Bitdefender

Bitdefender GravityZone XDR

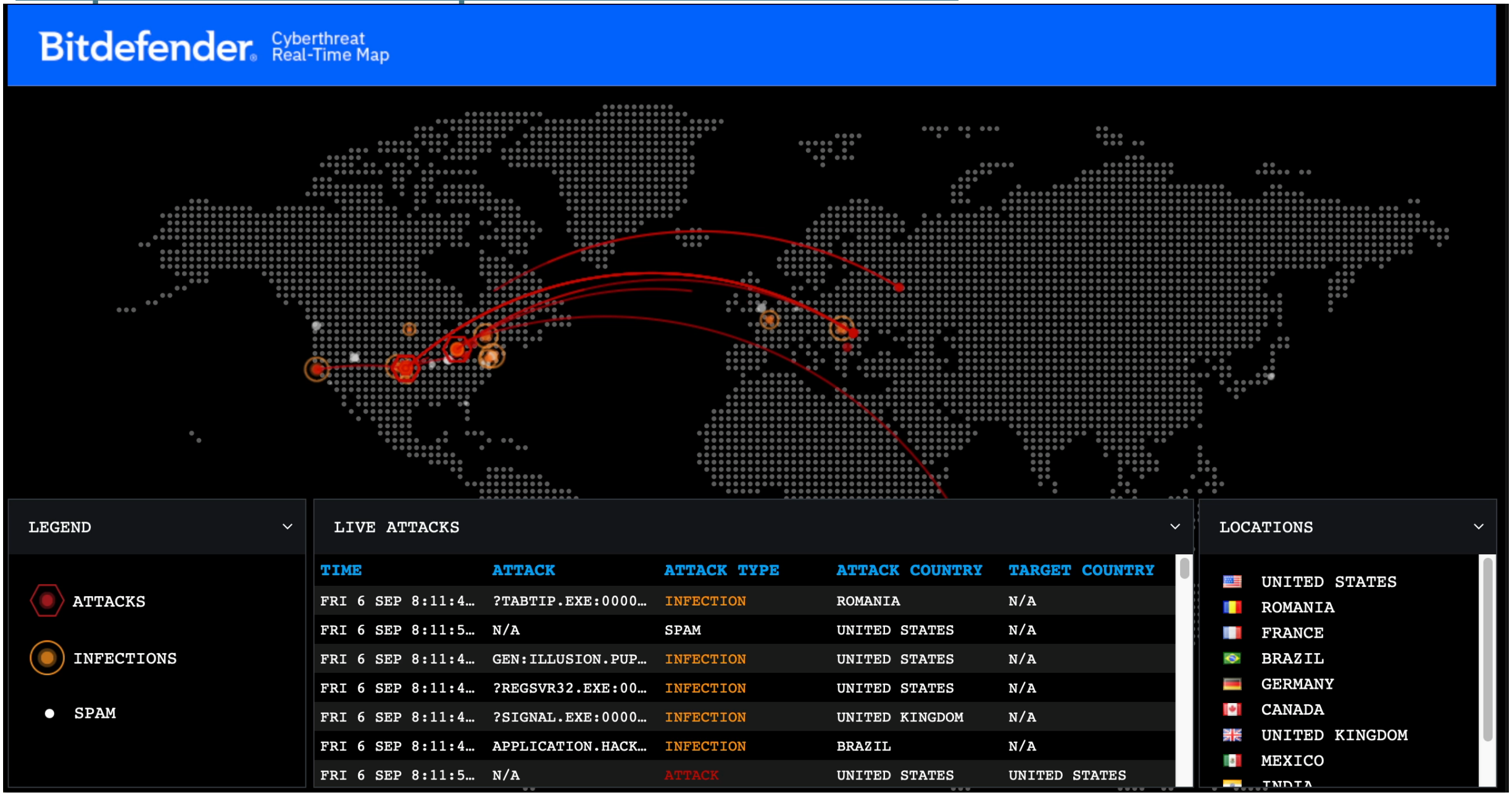
Bezpečnost šitá na míru každému uživateli

poznejte Bitdefender XDR , adaptivní AI based hardening PHASR, Compliance Manager a další novinky z Bitdefender LABS

René Pospíšil – Bitdefender Country Manager CZ/SK

IS4 security
Feel Real Trust

https://threatmap.bitdefender.com/



Vaše IT infrastruktura je jako budova plná hodnotných asetů

V minulosti se útočníci chovali jako nápadní pachatelé a lupiči, kteří lámali zámky a vnášeli především svůj vlastně vytvořený útočný kód dovnitř vaší budovy (například trojské koně a jiný malware)

