Global Leader
In Cybersecurity

Opava

IS4 security
Feel Real Trust

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

Bitdefender®

ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI STATUTÁRNÍHO MĚSTA OPAVY

Jiří Hasala - Bitdefender CZ & SK - Channel manager

Ing. Pavel Meletzký, MBA - Město Opava - náměstek primátora

IS4 security
Feel Real Trust

Country Partner Bitdefender

Pro Bitdefender zajišťujeme kompletní servis v ČR a SK :

- **Před / Po prodejní technickou podporu v českém jazyce jak pro partnery, tak pro koncové zákazníky**

+420 245 501 801
https://support.bitdef.cz
helpdesk@bitdef.cz

- **Lokalizaci produktů B2C i B2B do češtiny**

- **Pravidelně školíme partnerskou síť**

www.bitdefender.cz

Bitdefender

30 miliard

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

400+

Hrozeb odhaleno každou minutu

1,6 miliardy $

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

32

Zveřejněno dešifrovacích nástrojů po útoku Ransomwarem

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+

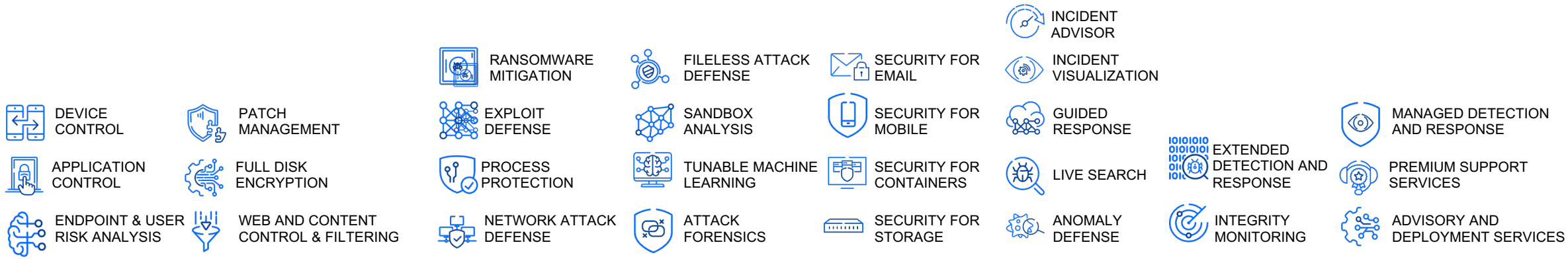
Zaměstnanců ve výzkumu a vývoji zaměřeného na cloud, nově vznikající technologie, IoT a strojové učení

285

Elitních security výzkumníků

GravityZone

Komplexní EDR/XDR řešení složené až z 38 vrstev ochrany. Podpořeno dnes již 487 patenty



PREVENTION | PROTECTION | DETECTION AND RESPONSE

GRAVITYZONE PLATFORM

ENDPOINT | CLOUD | NETWORK | MOBILE | IDENTITY | PRODUCTIVITY | IOT DEVICES

GravityZone XDR Sensors

Možnost rozšíření o další vrstvy ochrany pomocí různých XDR senzorů podle potřeb každé organizace

Identity Sensor

- Monitor, analyze, respond to events from AD, Azure AD
- Detects compromised accounts, Kerberos attacks, Brute Force and others. XDR responses include password reset or disabling accounts involved in suspicious activity

Productivity App Sensor

- Monitor, analyze, respond to O365, G Workspace events
- Detects disabled phishing protection, user creation, suspicious macros, spear phishing, exfiltration, Brute Force.
- Responses: delete suspicious emails, suspend accounts

