracují blízce při reakci na hrozby s orgány činnými v trestním řízení a s vedoucími akademiky v oblastech kvatových počítačů a kryptografii

400+ Zaměstnanců ve výzkumu a vývoji zaměřeného na cloud, nově vznikající technologie, IoT a strojové učení

UZNÁVANÝ INNOVATIVNÍ LÍDR

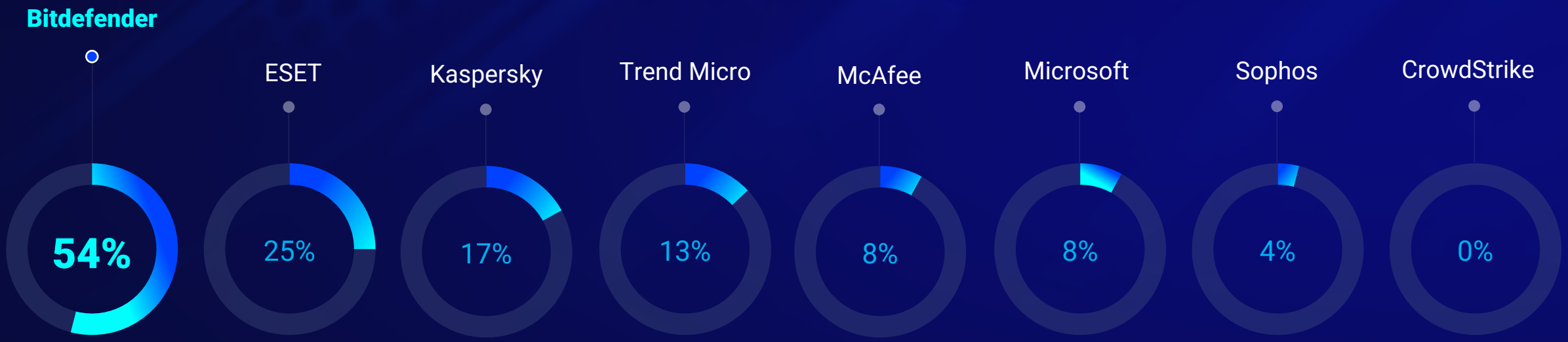
PATENTOVÉ PORTFOLIO: 111+ SCHVÁLENÝCH, 200+ PŘED SCHVÁLENÍM.
PRŮKOPNÍK V OBLASTI NASAZENÍ STROJOVÉHO UČENÍ JIŽ OD 2008.

Bitdefender

MARCH 26, 2022

NEJVÝKONNĚJŠÍ PREVENCE PROTI ÚTOKU

Nejvíce #1 hodnocení od 2018 do 2021 v AV comparatives test.



Bitdefender

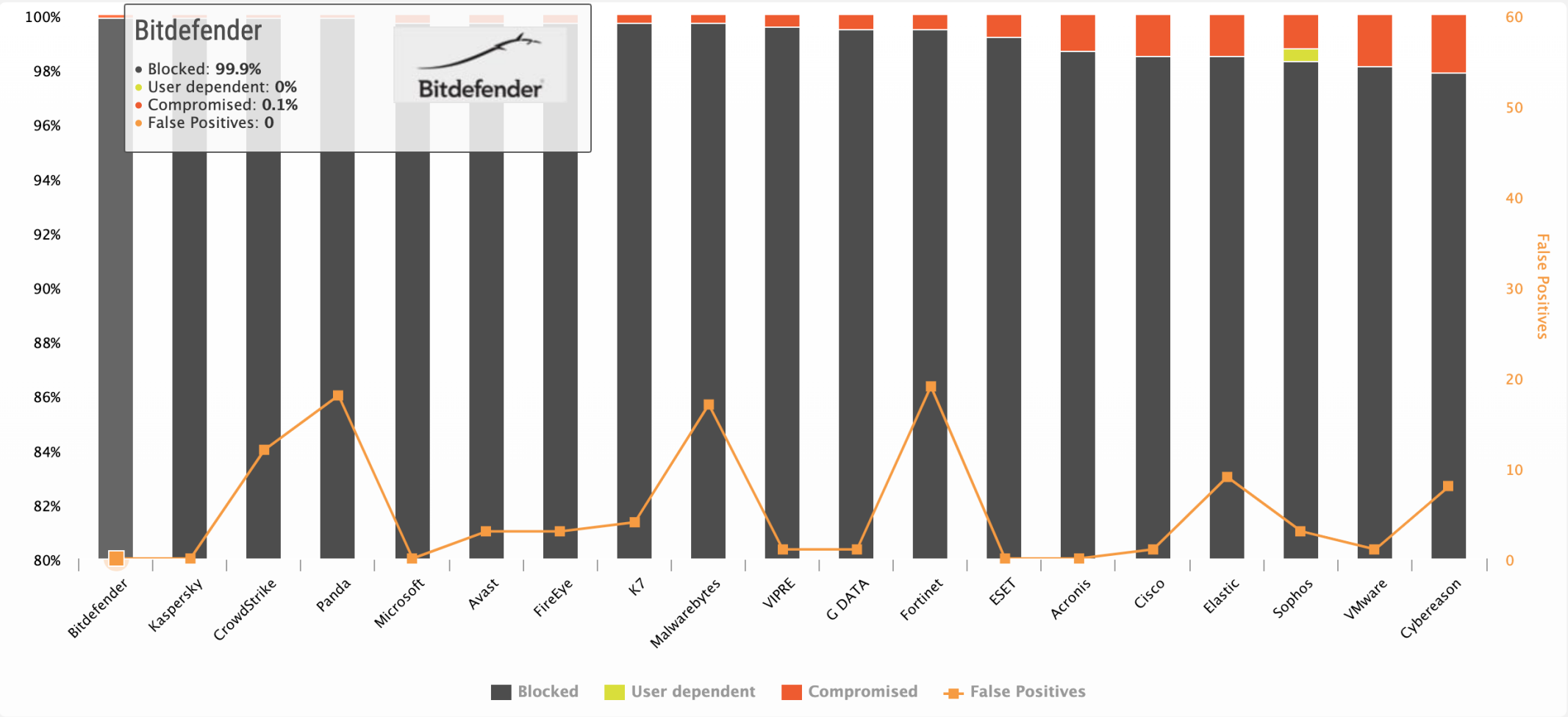
AV comparatives

BASED ON ENTERPRISE AV COMPARATIVES RESULTS FROM JAN 2018 UP TO JAN 2021 (REAL-WORLD PROTECTION, PERFORMANCE, MALWARE PROTECTION TESTS & ADVANCED THREAT PROTECTION).

Enterprise Test Charts

Export

Enterprise | Real-World Protection Test | 2021 | Aug-Nov | by protection value | 80 - 100%



https://www.av-comparatives.org/comparison/?usertype=enterprise&chart_chart=chart2&chart_year=2021&chart_month=Aug-Nov&chart_sort=1&chart_zoom=3

TECHNOLOGIE & SLUŽBY

EPP ochrana koncových bodů

Rozšířené EDR

Bezpečnost pro Cloud

Managed Detection and Response

Bitdefender GravityZone

Prevence porti útokům | Detekce Anomálií | Bezpečnostní Analytika | Threat Intelligence

Workstations

Servers

Virtual Machines

Cloud Platforms

Containers

Účinnost bezpečnosti

Optimalizace pracovní zátěže

Automatizace správy

B2C i B2B produkty jsou kompletně lokalizovány a průběžně podporovány již 7. rokem k dispozici kompletně v českém jazyce

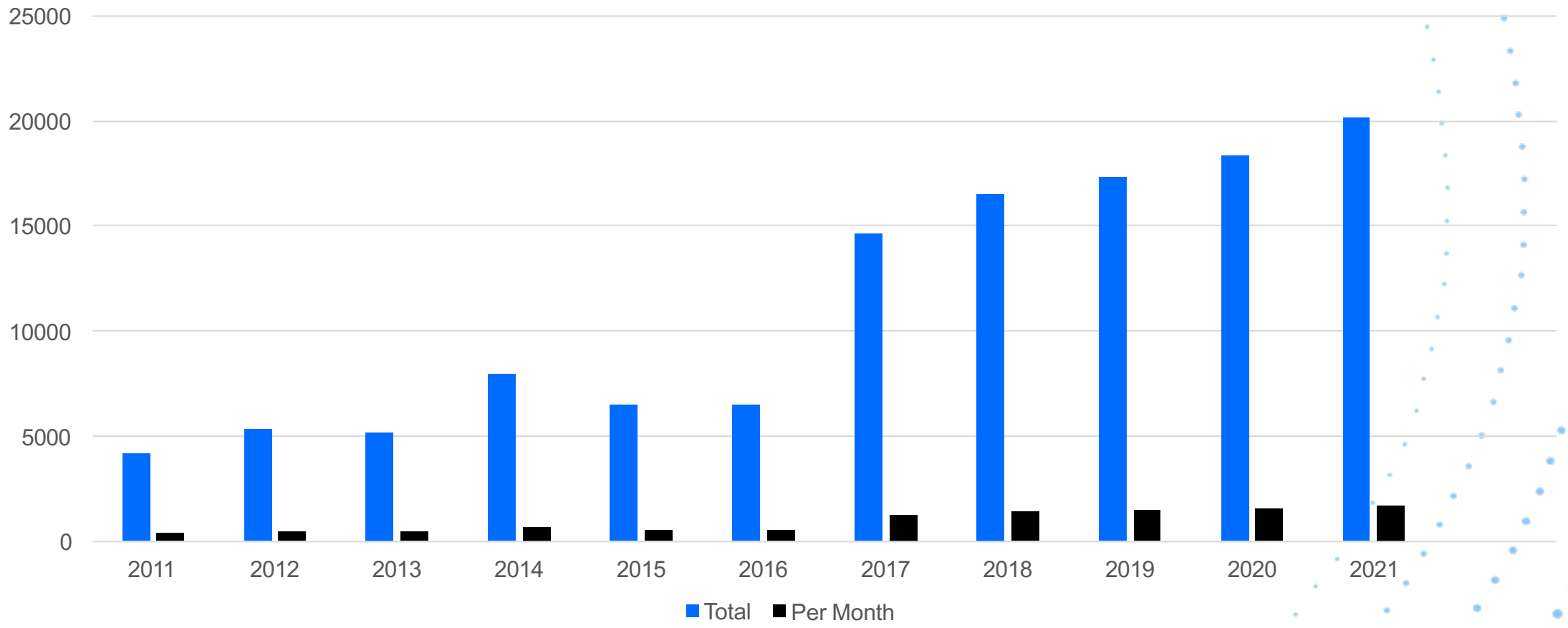
REvil AKA Sodinokibi Ransomware

Bitdefender pomohl odhalit zločince a ušetřil >10 miliard kč

REvil ransom demand for an encrypted MSP

Zranitelnosti v roce 2021 stouply …
Jak řešíte instalace aktualizací a záplat ?