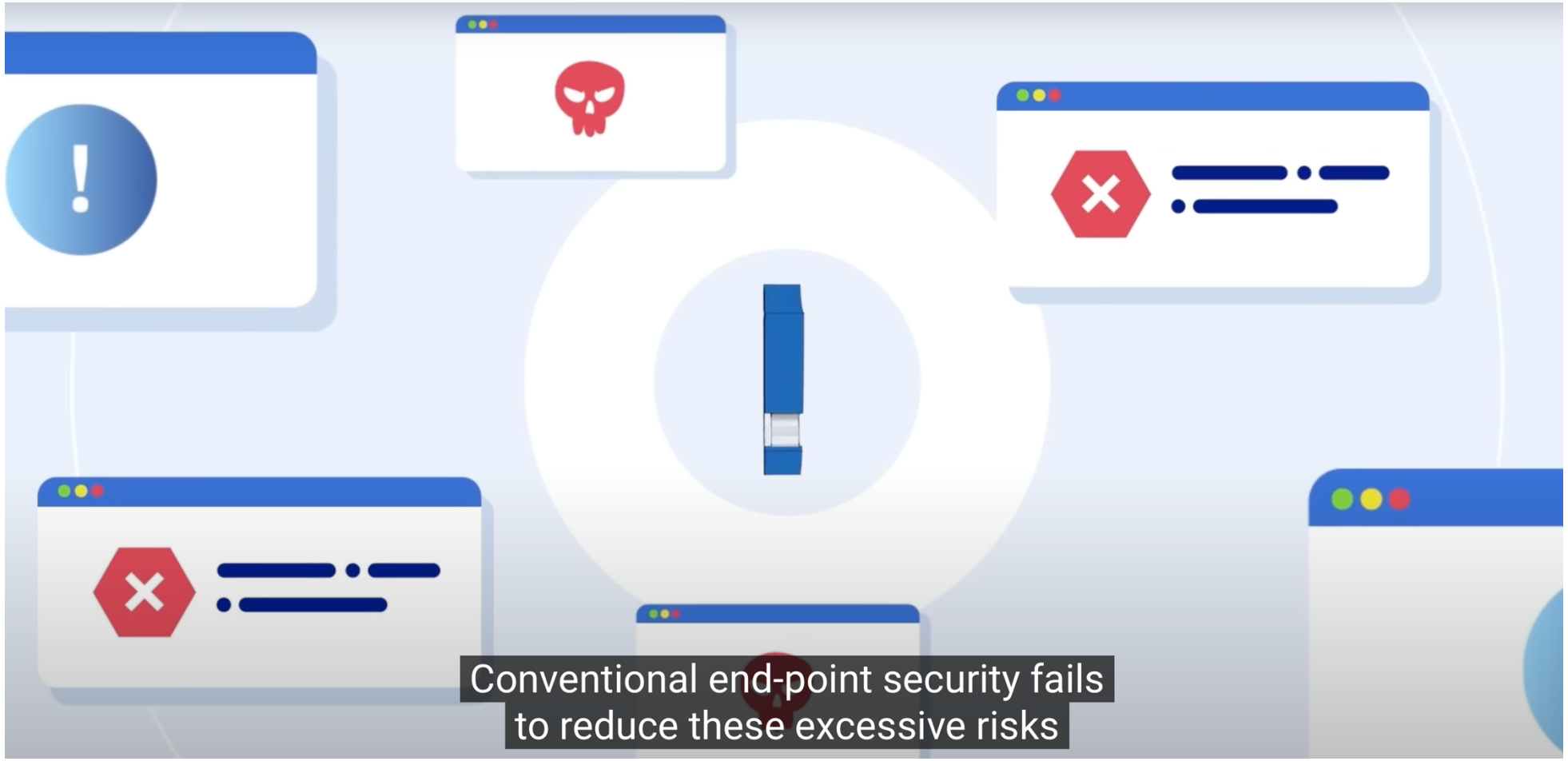
Jejich podezdřelé nástroje a chování tak spouštěly POPLACH ...

Dnes se útočnící především nevloupávají ale logují do vaší infrastruktury…
(ukradené přístupy , sociální inženýrství, z nechráněných zařízení atd.)

Využívají legitimní nástroje OS a běžné aplikace správy IT
84% útoků probíhá dnes za pomocí těchto nástrojů … (LOTL)

Až 95% útočné plochy tvoří tyto běžné nástroje pro IT správu ...

Běžná řešení ochrany koncových bodů nedokážou snížit tyto extrémní rizika.
Obtížně řešitelné dilema co povolit komu a kdy za jakých podmínek ...
Jak zaručit chod IT ? Komplikované vyjímky a pravidla jsou neudržitelnými...



Z tohoto důvodu mnoho institucí a firem se dnes spoléhá většinou na EDR/XDR řešení (detekci & odezvu řešením incidentu po průlomu …)

Bitdefender PHASR je jako chytrý Bodyguard který ví kdy a proč je konkrétní nástroj potřeba pro jakého uživatele v jaké situaci ...

PHASR je schopen díky pokročilké AI analýze podezřelého chování a s tím spojené korelaci potenciálních hrozeb řešit vše průběžně s ohledem na dynamické potřeby uživatele s ohledem na možné vektory útoků a to zcela individuálně a bezúdržbově.

Co je to tedy PHASR a k čemu slouží?

- Jedná se o nový produkt a technologii vyvinutou společnostíBitdefender.