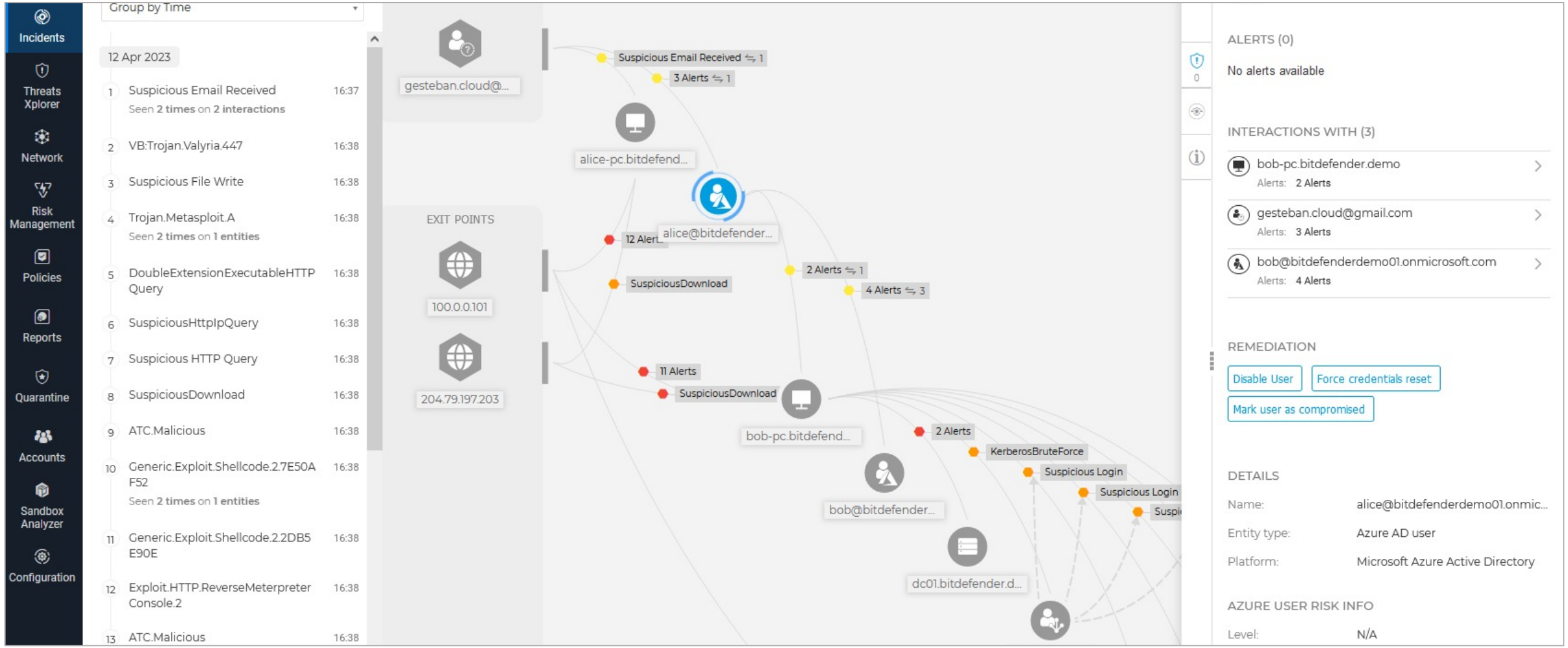
Network Sensor

- Monitor, analyze network traffic for signs of an attack
- Identifies lateral movement across the network, exfiltration, port scanning techniques, network originated Brute Force attacks