Bitdefender



Bitdefender

Výzvy v kyberbezpečnosti

2022

✓ **Příliš mnoho nástrojů a příliš velká nepřehlednost**
Zkoušení, implementace, učení a správa mnoha nástrojů

✓ **Nedostatečná prevence**
Vysoké riziko průlomů, vysoká míra „šumu“ (nepodstatných informací), vysoká závislost na obsluze pro detekci a rekci vs. Automatizace

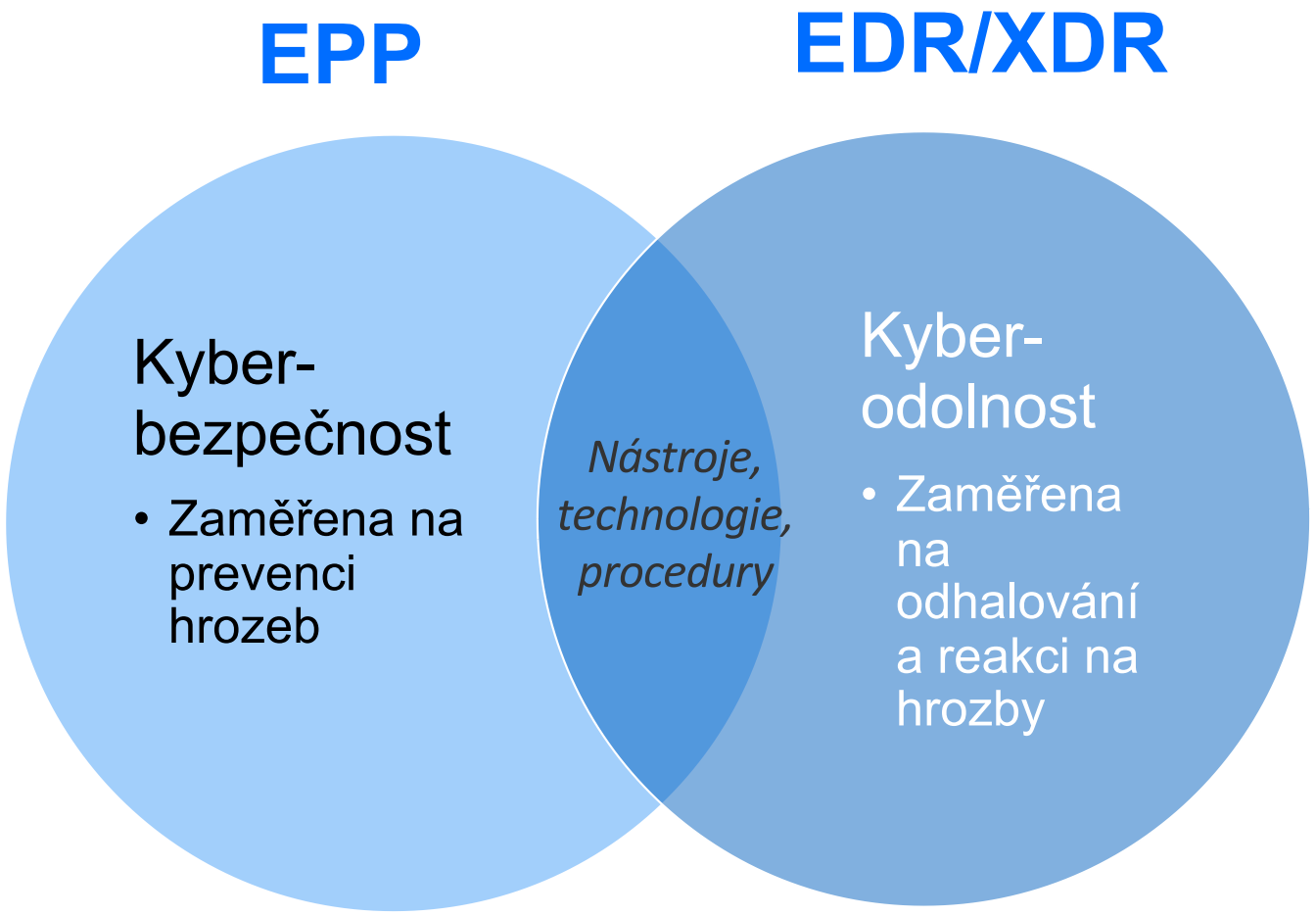
✓ **Oba přístupy - In-house i outsourcing mají svá rizika**
Je těžké sehnat in-house bezpečnostní experty pro zajištění provozu 24/7, laciný outsourcing nemá dostatečnou expertízu pro efektivní odpověď na odhalenou hrozbu

✓ **Je obtížné si udržovat náskok před vyvíjejícími se hrozbami**
Je velmi těžké porozumět kontextu , těžké rychle analyzovat a zamezit šíření..

✓ **Omezené rozpočty a neefektivní utrácení**
Vyšší cena, nižší ROI (návratnost) z nákupu mnoha nástrojů a služeb, zvýšené nároky na kvalitu a počet zaměstnanců

ROLE EPP vs EDR/XDR

Bitdefender



Bitdefender

Nový přístup:

Definice kyberodolnosti

“Schopnost udržet **důvěrnost, integritu a dostupnost** systémů a dat pomocí:

a) zabránění

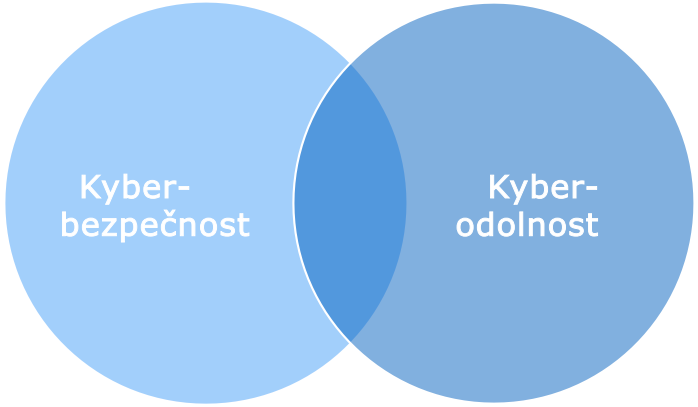
kyberútokům ve způsobení incidentu

NEBO / A

b) odhalení útoku a **reakce** omezující dopad tohoto útoku **v rámci předem stanovených mezí**.”

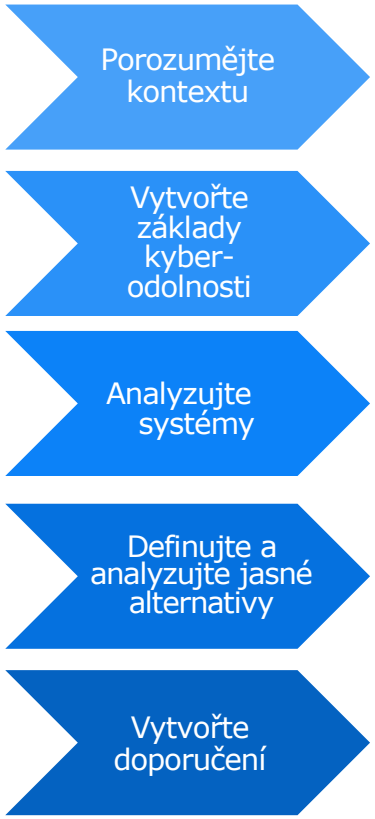
EPP

EDR/XDR

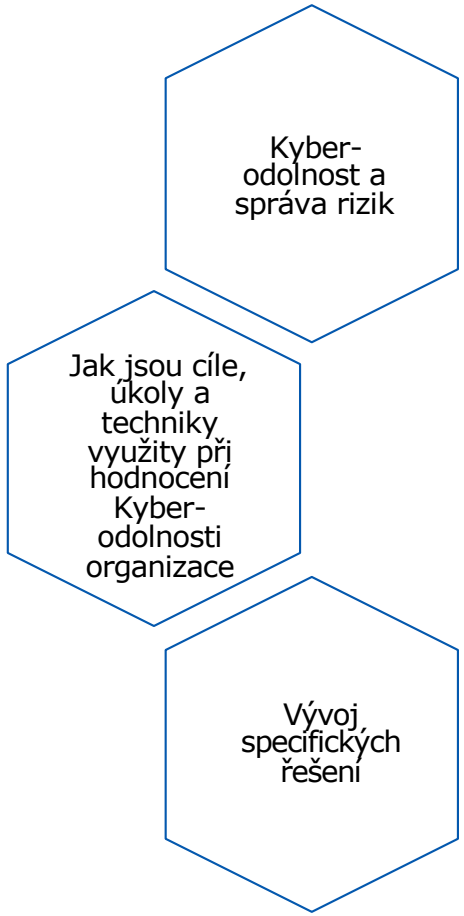


Důležitost kyberodolnosti v roce 2022

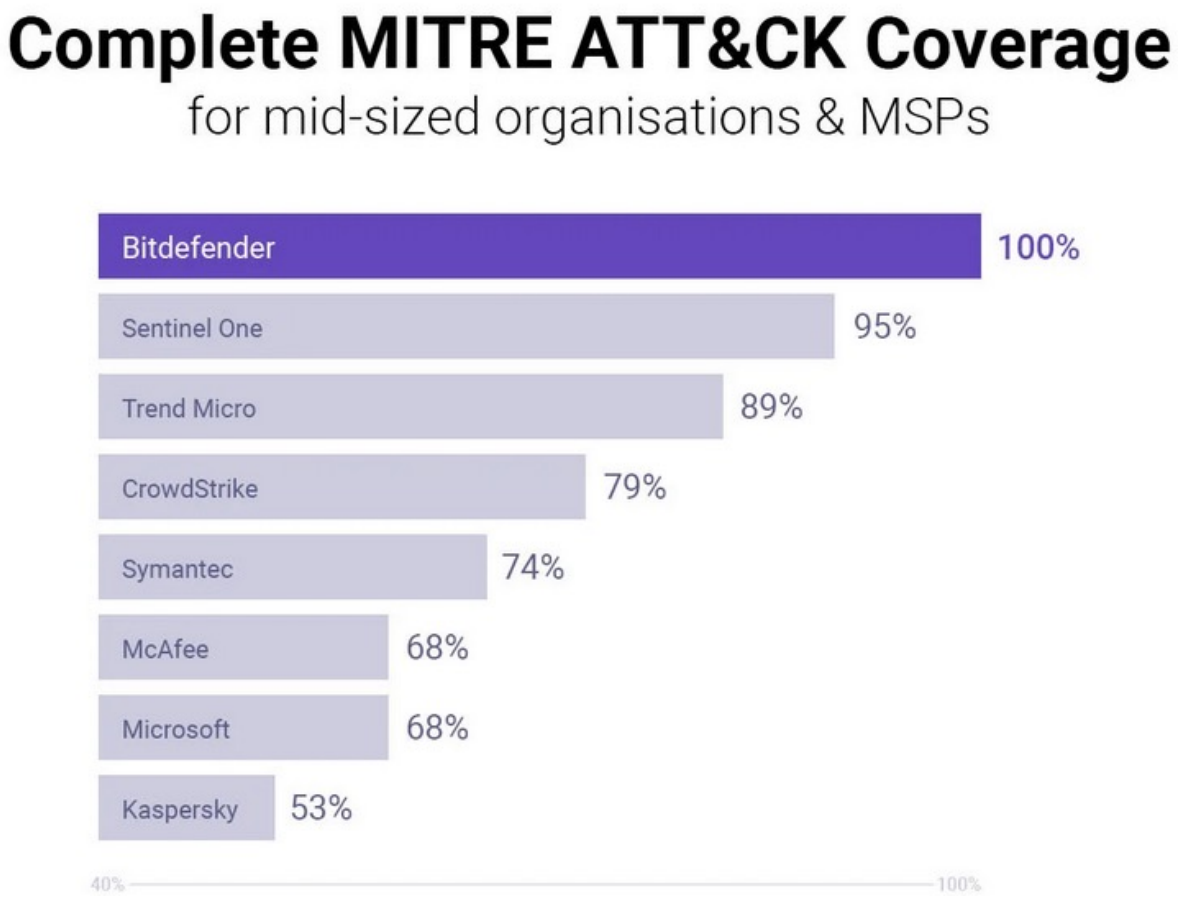
SCRAM



MITRE



EDR, XDR, MDR



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 šíře 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.