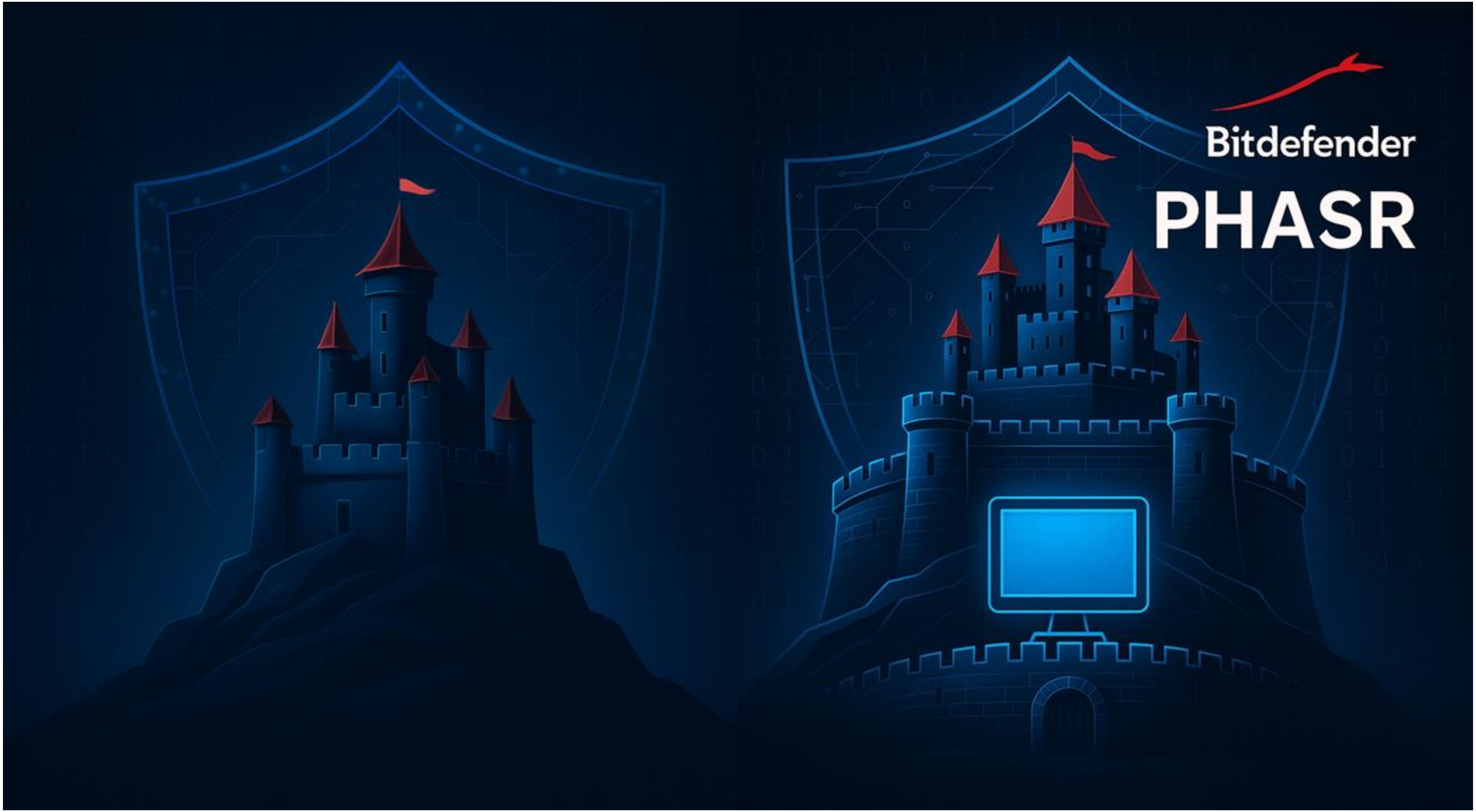
Zkratka pojmů **P**roactive **H**ardening and **A**ttack **S**urface **R**eduction

- volně přeloženo mými slovy

(Proaktivní vytvrzování a razantní snížení útočné plochy “útočníkovi”)

- Co se tedy skrývá pod těmito pojmy a co mně nebo mým zákazníkům může tento produkt přinést?

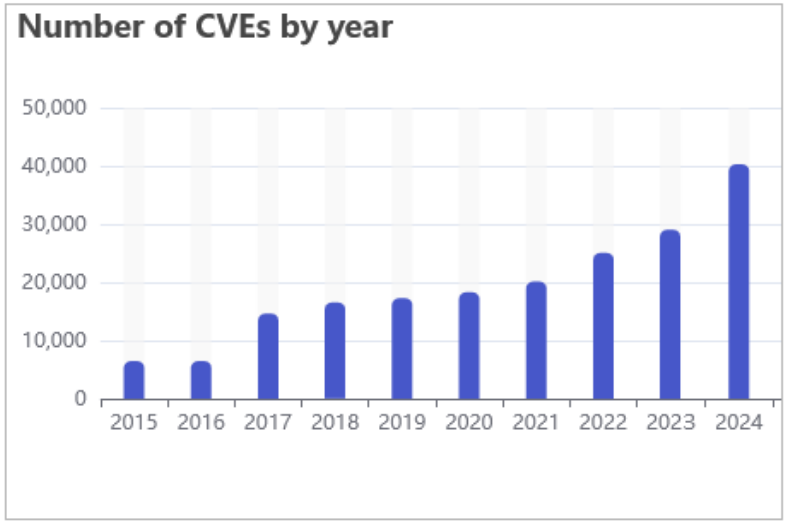
- Na tuto základní otázku se pokusíme odpovědět společně na konci této prezentace – společně s dalšími dotazy. Nyní je potřeba pochopit podstatu tohoto produktu a jak vlastně funguje. Začneme pojmy..


Bitdefender
PHASR

Bitdefender

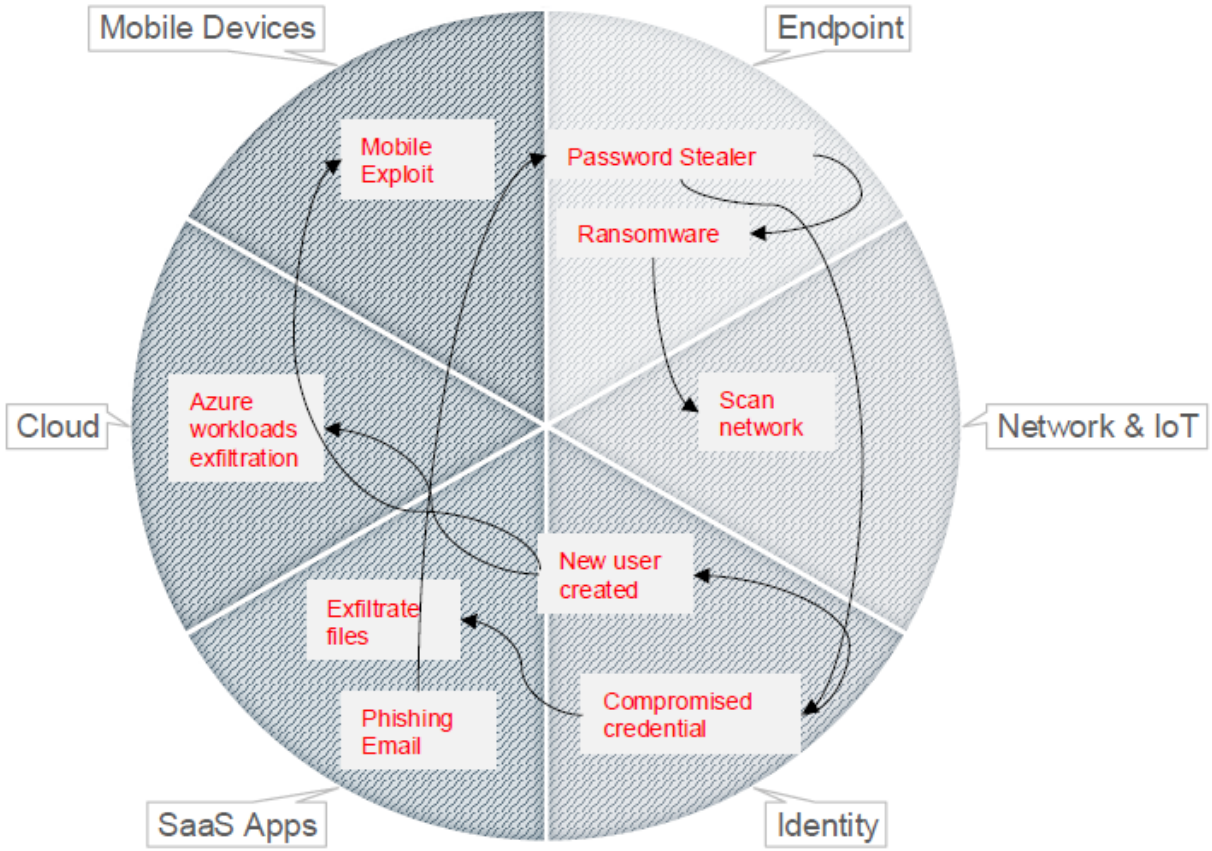
Vulnerabilities and Attack Surfaces Are Rapidly Increasing