Cloud Sensor

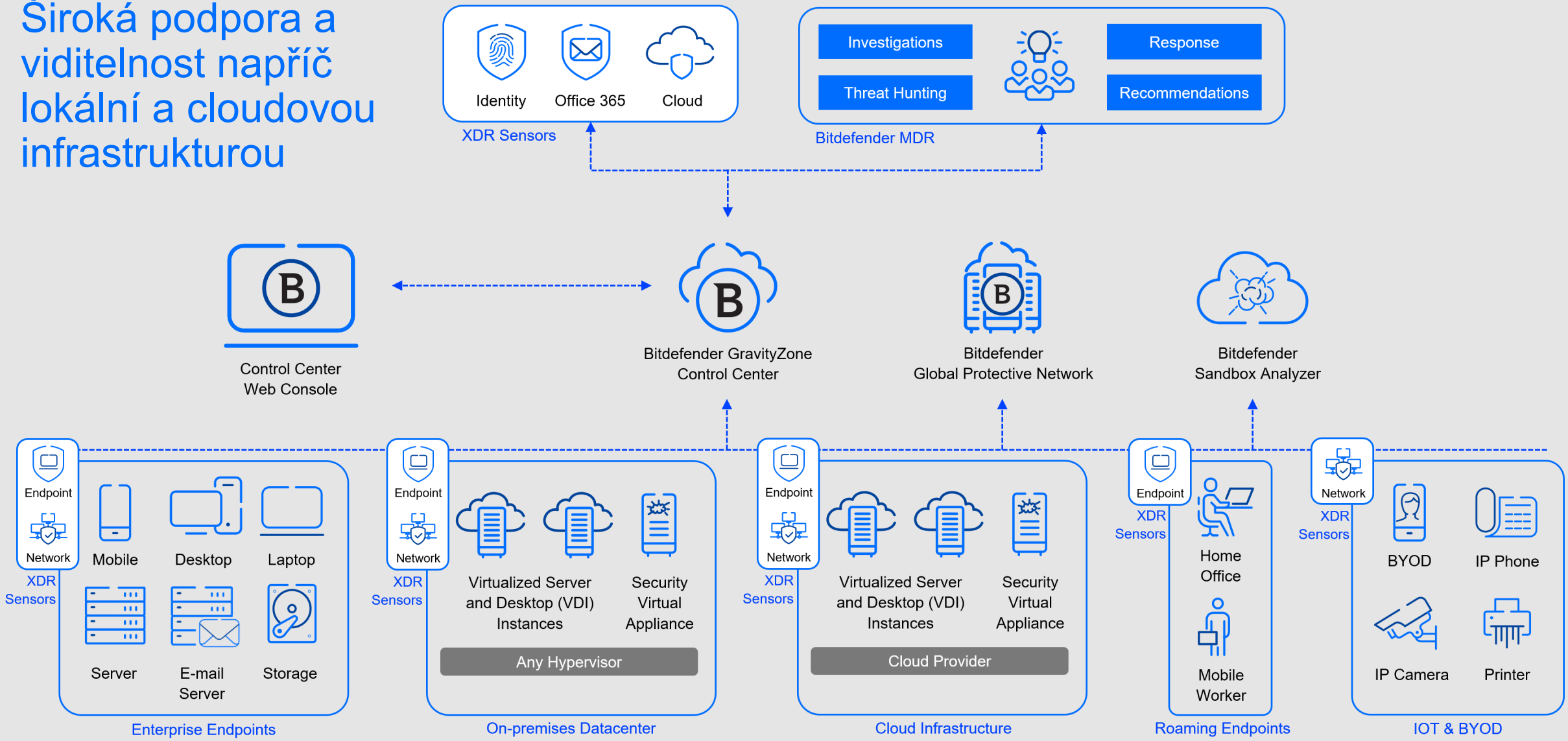
- Monitor, analyze security events from AWS, Azure, GCP
- Builds behavior baselines, reveals anomalies, use of Lambda function, encryption removal, monitoring services removal, reconnaissance, login failures, etc.

Automatická detekce incidentů , forenzní analýza útoků a korelace napříč celou organizací



Bitdefender

Široká podpora a viditelnost napříč lokální a cloudovou infrastrukturou



NAMED A CUSTOMERS' CHOICE FOR EMEA

In The 2023 Gartner Peer Insights™ Voice of the Customer for Endpoint Protection Platforms[1]

In the evaluation, **Bitdefender was also named a Strong Performer for EPP** overall, as well as by region for the **North America** segment and by company size for the **Midsize Enterprise & the Public Sector, Governments, Education**. Customers rated Bitdefender with a **94% Willingness to Recommend its EPP platform**.[2]

Gartner

Bitdefender is also named a Representative Vendor for the second consecutive time in The 2023 Gartner® Market Guide for Managed Detection and Response Services.