Bitdefender GravityZone®

Bitdefender

Cesta jak snížit počet nástrojů na minimum a vše zjednodušit

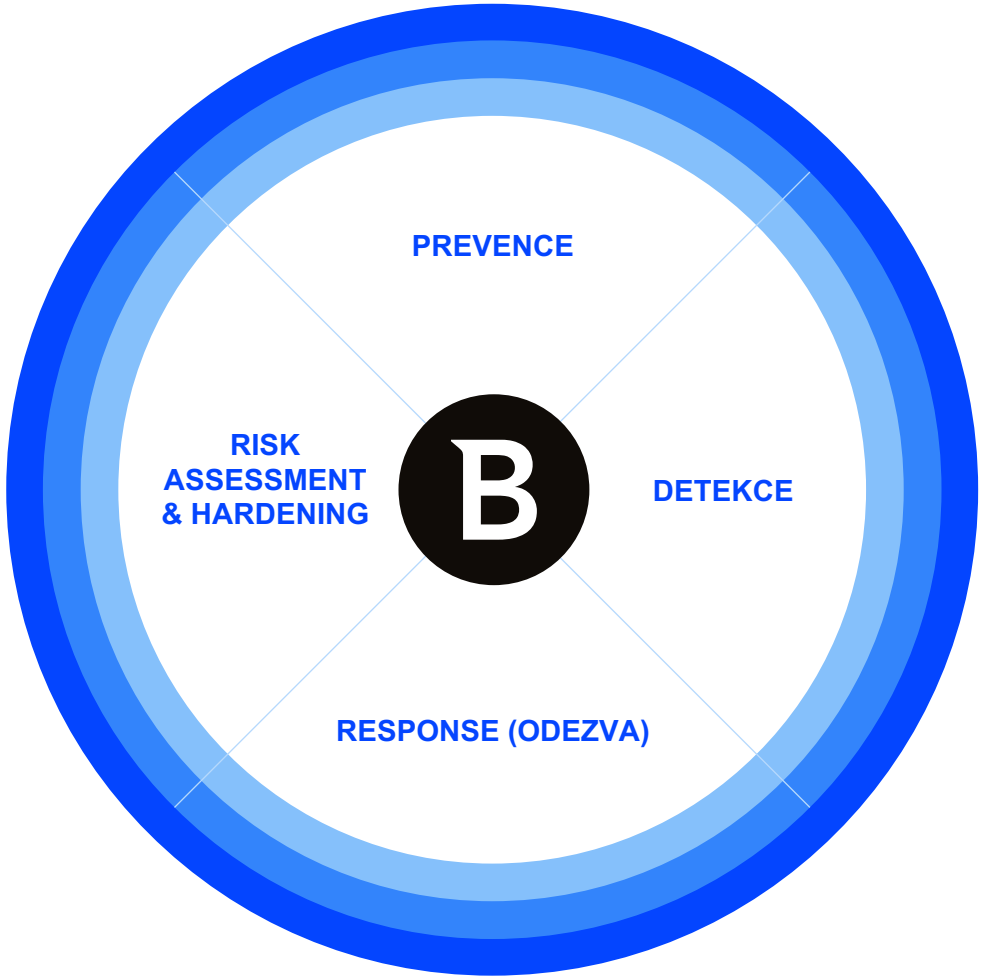
Jednotné řešení Ochrany a analytiky koncových bodů (EPP + EDR)

Bitdefender pracuje **napříč koncovými body a hybridním** prostředím **s vysokou účinností**, mnoha bezpečnostními funkcemi a **jednoduchou správou v českém jazyce.**

- **Jedna aplikace,** nízký dopad na zdroje (Windows, Linux, Mac)
- Nastaví se jednou, nasadí všude (fyzické, virtuální, kontejnery, cloudy)
- **Jedna konzole**, **jedna instalace**

Výběr z **EPP (prevence) a EDR (detekce a reakce)**

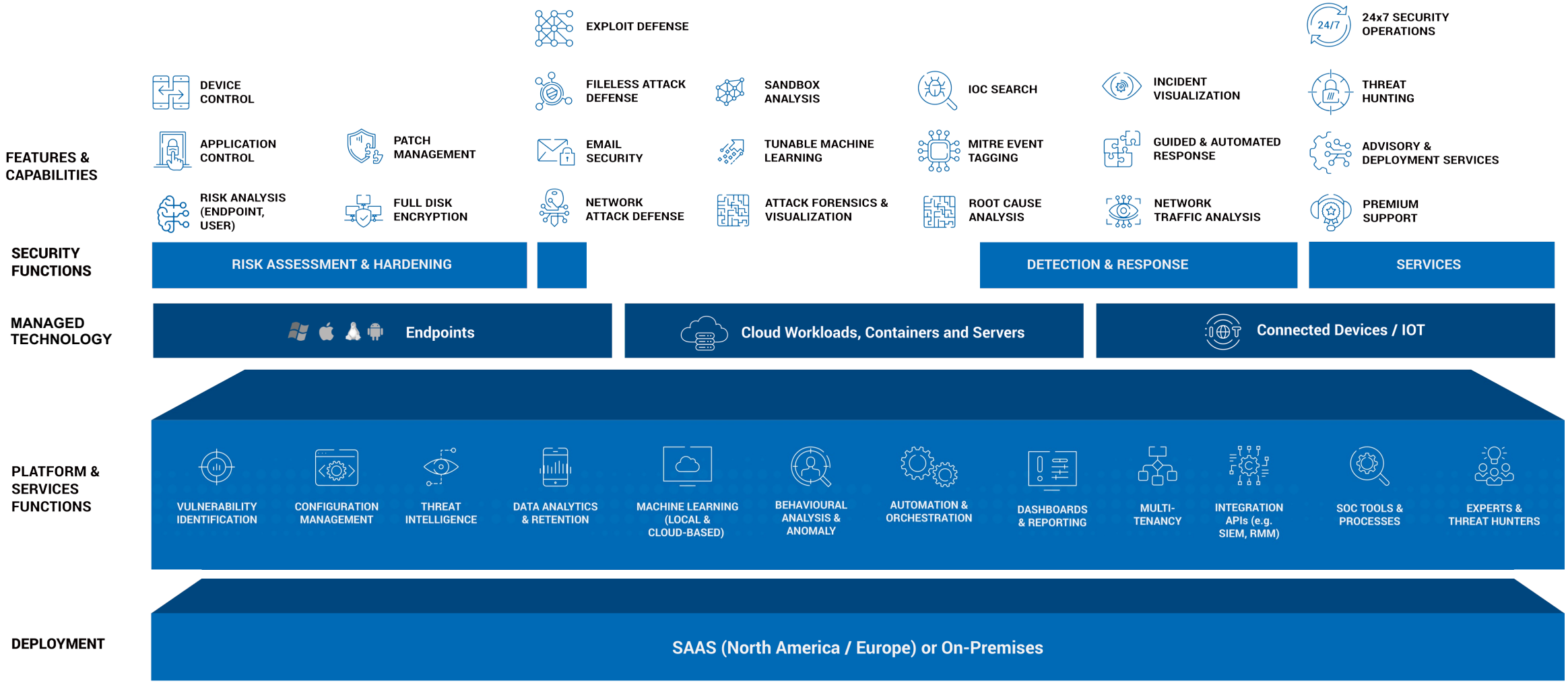
- Může být nasazeno jako plné kombinované EPP/EDR **Přídavné moduly** pro **správu aktualizací** (OS i aplikací třetích stran), ochrana **e-mailů, šifrování pevných disků a ochranu síťových datových úložišť**



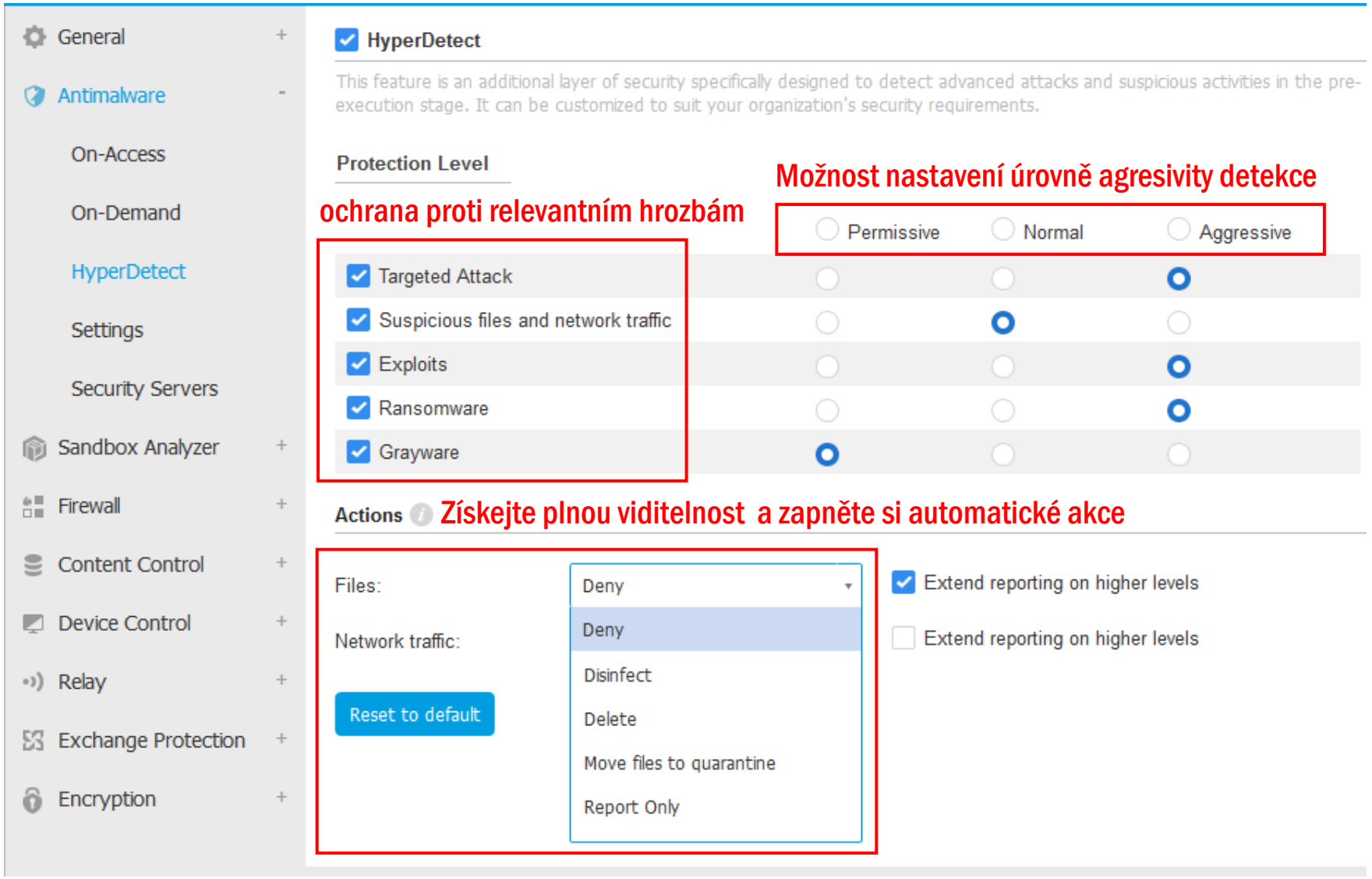
30 Vrstev ochrany v jedné konzoli správy v jednom agentu v českém jazyce

Bitdefender

Architektura Bitdefender GravityZone pro Kyberodolnost



POKROČLÁ, ÚČINNÁ a PŘESNÁ DETEKCE - Hyperdetect



Chrání proti:

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

Dodává plnou vizibilitu ohledně podezdřelých aktivit

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 společnostem prokázat dodržování předpisů
- Automatické upozornění správce IT na chybějící bezpečnostní/nebezpečnostní aktualizace.