More Vulnerabilities, faster exploitation



Source: https://www.cvedetails.com/

Expanding attack surface



Proč vznikl PHASR

Bitdefender

Unnecessary attack vectors

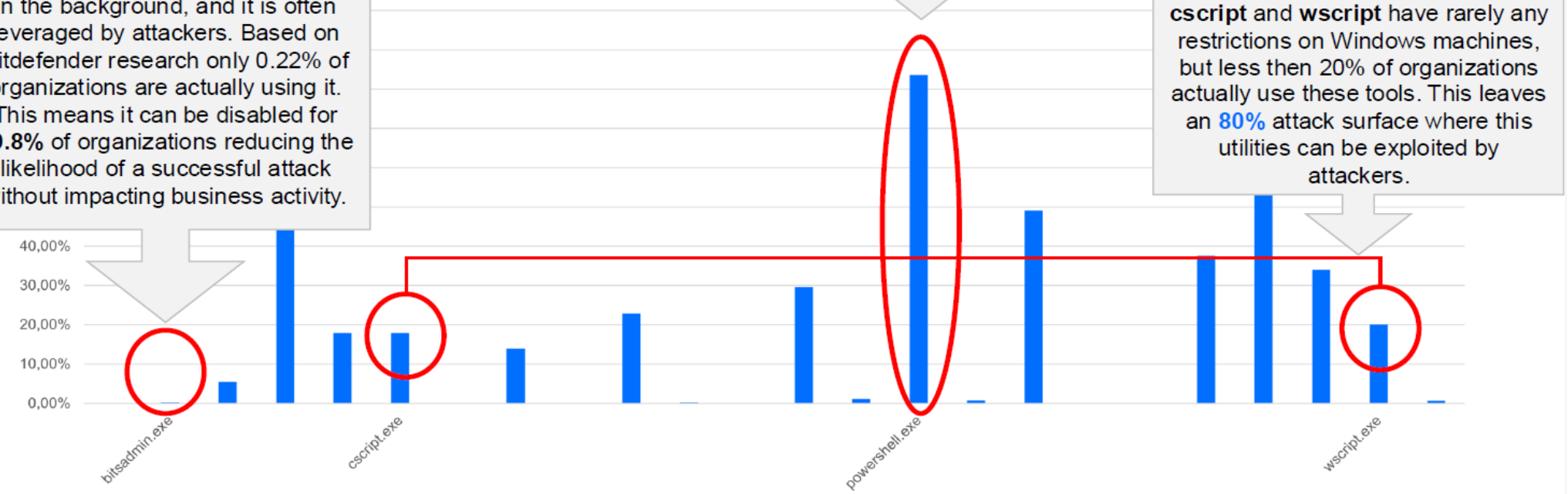
REAL-WORLD EXAMPLES

Furthermore, 90% of the PowerShell usage includes admin accounts, which means PowerShell could be disabled for local users.

PowerShell however it is being used by 83.6% of companies. It still means that in approx. **17% of cases** an attacker can run potential malicious payloads on devices where the user has never used Powershell.

Bitsadmin is a Microsoft command-line tool that facilitates file transfers in the background, and it is often leveraged by attackers. Based on Bitdefender research only 0.22% of organizations are actually using it. This means it can be disabled for **99.8%** of organizations reducing the likelihood of a successful attack without impacting business activity.

cscript and **wscript** have rarely any restrictions on Windows machines, but less then 20% of organizations actually use these tools. This leaves an **80%** attack surface where this utilities can be exploited by attackers.