[1]Gartner, Gartner Peer Insights 'Voice of the Customer': for Endpoint Protection Platforms, Peer Contributors, 15 September 2023.
[2]Based on 91 ratings submitted in the Endpoint Protection Platforms market on Gartner Peer Insights as of 30 June 2023

"Amazing Product, Great Support, Getting Better Every Year."
IT Security and Risk Management, Manufacturing
Firm size: 500M - 1B USD

"Beautiful Central Management At Its Best. You Won't Be Let Down."
IT, Healthcare and Biotech
Firm size: 50M - 250M USD

"Improved Attack Identification And Patch Management Are Great."
IT Associate
Firm Size: 250M - 500M USD

"Bitdefender has been outstanding in the onboarding process and after sales of their products. The MDR solution is also really efficient and helped us a lot."
IT, Insurance
Firm Size: 250M - 500M USD

"Great Product, With Excellent Support Team."
IT Manager, Education
Firm Size: Gov't/PS/ED <5,000 Employees

Proven Cybersecurity Leadership

- CONSISTENTLY HIGH SECURITY EFFICACY

MITRE ENGENUITY | ATT&CK® Evaluations

Highest level of detection for all major steps in 2023 MITRE Engenuity ATT&CK Enterprise Evaluations

First in AV-Comparatives enterprise tests, far more than any vendor

AV-Comparatives 2023

Highest Overall Performer in AV-Comparatives Endpoint Prevention & Response Report

35 consecutives VBSpam + awards

Industry and Peer Recognitions

FORRESTER®

Named a Leader in The Forrester Wave™: Endpoint Security, Q4 2023

Named Among Notable Vendors in the Managed Detection And Response Services Landscape In Europe, Q3 2023

Gartner

Named a Visionary in the 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

Named a Representative Vendor for the second consecutive time in the 2023 Gartner® Market Guide for Managed Detection & Response Services.

Named a Customers' Choice for EMEA in the 2023 Gartner Peer Insights™ for Voice of the Customer for Endpoint Protection Platforms

CRN Partner Program Guide Award for MDR 2023

FORRESTER®
WAVE LEADER 2023
Endpoint Security

NAMED A LEADER

In The Forrester Wave™: Endpoint Security, Q4 2023

"Bitdefender differentiates with its aggressive prevention-first mindset."