Pojistka proti zašifrování Ransomware remediace

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 simultaror 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**

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 noteboocích, 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

Nová ochrana OS Linux a Kontejnerů

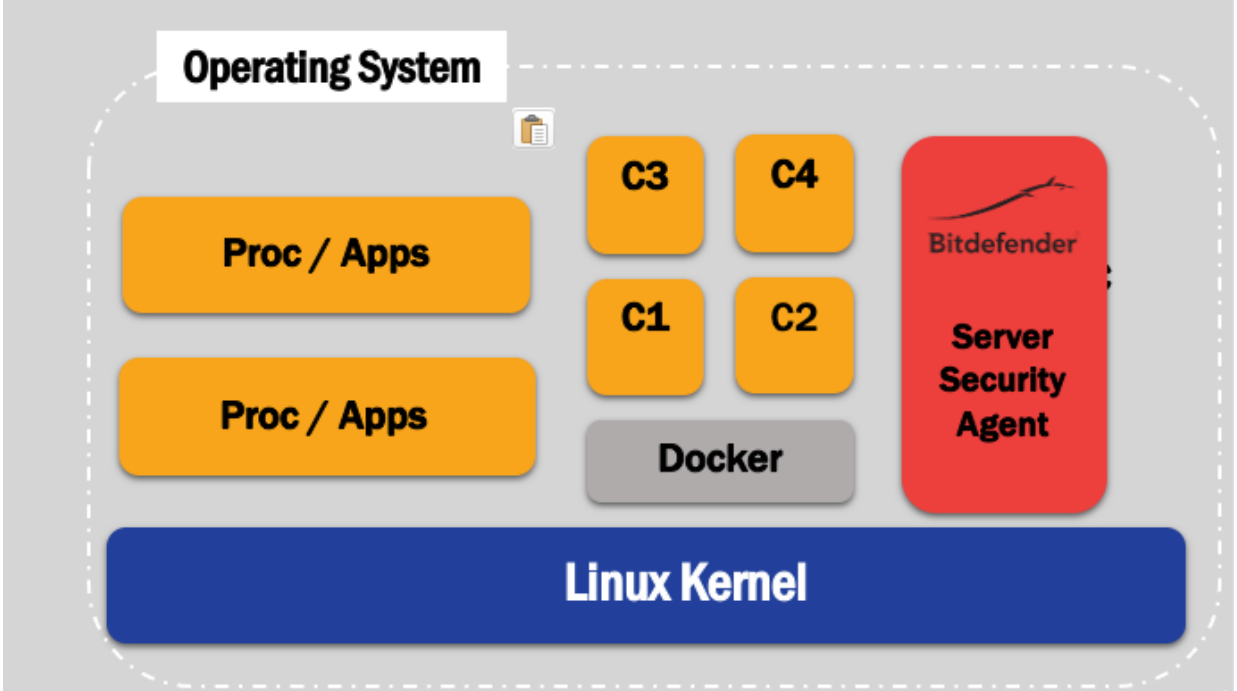
“zbavte se závislosti na jádru”

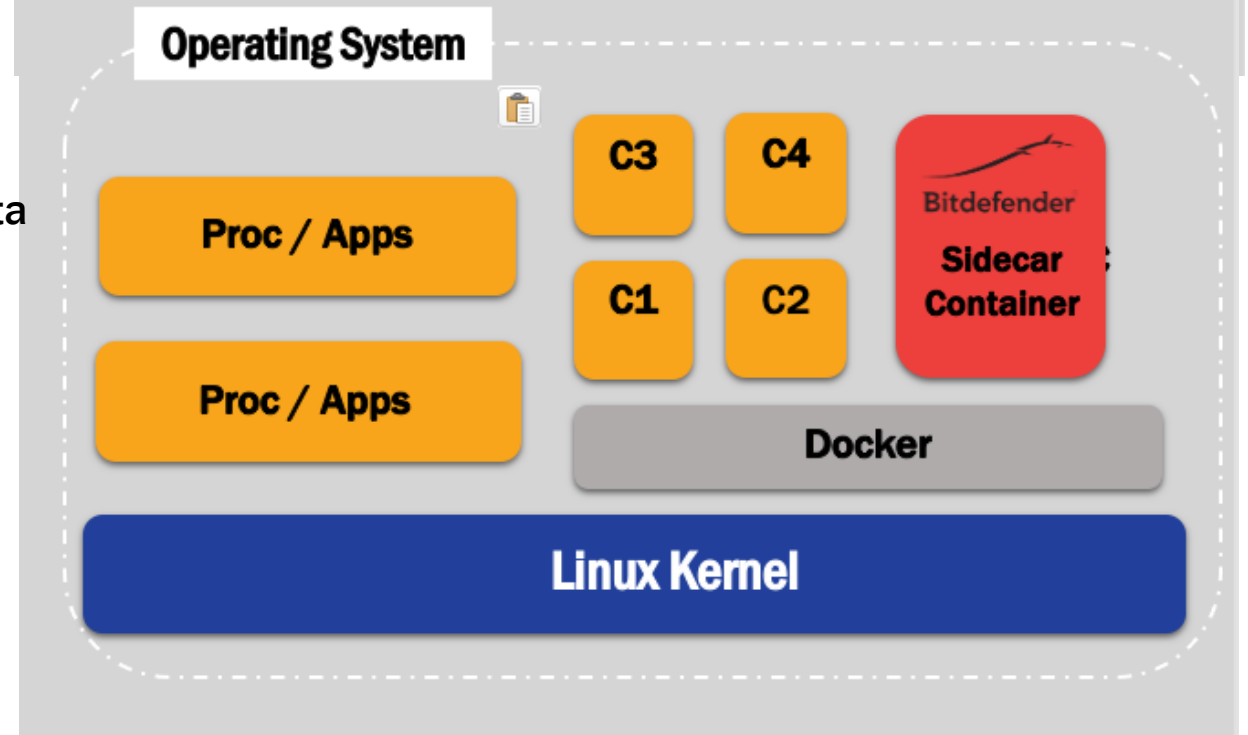
1. Model nasazení: Guest Agent

- 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

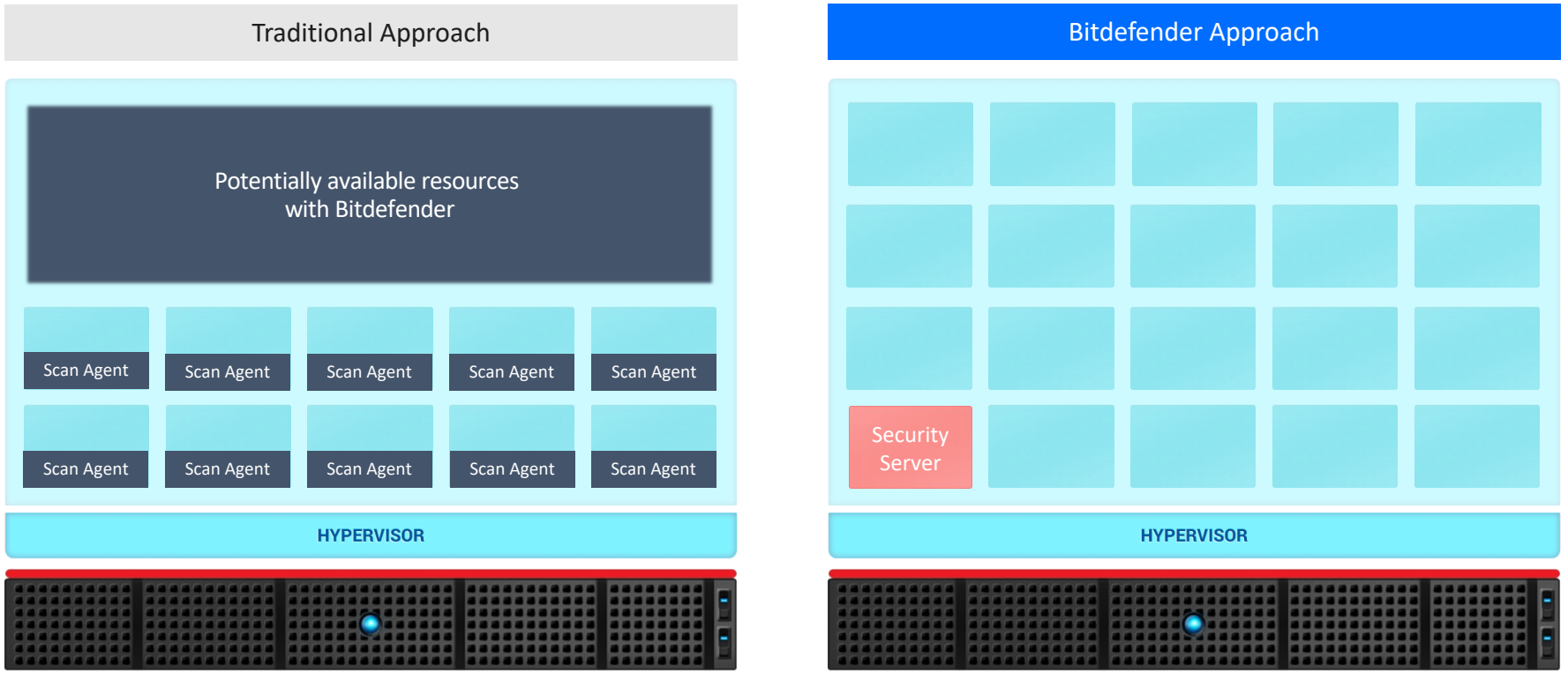
- Vhodný pro prostředí která neumožňují přímý přístup na hosta
- Nasazení PaaS
  - Cloud-nativní distros
- Běží jako privilegovaný kontejner
  - Monitoruje sousedící kontejnery
  - Monitoruje guest OS
- Běží na “OCI compliant runtimes”





OCHRANA VIRTUALIZACE

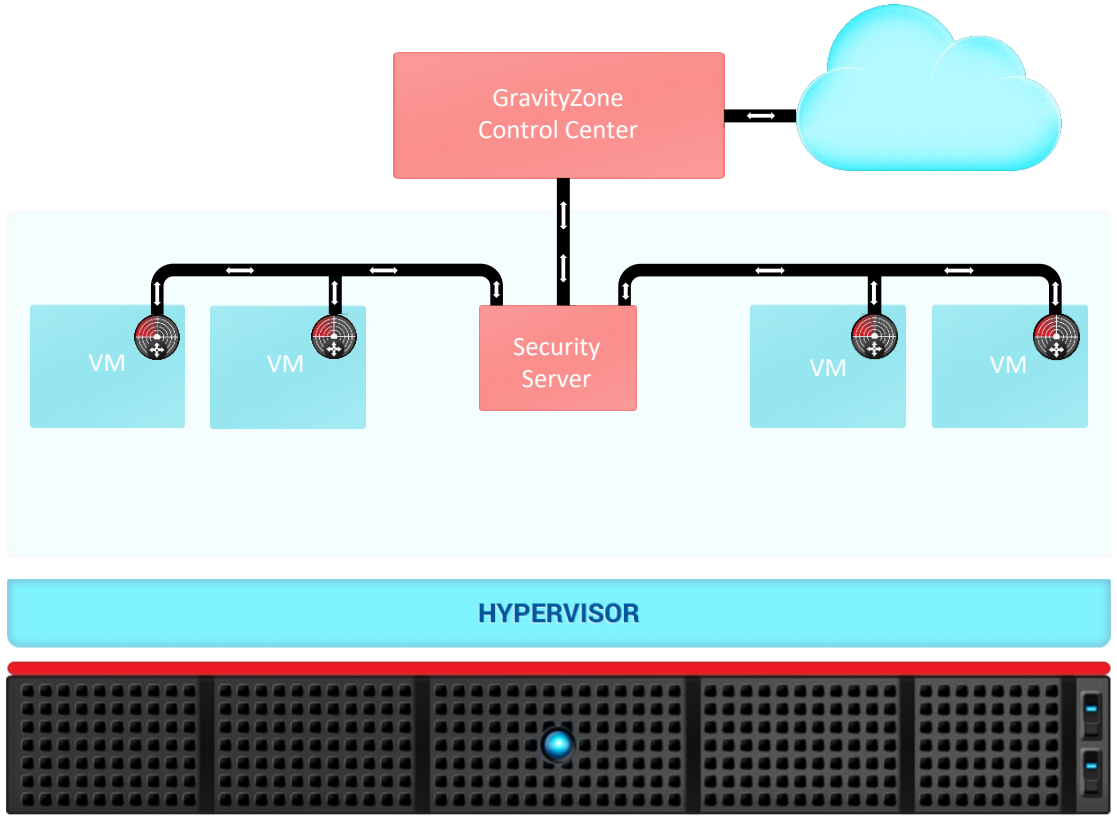
TRADIČNÍ PŘÍSTUP VS. PŘÍSTUP BITDEFENDERU