PHASR základy

- PHASR je novou součástí našich vrstev “prevence a hardening(u)” ale detekce či odezvy a jeho primárním cílem je dynamicky zmenšovat prostor k útoku nejen pro společnost, ale i pro každého jednotlivce v organizaci.
- Čili jedná se jednodušeji řečeno o technologii, která má za úkol zúžit prostor případnému útočníkovi k útoku. A to tím, že znemožní zneužití systémových aplikací tak, že je znepřístupní lidem, které tyto aplikace nepoužívají.
- To se docílí díky tzv. “hardening” nebo-li vytvrzování viz. předchozí slide hradů…

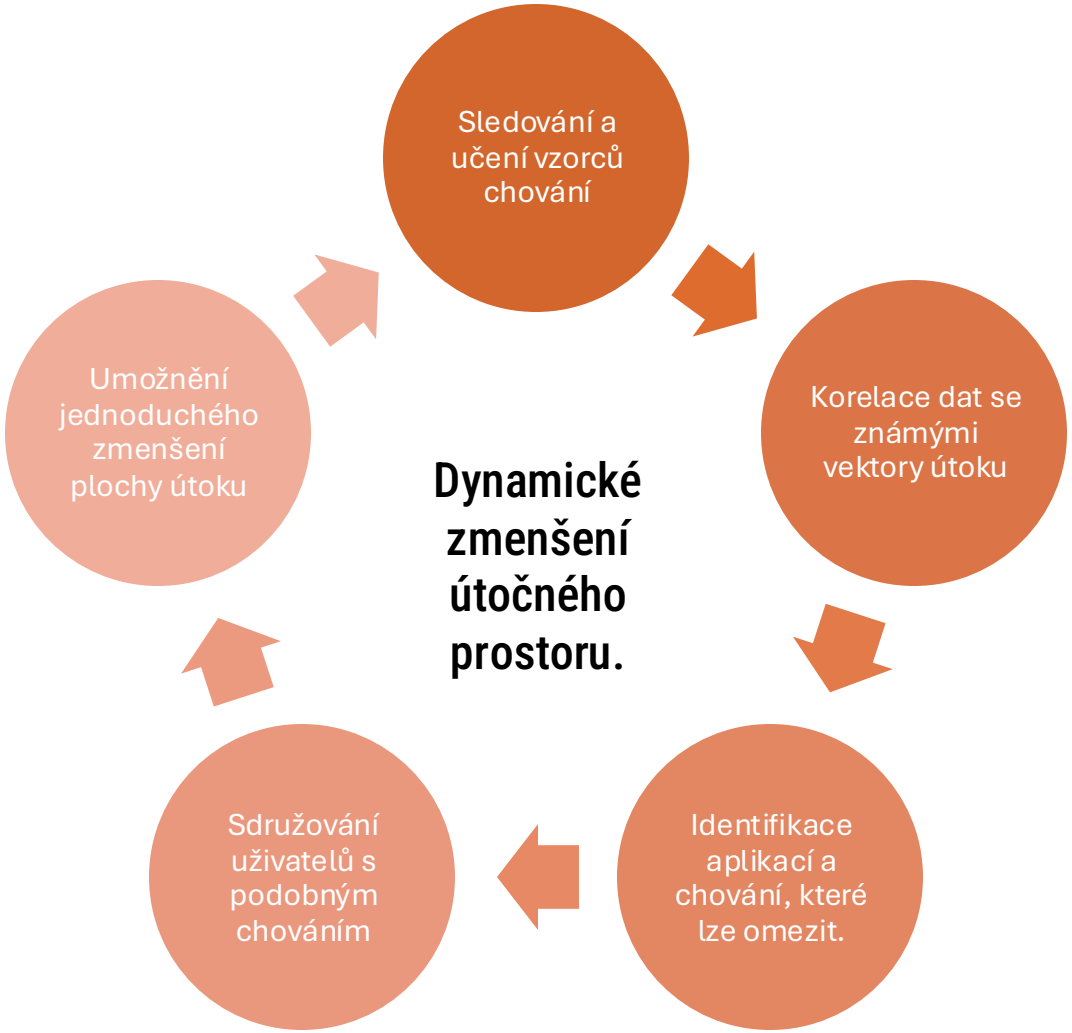
Jak PHASR funguje?

Používá přizpůsobené algoritmy strojového učení k identifikaci neobvyklého chování uživatelů/skupin.

Identifikuje nástroje a konkrétní akce, které lze omezit, aniž by to mělo dopad na běžného uživatele.

Např: PowerShell, uživatelem iniciovaný příkaz Bitlocker

Automaticky se přizpůsobuje chování uživatelů a vyvíjejícím se hrozbám, čímž posiluje neustálé snižování rizik.



Jak probíhá sběr informací?

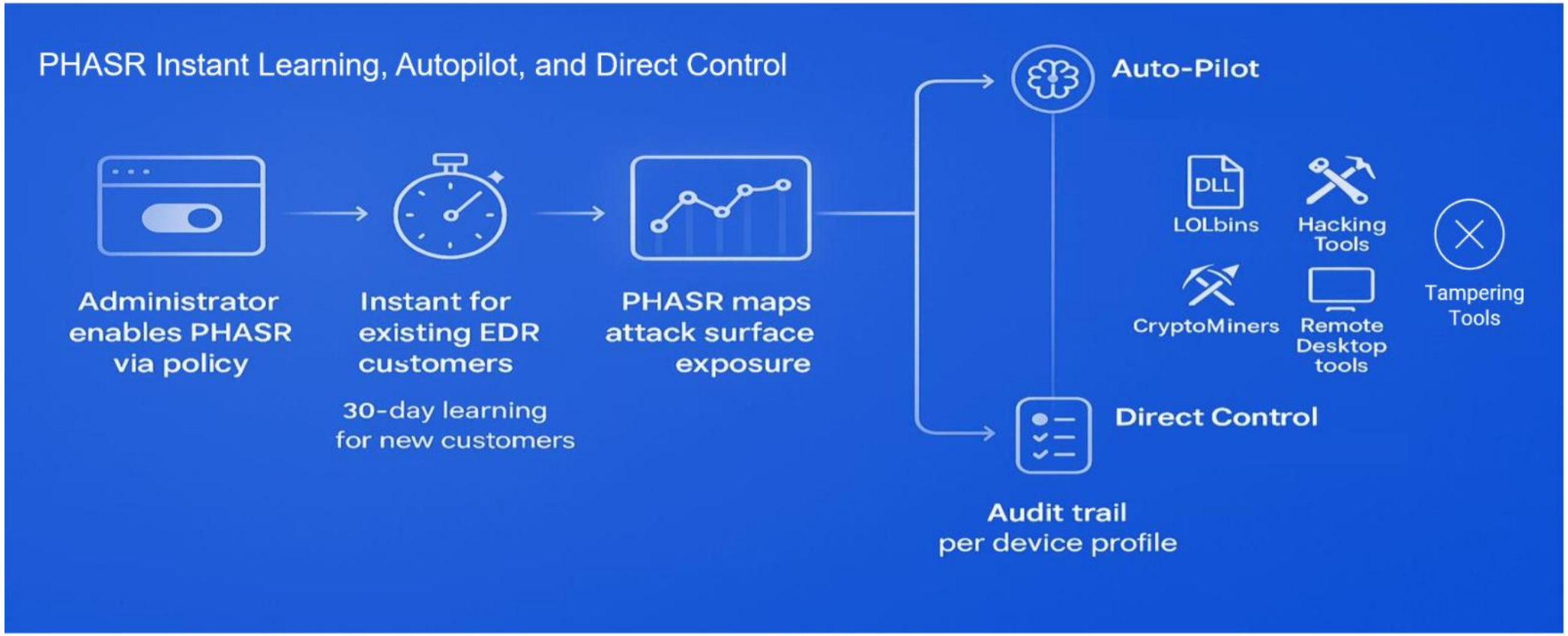
- Sběr informací probíhá jak z chování uživatele – user behavior díky modulu Enpoint Risk Analytics (ERA) tak i přímo ze stanice pomocí EDR modulu. Je to z důvodu toho, že se v rámci domény může uživatel hlásit k více zařízení v rámci domény