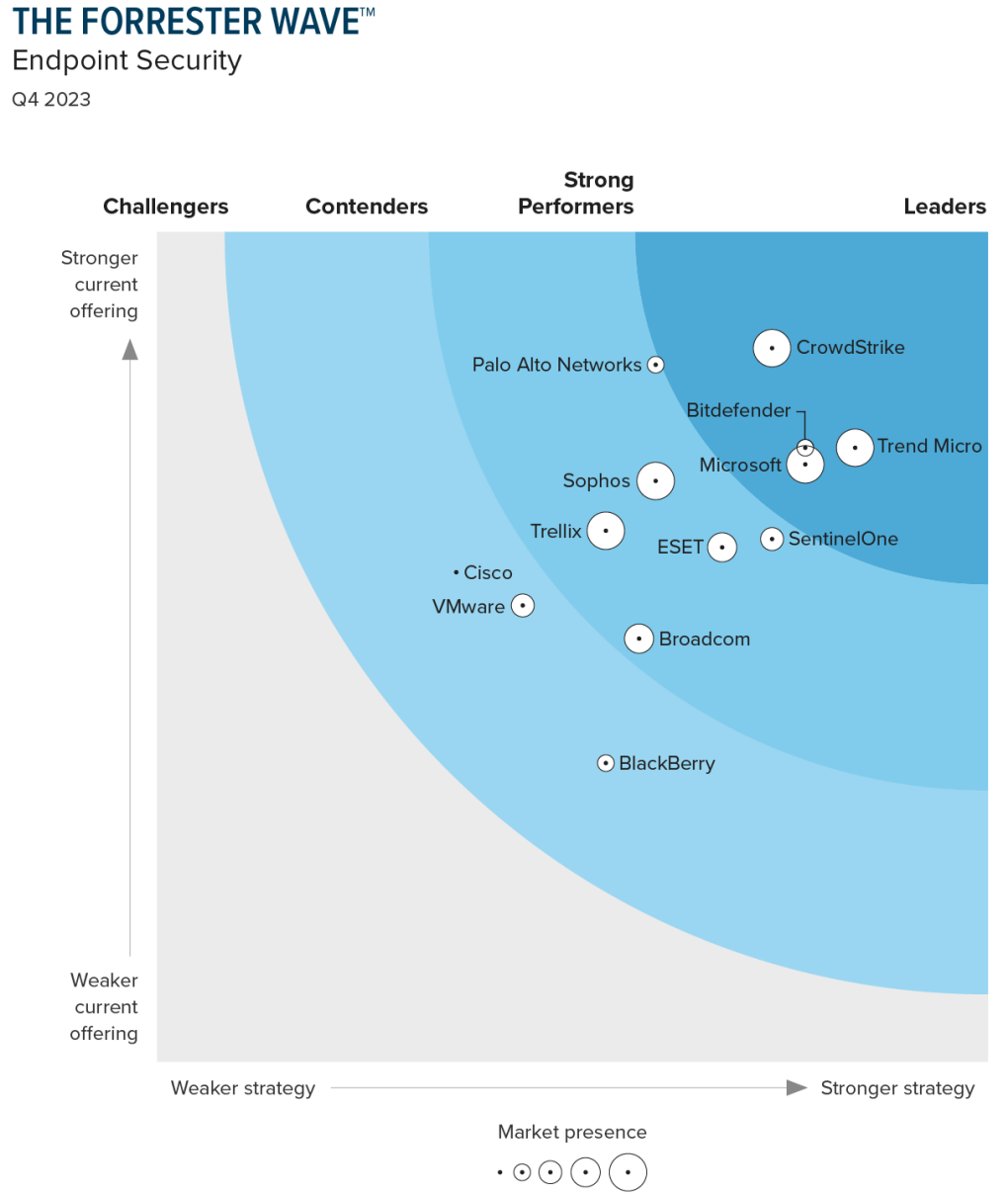
Maximum Scores Possible in **Identity Protection, Malware Prevention, Exploit Prevention**, **Attack Remediation, Vulnerability Remediation, Patching Remediation**, **Network Threat Detection, and Innovation, Adoption, Pricing Flexibility & Transparency**

FORRESTER®

Bitdefender is also Named a Notable MDR Provider in The Forrester MDR Services Landscape in Europe, Q3 2023

FIGURE 1

Forrester Wave™: Endpoint Security, Q4 2023



KAPITOLA 04

PROČ SPOLUPRACOVAT S IS4 SECURITY

Ve spolupráci s našimi partnery zajistíme celý proces implementace kybernetické bezpečnosti do vaší společnosti, počínaje auditními a analytickými službami, přes návrh a plán implementace, zajištění financování, až po realizaci a následné monitorování.

PROCES ZAJIŠTĚNÍ SOULADU SE SMĚRNICÍ NIS2 A NOVÝM ZOKB:

AUDITNÍ A ANALYTICKÉ SLUŽBY

Než se pustíte do akce, je potřeba vědět, odkud vycházíte! Počáteční audity odhalí, jak daleko je vaše firma od shody s NIS2.

NÁVRH A PLÁN IMPLEMENTACE

Na základě analýzy vám navrhneme individuální řešení a plán implementace. Každé řešení je šité na míru vašim specifickým požadavkům a situaci.

ZAJIŠTĚNÍ FINANCOVÁNÍ

Zajistíme financování kybernetické bezpečnosti a digitální transformaci vaší firmy. Dotace až 60% (průběžná i ex post)

REALIZACE A MONITOROVÁNÍ

Po schválení plánu kybernetické bezpečnosti nastává fáze realizace. V ní se navržená řešení převedou do praxe

JAK ŘEŠENÍ Z PORTFOLIA IS4 SECURITY POMŮŽE SE SPLNĚNÍM POŽADAVKŮ NIS2?