Bitdefender

SECURITY FOR VIRTUALIZED ENVIRONMENTS

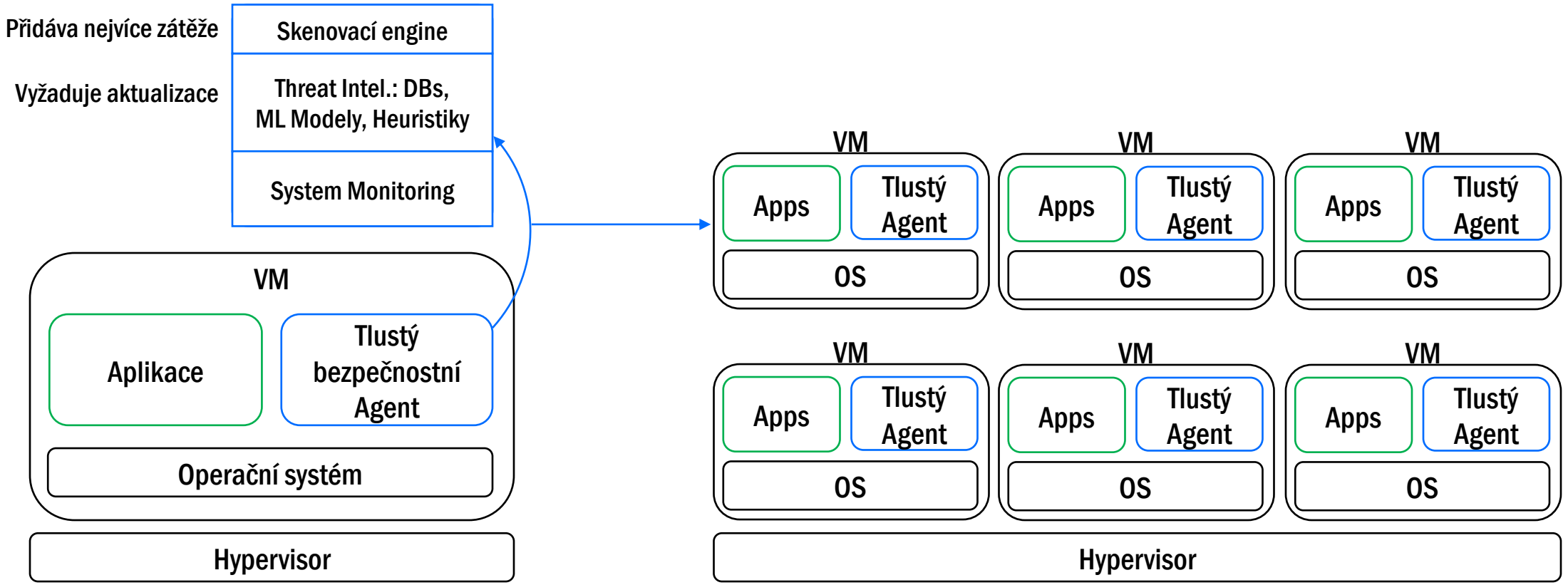
MULTIPLATFORMNÍ ARCHITEKTURA



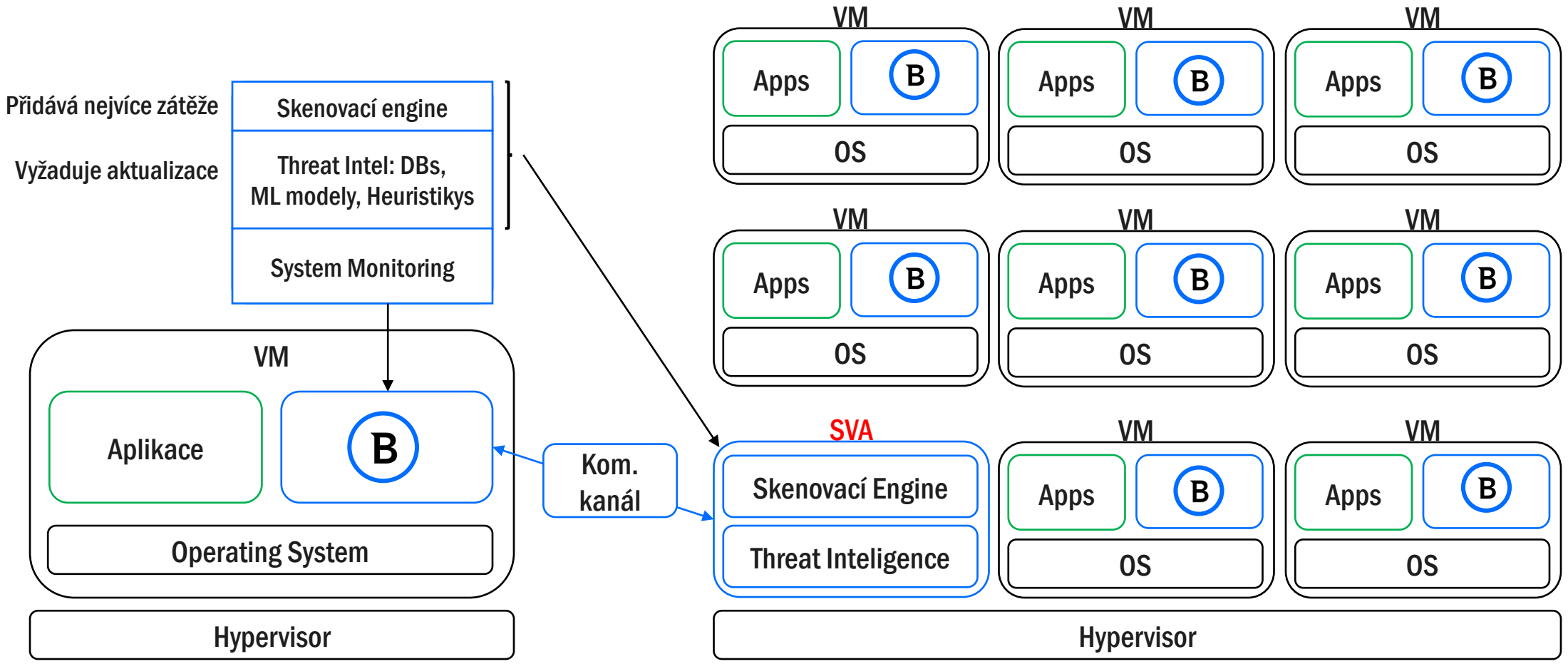
BEST s Centrálním Skenem

Bitdefender

Vliv klasického ANTIVIRU na výkon VS/VDI
Výzva: AKTUALIZACE Signatur snižují VÝKON

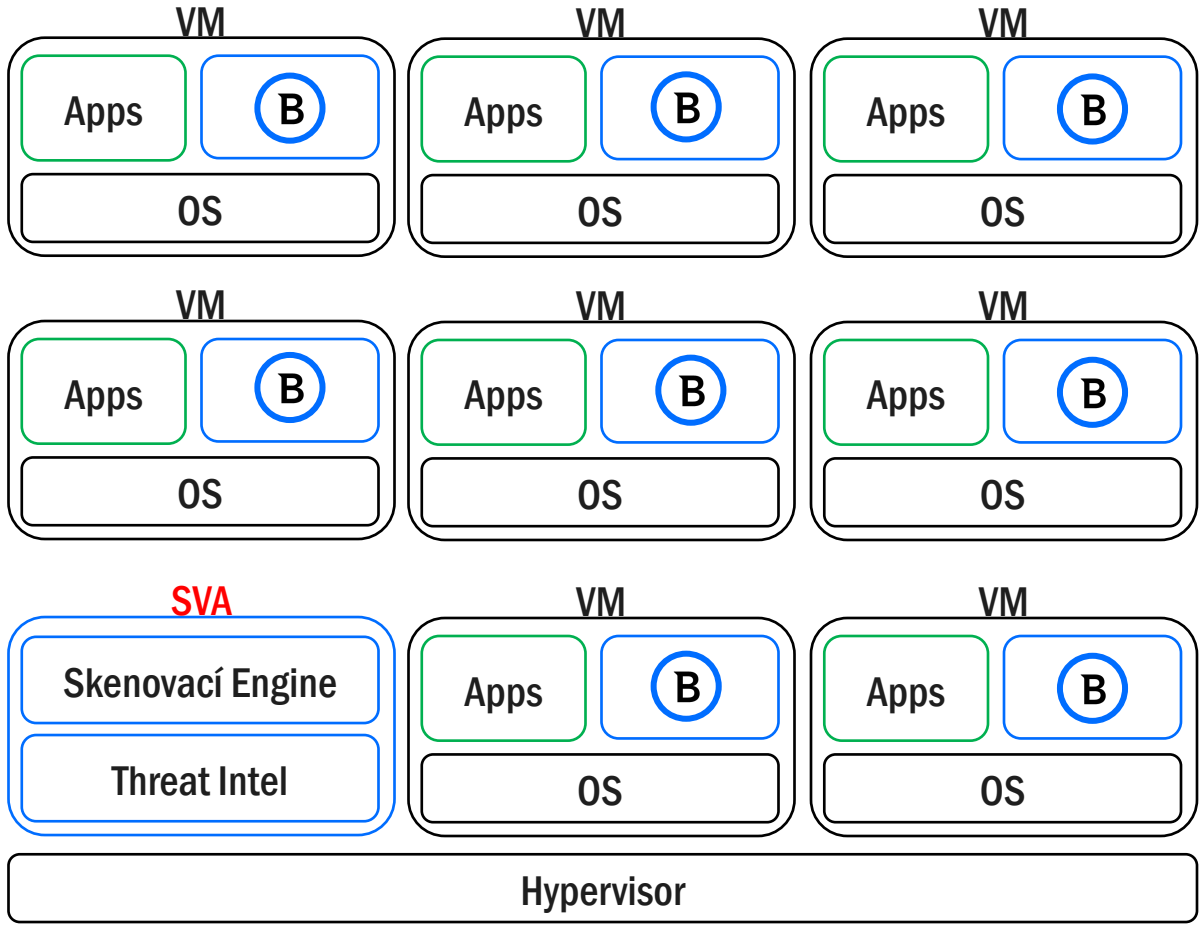


Přenesení skenů (Scan offloading)
Bitdefender řeší tento problém lehkými klienty



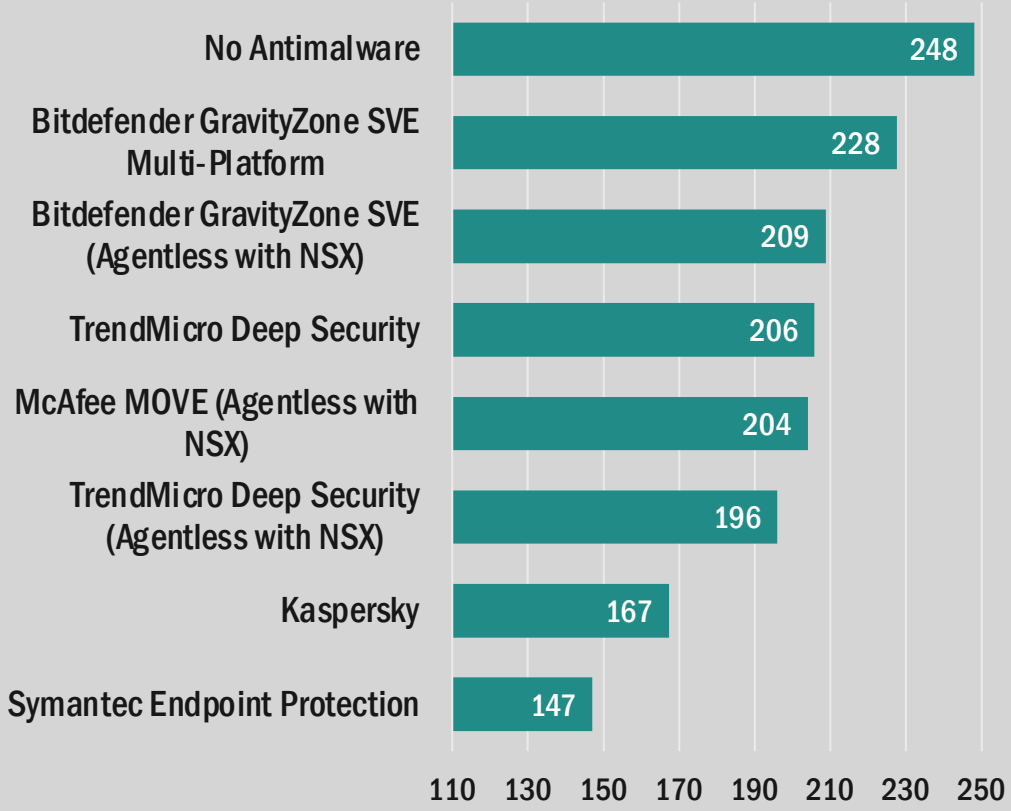
Přenesení skenů (Scan offloading) řeší tento problém