- Pokud používáte v rámci domény roli AD Integrátor i ten je zdrojem informací pro konfiguraci PHASR (u)

Jak PHASR funguje - jednoduše

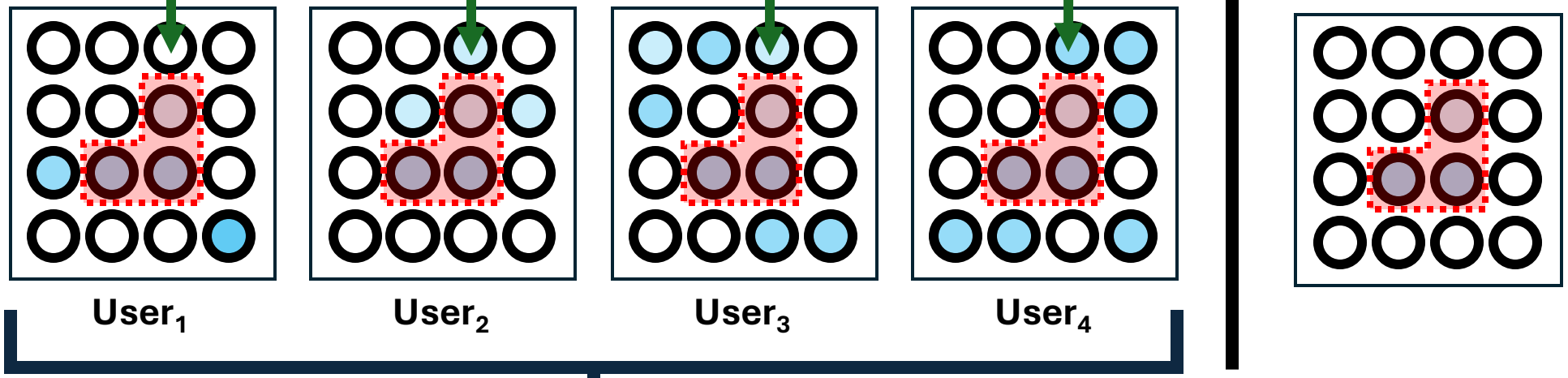
Bitdefender GravityZone PHASR

PHASR'S SIMPLISTIC CONTROLS



Každý uživatel je jedinečný. Zabezpečení těchto uživatelů by mělo být také.

U klasických bezpečnostních řešení jsou spravovány pouze běžné plochy útoku.

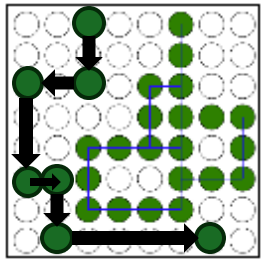


PHASR používá pro každého uživatele jinou detekci, která se dynamicky mění a je pro daného uživatele nejvhodnější (ne pro všechny).

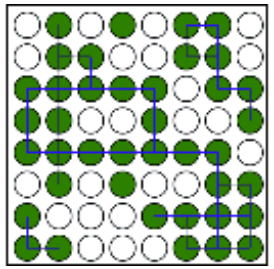
Jak PHASR – funguje detailněji ?

- Každý uživatel je jedinečný a proto přístup k tomu jak své zařízení využívá nebo např. které aplikace či nástroje jsou nezbytné pro jeho každodenní pracovní činnost je třeba vyhodnotit zvlášť.

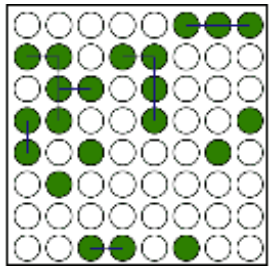
Na obrázcích můžete vidět jak pomcí teček buď nejčastěji probíhá vzorec útoku a na dalších jak PHASR díky proaktivnímu Hardeningu pomáhá bránit útočníkovi zneužít legitimní systémové aplikace a tím mu zabraňuje přejít do další fáze útoku.