Firemní koncept „**Vendor Representative Company**" umožňuje kombinovat nejlepší technologie jedním dodavatelem. Řešení kybernetické bezpečnosti tak můžete pokrýt řešeními, které se vzájemně doplňují.

Bitdefender endian sectona

ANALÝZA RIZIK A BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

Analýza rizik a zajištění bezpečnosti informačních systémů je kritické pro ochranu proti kybernetickým hrozbám. Identifikuje a hodnotí možné nebezpečí, zranitelnosti a jejich dopad. Na základě této analýzy lze navrhnout a implementovat opatření pro prevenci, detekci a reakci na útoky. To zabezpečuje ochranu dat, zachování důvěrnosti a nepřetržitou dostupnost systémů.

Bitdefender.

Bitdefender® GravityZone Risk Management

Umožňuje bezpečnostním týmům vyhledávat a identifikovat rizika spojená s chybnou konfigurací operačních systémů, se zranitelnými aplikacemi a nebezpečným chováním uživatelů. Identifikace rizik je přímo šitá na míru odvětví dané organizace.

VÍCE INFORMACÍ →

Bitdefender.

Bitdefender® GravityZone Patch Management

Posílení zabezpečení a snížení rizika potenciálních zranitelností software, operačních systémů a aplikací, pomocí automatizované správy záplat. S modulem GravityZone Patch Management můžete udržovat své operační systémy a softwarové aplikace aktuální, a využívat komplexní přehled o stavu záplat v celé instalační základně systémů Windows, Linux a MacOS. Modul automatizované správy záplat poskytuje aktualizace pro celou síť pracovních stanic, fyzických serverů nebo virtuálních serverů organizace.

VÍCE INFORMACÍ →

ŘEŠENÍ INCIDENTŮ A ZAJIŠTĚNÍ KONTINUITY PROVOZU

Efektivní správa strukturovaných incidentů má potenciál minimalizovat následky kybernetických útoků a zabezpečit integritu dat a systémů ve vaší organizaci. Klíčovým faktorem pro úspěšnou manipulaci s incidenty je rozpoznání samotného útoku.

Bitdefender.

Bitdefender® GravityZone Business Security Enterprise

Dosahujte bezkonkurenční rychlosti a efektivity detekce a reakce napříč koncovými body, identitami, sítěmi, produktivními aplikacemi, cloudy a mobilními zařízeními. Přináší pokročilou ochrana před hrozbami, potlačení útoku prostřednictvím automatické, a lidmi řízené, reakce. Sjednocuje technologie EDR/XDR, Risk Analytics a Hardening do jedné konzole s jediným agentem, a využívá 30 vrstev pokročilých technik k úspěšnému zastavení útoků v celém životním cyklu hrozeb, od prvního kontaktu, přes případné proniknutí, persistenci, až po škodlivé aktivity. Funkce Bitdefender Ransomware Remediation blokuje útoky ransomwaru a automaticky obnovuje obsah zašifrovaných souborů bez nutnosti platit výkupné.

VÍCE INFORMACÍ →

endian

Endian® UTM & Bezpečnostní gatewaye Endian IoT

Bezpečnostní gatewaye Endian IoT jsou vybaveny několika bezpečnostními funkcemi, které dokáží odhalit a zastavit kybernetické útoky: Hloubková kontrola paketů (DPI) analyzuje datové pakety, odesílané přes síť. Na rozdíl od tradičních metod analýzy, které se zaměřují pouze na metadata, DPI provádí analýzu až na uživatelskou úroveň a identifikuje více než 300 protokolů IT/OT. a 2000 aplikací. To umožňuje zjistit běžný stav sítě. Pokud se v síti vyskytne anomálie provozu, je odhalena pomocí systému detekce narušení (IDS). Pokud se jedná o útok, použije se systém prevence narušení (IPS - Intrusion Prevention System) zasáhne, aby jej zastavil.