- Security Virtual Appliance (SVA) se aktualizuje 24/7
- klient potřebuje méně aktualizací
- Většina zátěže CPU / paměti / disku je přenesena na SVA
- Prostředí dosahuje vyšší VM-to-Host hustoty a lepšího výkonu



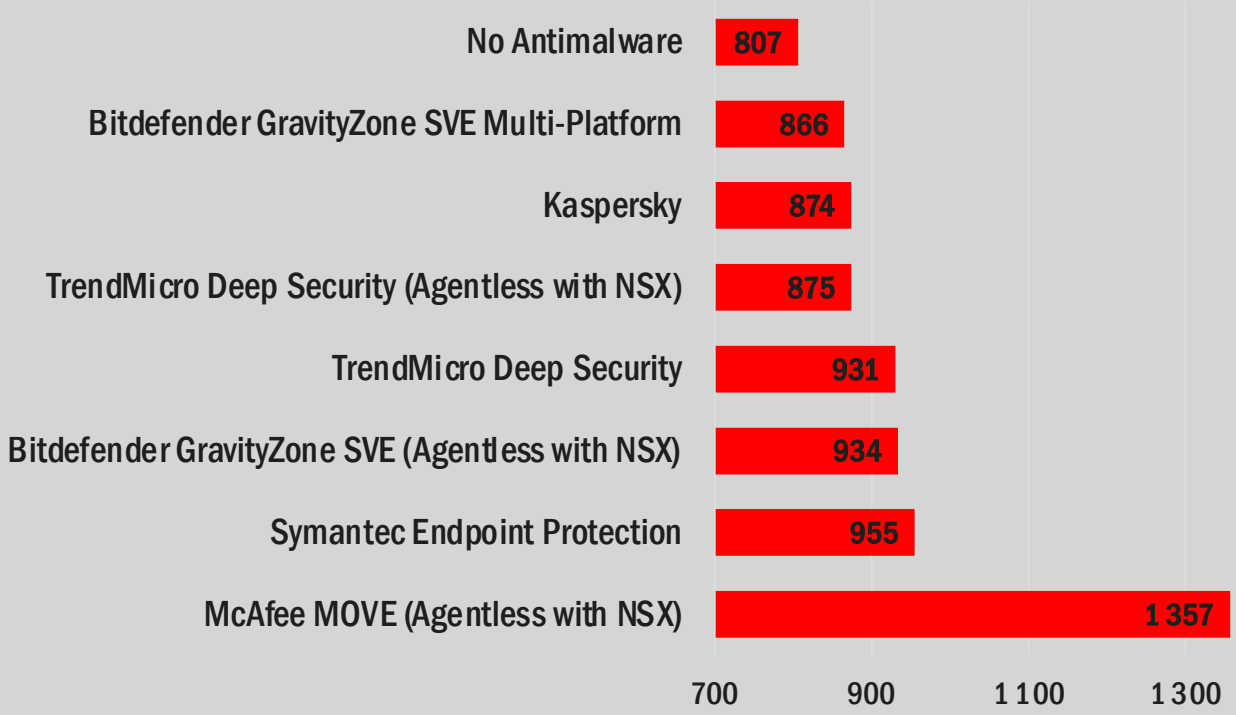
Snížení nároků na infrastrukturu = úspora nákladů

Maximální počet konkurentních VDI Sessions per Host

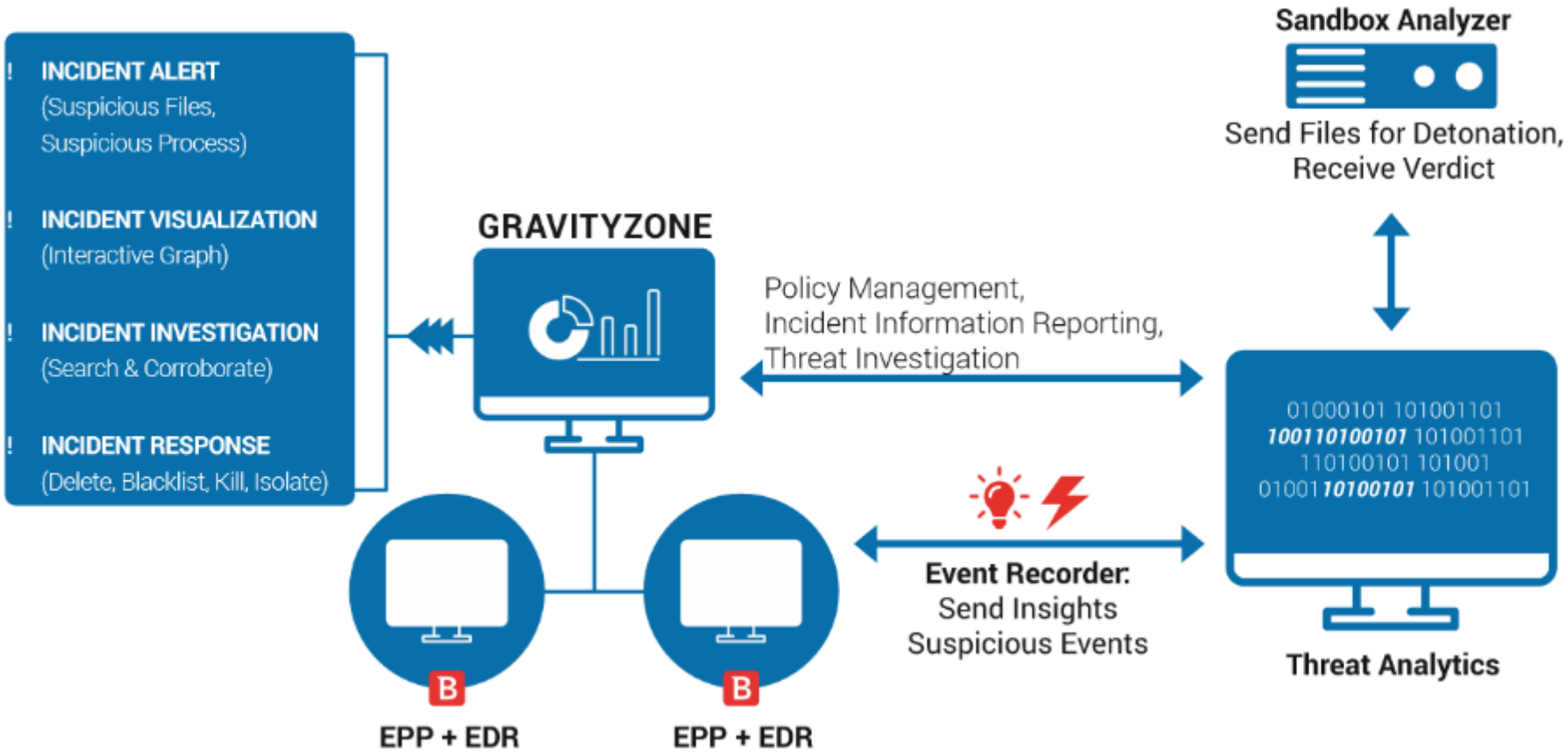


AŽ O 36% RYCHLEJŠÍ ODEZVA APLIKACÍ

Čas odpovědi nestresovaného systému (v Milliseconds)



XEDR – PRO Vizibilitu a RYCHLOU NÁPRAVU



Minimimalizuje čas vystavení se nákaze a zastavuje průlomy.

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

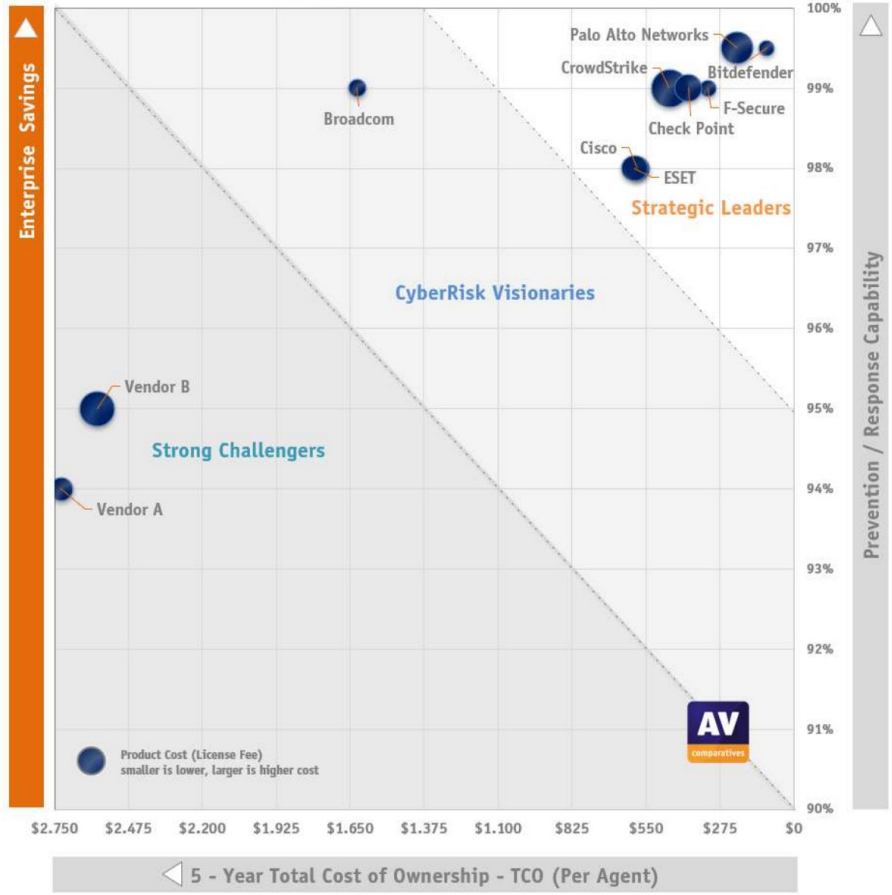
Snižuje požadavky na lidské zdroje a jejich znalosti a schopnosti provádět brzké detekce a nápravná opatření

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

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

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

Výstrahy s automatickou analýzou a tagováním dle metodologie MITRE

Bitdefender

Rozšířené Incidenty | Incidenty koncového bodu | Zjištěné Hrozby

OTEVŘENÉ INCIDENTY

Vysoký	0
Střední	2
Nízký	1

NEJVYŠŠÍ UPOZORNĚNÍ

SuspiciousSignedProcessExecution	2	SuspiciousTokenImpersonation	2
Attack.Bruteforce.RDP	2	ATC.Malicious	1
CopyWindowsComponentGeneric	2	WMILocalProcessCreated	1

NEJLEPŠÍ TECHNIKY

Command and Scripting Interpreter
Application Layer Protocol
Process Injection

Změnit status | Název výstrahy | Hledat náz

ID	Datum	Stav	Skóre závažnosti	Provedená akce	Koncový bod
Hledat...	Vybrat...	Vyberte...	Vyberte...	Vyberte...	Hledat...
#4	Aktualizováno před 22 minutami	Otevřít	65	Blokováno	IS4DEMOTARGET
#3	Aktualizováno před 31 minutami	Otevřít	64	Hlášeno	IS4DEMOTARGET
#1	Vytvořeno před 49 minutami	Otevřít	38	Blokováno	DESKTOP-RUBGCRI

3 položek | První strana | 1 z 1 | Poslední stránka | Zobrazit 20

#3
Hlášeno

DETEKCE

Skóre závažnosti: 64
Spouštěč Incidentu: 192.168.231.191

Attack.Bruteforce.RDP

INFO O ÚTOKU

Typy útoku: Other

Taktiky:
Privilege Escalation
Defense Evasion
Command And Control
Credential Access
Execution
Lateral Movement

ATT&CK techniky

Access Token Ma...	T1134.001 Token Impersonation/...
Application Layer...	T1071
Brute Force:	T1110.001 Password Guessing
Command and S...	T1059
Exploitation of R...	T1210
Masquerading:	T1036.005 Match Legitimate Na...
Non-Application ...	T1095
Process Injection:	T1055
Subvert Trust Co...	T1553.002 Code Signing