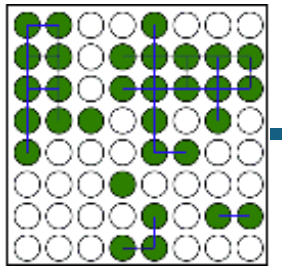
Attack Pattern Identified by the attacker



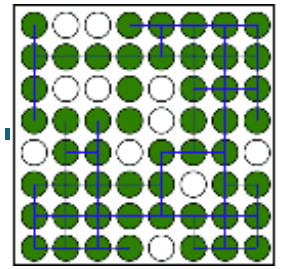
$User_1$ Attack Surface Protection



$User_2$ Attack Surface Protection



$User_3$ Attack Surface Protection



$User_n$ Attack Surface Protection

Shrnutí požadavků pro instalaci PHASR

- Je nutné mít produkt s EDR tzn. GravityZone Business Security Enterprise nebo alacarte + add-on EDR popř. MDR (či MSP Secure, Secure Plus či Secure Extra)

- EDR modul musí být na daném zařízení aktivní a nainstalován

- V politice je nutné zapnout PHASR

- PHASR je úzce napojen na risk management (ERA), proto je nutné mít zapnut v politice i ten

Základní otázky, které si možná nyní kladete:

Co znamená možnost "autopilot"

pokud je autopilot aktivní, rozhodne o omezení přístupu na úrovni koncového bodu. Rozhodování je podmíněno strojovým učením

Kdy PHASR skončí s učením?

Nikdy, obdobně jako EDR se bude učit neustále

Jak dlouho bude trvat učení?

Toto určuje PHASR na základě nastavení pravidel. V případě nového zákazníka nebo povýšení produktu o EDR modul a v závislosti na monitor rules až 30 dní.

Pokud již ve firmě EDR běží, trvá učení jen několik dní..

Proč trvá učení této technologie tak dlouho?

30 dní učení neznamená, že trvá 30 dní než se PHASR naučí dané vzorce chování. Jedná se o nové a nově nainstalované stroje, které do té doby BEST agentem nedisponovali vůbec.

Kdy začně PHASR provádět nějaké akce na stanici?

Jakmile (Monitored rules)sledovaná pravidla se technologie naučí, začne na jejich základě Phaser provádět akce

Základní otázky, které si možná nyní kladete:

Může BitDefender EDR bez technologie Phaser odhalit útoky typu „living-of-the-land“?

Odpověď je ano. Ale většinou v pozdější fázi, V EDR senzoru existují detekce i pro tyto druhy nástrojů včetně vlastního machine learningu.

Jediný rozdíl je, jak jsem řekl v prezentaci, že PHASR vám pomůže identifikovat tyto útoky mnohem dříve v řetězci útoků (attack chain čili vektor útoku) EDR musí mít vždy vyšší stupeň důvěryhodnosti pro spuštění incidentů.

Bude se dále do budoucna rozšiřovat působnost PHASR o další nástroje, než-li těchto 5 základních?

ANO

Co když bude stroj offline nebo nebude mít přístup k internetu, bude PHASR fungovat?

ANO! Ale je třeba myslet na to, že stroji musí být nějakým způsobem (např. pomocí relaye) přiřazena politika. A samozřejmě, že se případné změny v nastavení PHASER na stanici nepropíší dokud se stroj znovu nespojí s GravityZone. Strojové učení “autopilot” je navrženo tak, aby běželo lokálně v rámci BEST agenta bez potřeby GZ konzole.

Jaká je cenová politika produktu a kolik to bude stát?

Produkt je licencován pouze na celkový počet zařízení základní licence (nelze proto zakoupit na vybrané stroje nebo zákazníkem zvolený počet zařízení a tímpádem se odvíjí od původní licence BSE či součtu alacarte + EDR . Ohledně ceny budete muset kontaktovat Vámi přiděleného obchodníka.

Závěrem

Užitečně linky:

PHASR

https://www.bitdefender.com/business/support/en/77209-1192263-phasr.html#UUID-2297300c-dec9-06eb-f8fd-43e01347c005

MasterClass -> Jedná se krátké webináře, kde naleznete On-Boarding, Best Practices, Troubleshooting, instalace, investigaci incident popř. vysvětlení DEMO incident v GZ.

https://www.bitdefender.com/masterclass

Status of GravityZone -> zjištění, zda-li běží všechny služby + informace o již nahlášených problémech v rámci GravityZone

https://status.gravityzone.bitdefender.com/

KB včetně release notes, best practices atp, možnosti nastavení politik, atp.

https://help.gravityzone.bitdefender.com/

stránka s podbrobnosti o nalezených zranitelnostech v rámci produktů BD

https://www.bitdefender.com/support/security-advisories/

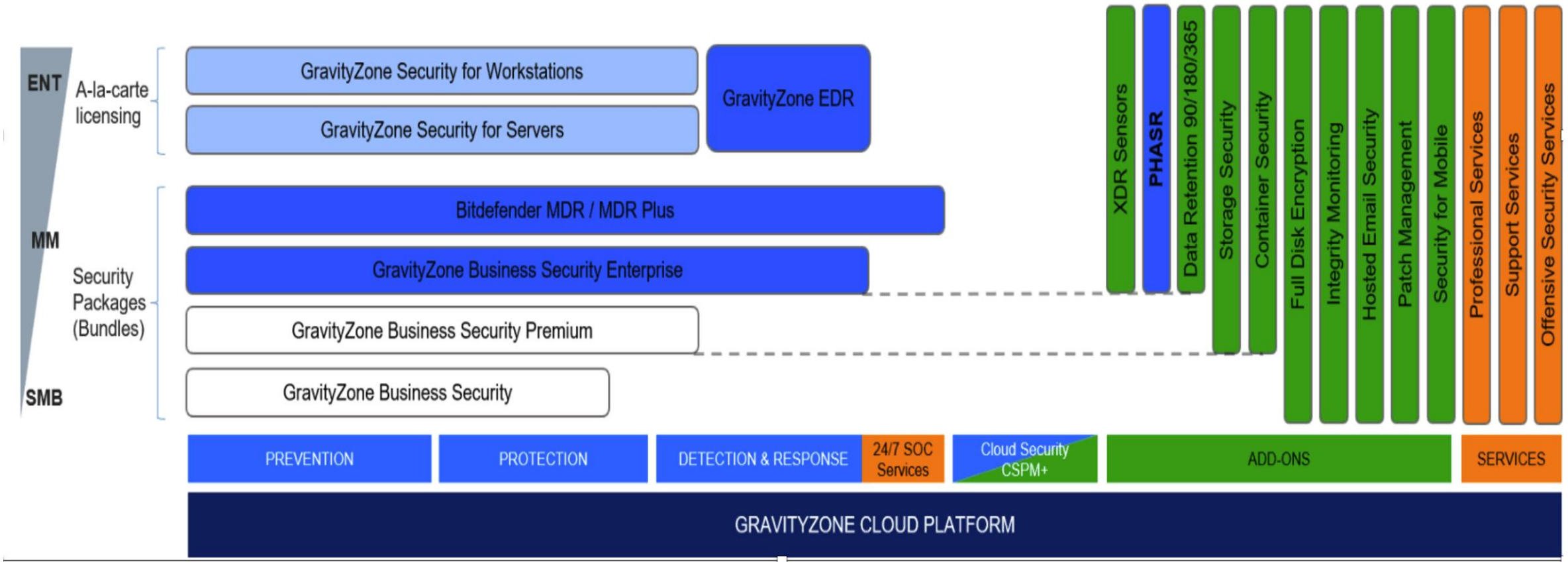
TechZone - detailnější technické informace o vybraných produktech