VÍCE INFORMACÍ →

BITDEFENDER BUSINESS SECURITY ENTERPRISE

STAV PŘED

- Symantec Endpoint Protection (základní antivirová ochrana koncových stanic a serverů)
- Symantec Brightmail (antispam)
- Webmarshal (kontrola webového provozu)
- Nasazeno na 470 stanicích a serverech

! Správa 3 samostaných konzolí = náročnost správy

NAŠE HLAVNÍ POŽADAVKY

- **Antimalwarová ochrana včetně EDR/XDR**

  Potřebovali jsem povýšit zabezpečení koncových bodů a serverů proti cíleným útokům, ramsomware, phishingu atd.
- **Patch management**

  Mezi naše požadavky patřilo také, vyřešit správu aktualizací a záplat. A to pokud možno efektivně a automatizovaně.
- **Šifrování dat na NTB**

  Potřeba byla také na vyřešení šifrování dat na NTB, které opouští úřad a při jejich ztrátě, krádeži hrozí únik citlivých informací
- **Správa a monitoring flash disků a dalších USB zařízení**

NASAZENÍ

- Produktem **Bitdefender GravityZone** jsme nahradili všechny tři výše zmíněné systémy.

- **Vše spravujeme v jedné konzoli**
  - včetně automatizované správy a implementací patchů
  - ochrany virtualizace proti bezsouborovým útokům

+ jsme získali i **analýzu rizik** z hlediska chování uživatelů a **přehled o miskonfiguracích OS**

- **Bitdefender GravityZone**

  Zvolil jsme nasazení s cloudovou správou, tudíž jsme instalovali pouze server na propojení s AD, a dále bezpečnostní server sloužící pro skenování virtualizace tak, aby nedocházelo k zatížení serverů

- provedli jsme registrace licence pro vytvoření administrátorské konzoly.
- instalace serveru na propojení s AD a následné načtení koncových stanic a serverů do konzole

- V konzoli jsme spolu s dodavatelem vytvořily instalační balíčky pro koncové stanice, servery.

  V rámci instalačních balíčků bylo nastaveno „odinstalovat stávající bezpečnostní řešení“, což nám umožnilo při instalaci nového klienta automaticky odebrat předchozího klienta.

- Instalace proběhla hladce

90 na 10

Samotná instalace proběhla z 90% bez problémů,

ve zbývajících 10% byla nutná ruční odinstalace původního klienta, restart a následná instalace nového klienta.

ZKUŠENOSTI

Konzole je v cloudu a není třeba instalace a aktualizace lokálních serverů, a vše se ovládá z jedné konzoly:

+ možnost distribuce rozdílných politik na stanice a servery (konfigurační profily)
+ jednoduchá správa v jedné konzoli
+ ochrana virtualizace i proti bezsouborovým utokům
+ skenování HTTPS provozu
+ sandbox analýza v reálném čase
+ možnost zapnutí FW
+ patch managament (záplaty Microsoftu plus dalších aplikací třetích stran)

NASAZENÍ A ZKUŠENOSTI

+ EDR
+ široká možnost reportů
+ ochrana pošty proti phishingu
+ možnost zapnutí FW

- jednodušší antispam
- nelze jednoduše zjistit z jakého důvodu byla vyhodnocena zpráva jako SPAM (nutno kontrolovat logů)

PLÁNY

- Rozšíření stávající ochrany KB o SIEM
- Outsoursování fyzické detekce – služby SOC
- Služba SOC musí napojit všechny stávající systémy ochrany, včetně EDR systému Bitdefender
- Rozšíření o další XDR senzory

ZÁVĚR

V letošním roce Opava slaví!!!
Město Opava v letošním roce slaví 800 let od udělení městských práv Přemyslem Otakarem I.
O tom napovídají i naše hashtagy #opavaslavífest a #perlíme.
A my chceme slavit, nechceme řešit kybernetickou bezpečnost a hackerské útoky. Proto jsme rádi, že za nás pracují systémy jako právě

BITDEFENDER GRAVITYZONE BUSINESS SECURITY ENTERPRISE

DĚKUJI ZA POZORNOST

OPAVA 800

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/