Zobrazit graf | Zobrazit události

Výstrahy s automatickou analýzou a tagováním dle metodologie MITRE

Bitdefender

Rozšířené Incidenty | Incidenty koncového bodu | Zjištěné Hrozby

OTEVŘENÉ INCIDENTY

Vysoký	0
Střední	2
Nízký	1

NEJVYŠŠÍ UPOZORNĚNÍ

SuspiciousSignedProcessExecution	2
CopyWindowsComponentGeneric	2
SuspiciousTokenImpersonation	2
Attack.Bruteforce.RDP	2
Gen:Variant.Bulz.693561	1
URL.Malicious	1

NEJLEPŠÍ TECHNIKY

Command and Scripting Interpreter
Application Layer Protocol
Abuse Elevation Control Mechanism

Změnit status | Název výstrahy | Hledat náz

ID	Datum	Stav	Skóre závažnosti	Provedená akce	Koncový bod
Hledat...	Vybrat...	Vyberte...	Vyberte...	Vyberte...	Hledat...
#4	Aktualizováno před 24 minutami	Otevřít	65	Blokováno	IS4DEMOTARGET
#3	Aktualizováno před 33 minutami	Otevřít	64	Hlášeno	IS4DEMOTARGET
#1	Vytvořeno před 50 minutami	Otevřít	38	Blokováno	DESKTOP-RUBGCRI

3 položek | První strana | 1 z 1 | Poslední stránka | Zobrazit 20

#4
Blokováno

INFO O ÚTOKU

Typy útoku: Malware, Ransomware, Potentially unwanted applica..., Other

Taktiky: Privilege Escalation, Defense Evasion, Command And Control, Collection, Persistence, Execution, Impact, Discovery

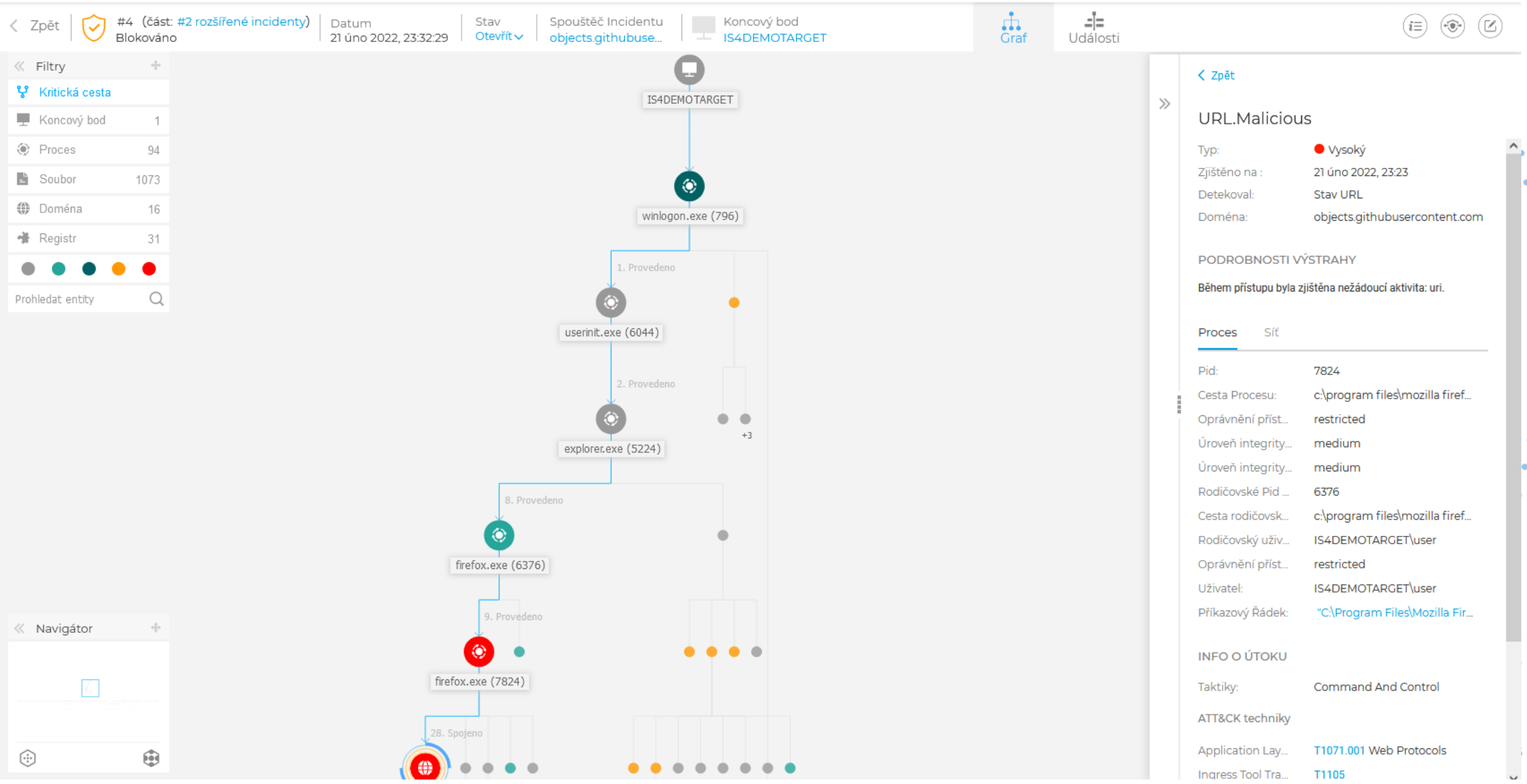
ATT&CK techniky

Abuse Elevation ...	T1548.002 Bypass User Access C...
Application Layer...	T1071.001 Web Protocols
Automated Colle...	T1119
Boot or Logon A...	T1547.001 Registry Run Keys / St...
Boot or Logon Ini...	T1037
Command and S...	T1059.003 Windows Command S...
Data Destruction:	T1485
Data Encrypted f...	T1486
Data Manipulatio...	T1565.001 Stored Data Manipula...
Data Staged:	T1074.001 Local Data Staging
File and Director...	T1083
Hijack Execution ...	T1574.010 Services File Permissio...

Zobrazit graf | Zobrazit události

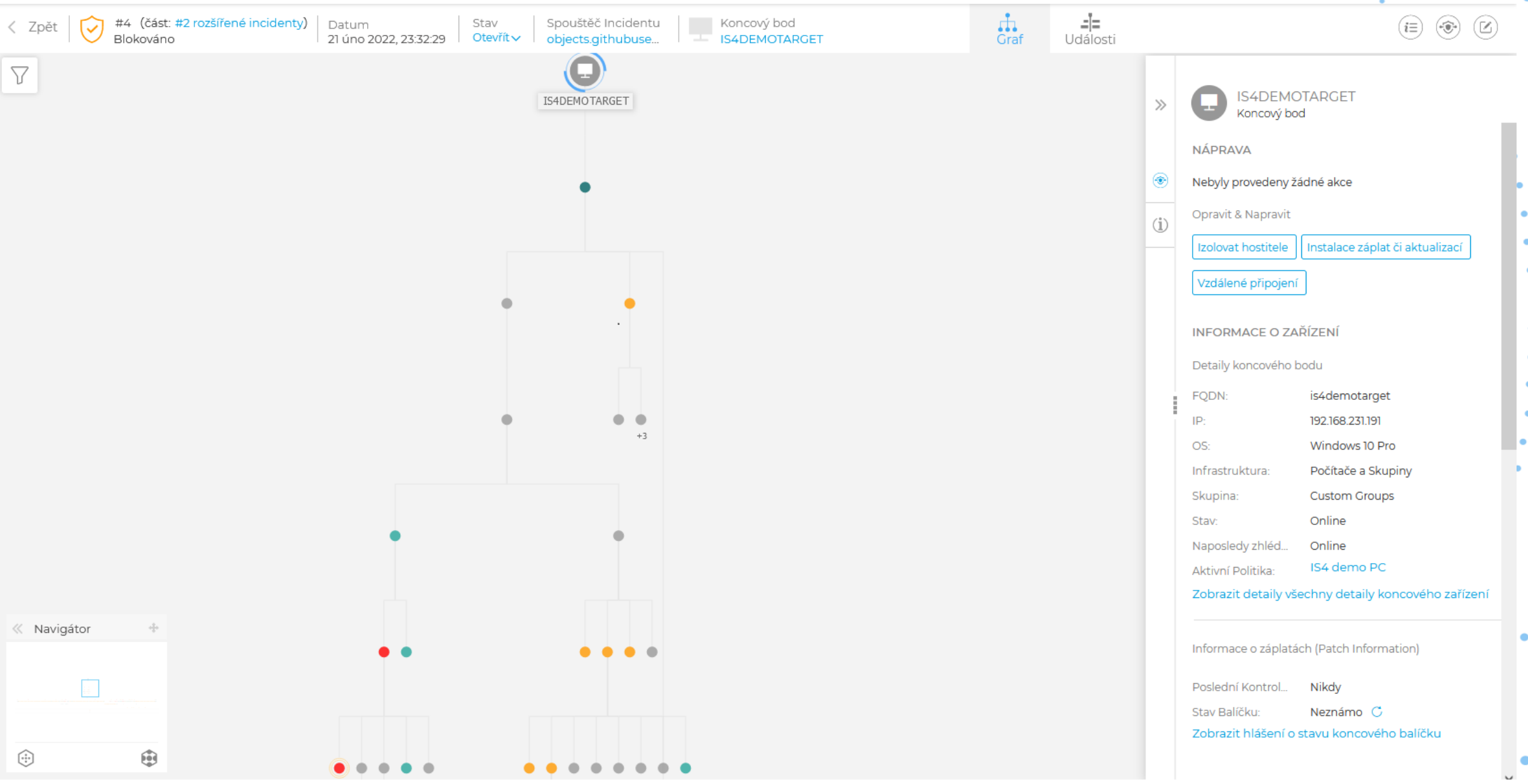
Detail bezpečnostního incidentu s kontextem díky integrovanému EDR

Bitdefender



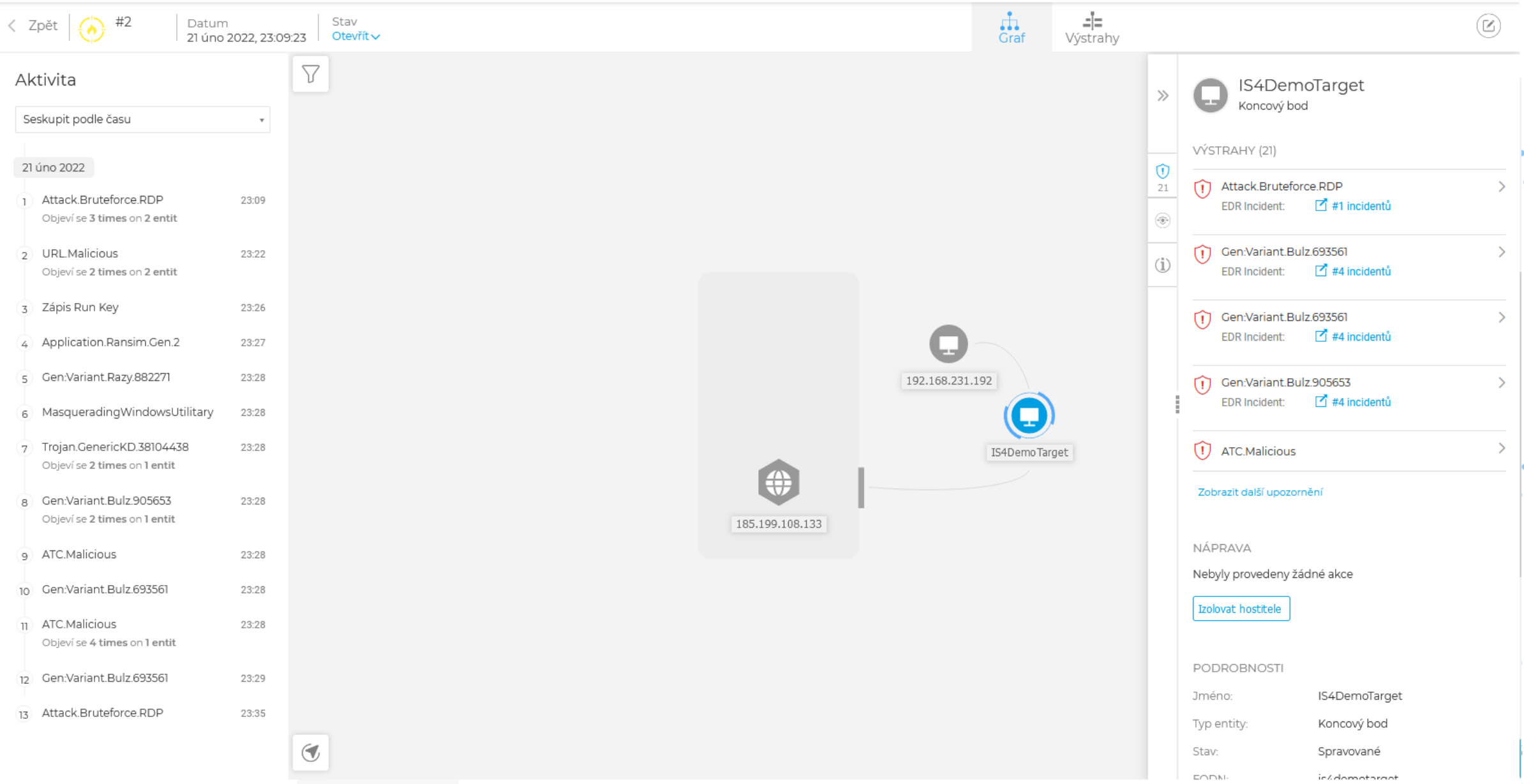
Možnost izolace koncového bodu ze sítě + možnost vzdáleného připojení

Bitdefender

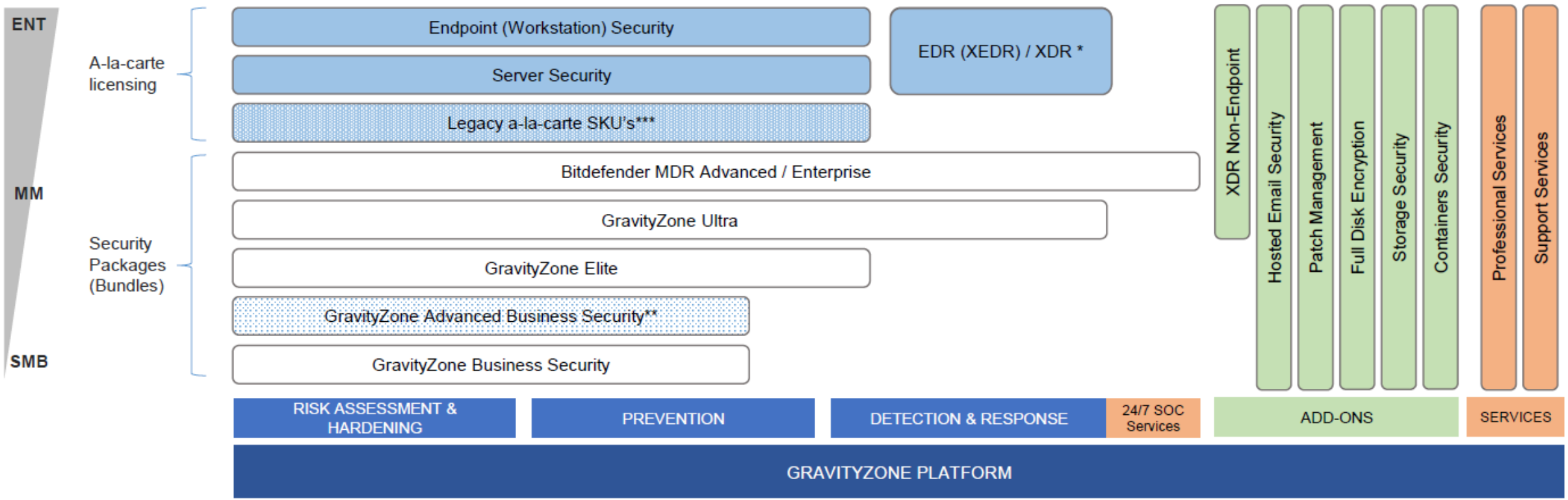


Rozšířený bezpečnostní incident – rychlý přehled průběhu útoku napříč sítí díky XDR

Bitdefender

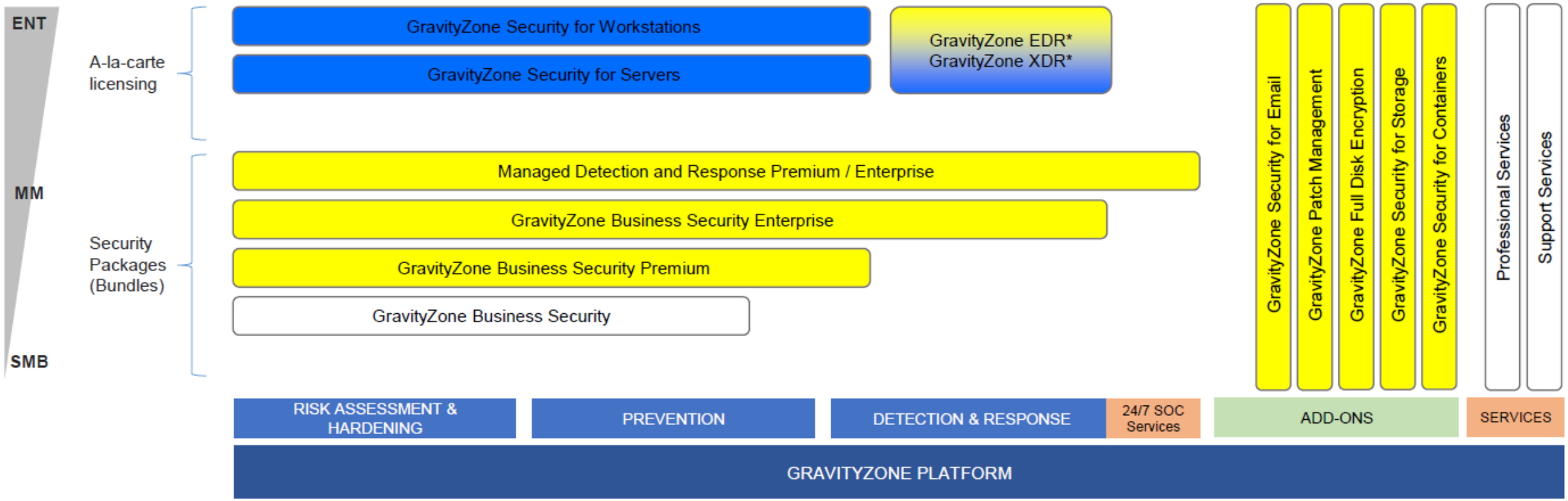


New Portfolio Structure



* XEDR and XDR available only for cloud deployments. Standard EDR available for on-premises deployments.
**GravityZone ABS available only for renewals, up to 3 years, starting March 31st, 2022. Not available for new customers.
***Legacy a-la-carte SKU's available only for renewals, up to 3 years, starting March 31st, 2022. Not available for new customers.

New Portfolio Naming



! *XEDR and XDR available only for cloud deployments. Standard EDR available for on-premises deployments.

Co to přinese zákazníkům / partnerům?

- Jednodušší licencování A LA CARTE

Licence pro **servery** nově nerozlišuje typ serverů
(fyzický / virtuální)

Licence pro **stanice** nově nerozlišuje její typ
(fyzická / virtuální)

+ přidání nových funkcí do těchto produktu
= NAVÝŠENÍ OCHRANY

Co to přinese zákazníkům / partnerům?

- Vrstvy ochrany navíc v A LA CARTE licencování

- Nově cloudová správa

- HyperDetect modul

- Cloudový sandbox

- Vizualizace incidentů

Co nabízíme Vašim zákazníkům ?

- **Zajímavé cenové podmínky včetně sektorových slev na TOP produkty na trhu**

- **Slevy pro přechod od konkurence -** V případě, že váš zákazník používá konkurenční placený produkt má nárok na CUPG slevu ze STD cen – Nutno doložit původní certifikát

- **Odkupné -** Pokud zákazník používá placený konkurenční produkt, který mu nevyhovuje a chce přejít na Bitdefender nabízíme odkup původních licencí

- **Možnost dokupu licencí –** Pokud zákazník potřebuje během platnosti licence dokoupit ochranu pro další zařízení. Může ji zakoupit pouze na zbývající měsíce do konce platnosti původnho certtifikátu. Všechny licence mu budou končit v jednu dobu.

- **Trial licence na odzkoušení až na 75 dní**

Bitdefender Spring Promo 2022

1. varianta: ODKUPNÉ

Zákazníkům, kteří používají placené konkurenční řešení, nabízíme odkupné v délce až 12 měsíců. **Akce se vztahuje pouze na nové zákazníky!**

Podmínky promoakce:

- Zákazníci mohou zakoupit produkty s cenovým zvýhodněním přechodu od konkurence na produkty (CUPG):
  - Bitdefender GravityZone Business Security
  - Bitdefender GravityZone Elite
  - **À La Carte produkty** (licencované na konkrétní zařízení)
  a
  - Bitdefender GravityZone Ultra + **EDR** bez zvýhodnění CUPG
- Při aplikaci odkupného je nutno dodat certifikát a fakturu původního řešení pro výpočet výše odkupného
- Částka za odkupné je maximálně do výše ceny produktu Bitdefender (nesmí být záporná)
- Navíc může zákazník získat 50% slevu ze standardních ceníkových cen na produkt Patch Management
- Navíc může zákazník získat 50% slevu ze standardních ceníkových cen na produkt Fulldisk Encryption
- Slevu na Patch Management a/nebo Fulldisk Encryption je možné využít pouze při společném nákupu (v jedné objednávce) s některým z hlavních produktů
- Promoakce se vztahuje na všechny **nové zákazníky** na licence o délce 1, 2 a 3 roky
- Promo akce platí pro zakázky do 1000 licencí. Nabídky nad 1000 licencí se řeší individuálně.
- Doba platnosti promoakce: do 30.5.2022

2. varianta

Určeno zákazníkům, kterým se 1. varianta s odkupným nevyplatí, a odkupné se tedy v tomto případě neřeší. **Akce se vztahuje pouze na nové zákazníky!**

Podmínky promoakce:

- Zákazník získá 50% slevu ze standardních ceníkových cen na produkt Bitdefender GravityZone Elite
- Navíc může zákazník získat 50% slevu ze standardních ceníkových cen na produkt Patch Management
- Navíc může zákazník získat 50% slevu ze standardních ceníkových cen na produkt Fulldisk Encryption
- Slevu na Patch Management a/nebo Fulldisk Encryption je možné využít pouze při společném nákupu (v jedné objednávce) s některým z hlavních produktů
- Promoakce na produkt Bitdefender GravityZone Elite se vztahuje se na všechny **nové komerční zákazníky**
- Akce na 50% slevu na Patch Management a Fulldisk Encryption se vztahuje na všechny komerční zákazníky, včetně zákazníků GOV, EDU, HEALTHCARE, na licence o délce 1, 2 a 3 roky
- Promo akce platí pro zakázky do 1000 licencí. Nabídky nad 1000 licencí se řeší individuálně.
- Doba platnosti promoakce: do 30.5.2022

Žijeme v propojeném světě, kde kyberútočníci neúnavně hledají, jak napáchat škody organizace čelí nepředvídatelným rizikům...

Bitdefender

je postaven pro odolnost.

S námi zvýšíte kyberodolnost vašich systémů a ochráníte data vašich zákazníků

Postavte své služby na GravityZone řešení.

Bitdefender

Váš partner pro kyberbezpečnost a kyberodolnost

Globální průkopník

- Založen 2001
- 1600+ employees
- Zákazníci ve 170 zemích světa

Finančně stabilní

- Rychlý růst
- Zisková společnost
- 45,000+ B2B zákazníků

Inovátor

- 50%+ pracovní síly v technickém oddělení, výzkumu a vývoji
- 111 vydaných patentů, 200+ před schválením
- Silný podporovatel open-source

Bitdefender®

BUILT FOR RESILIENCE

www.bitdefender.cz

Jordánská 391
19800 Praha 9

Technická podpora pro ČR/SK
Tel: +420 245 501 801

https://support.bitdef.cz/