https://techzone.bitdefender.com/

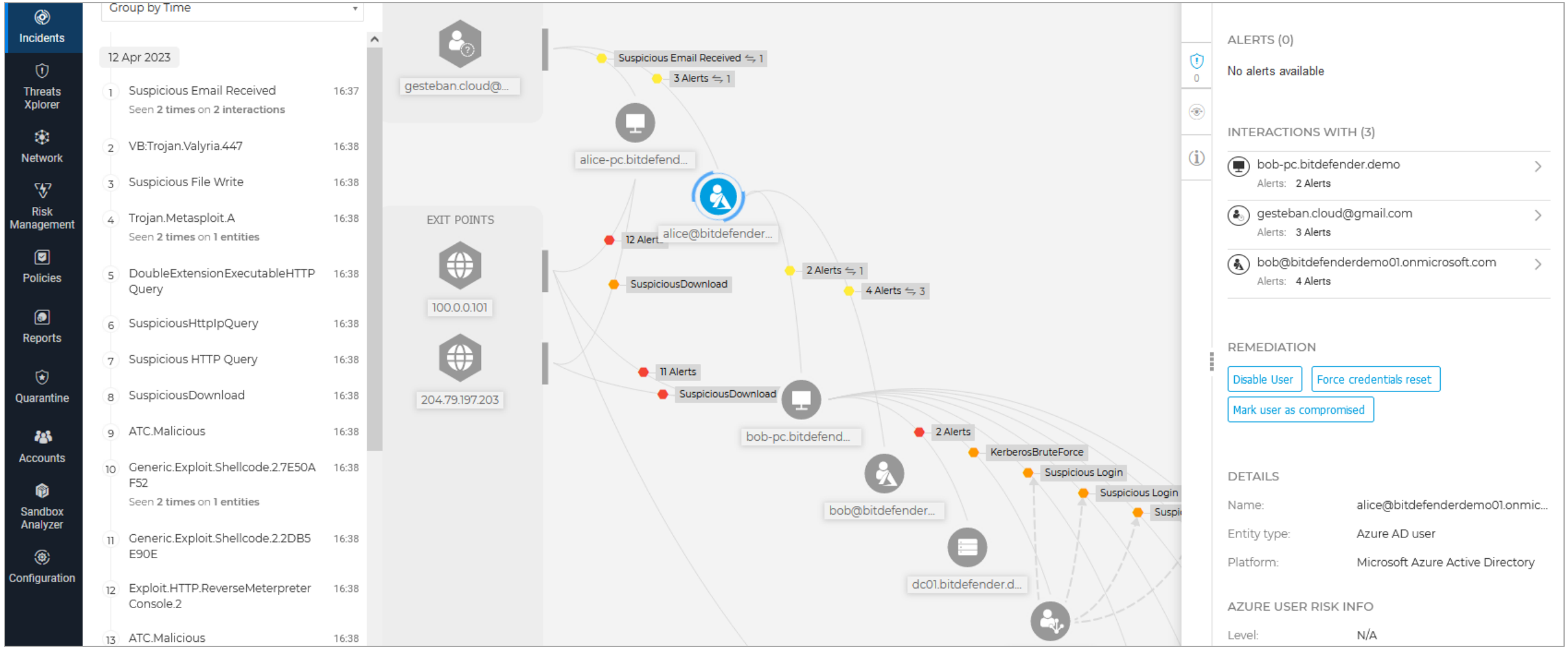
DEMO Zone GZ -> možnost vidět po grafické stránce jak produkty či jeho části fungují

https://www.bitdefender.com/business/demo-zone

Licencování a požadavky PHASR - addon modul pro Bitdefender GravityZone Enterprise (EDR/XDR) platformu



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



Sledování
Incidenty
Xplorer hrozeb
Síť
Risk Management
Pravidla
Reporty
Karanténa
Účty
Sandbox Analyzér
Konfigurace

96/100
Skóre závažnosti incidentu

Vytvořeno: 18 Bře 2024, 20:26:59
Aktualizováno: 18 Bře 2024, 21:32:54
Typ útoku: LateralMovement Exploit

SHRNUTÍ

V rámci 18 upozornění bylo zjištěno potenciální narušení sítě pocházející z nespravovaný produkt: 192.168.190.2, které ovlivňuje nespravovaný produkt: 192.168.190.254, a 5 spravovaná aktiva.

Ve vaší síti byl zjištěn postraní pohyb pocházející z 3 spravovaná aktiva, který je součástí 22 upozornění a ovlivňuje 3 spravovaná aktiva. Pověření mohla být ohrožena na 5 spravovaná aktiva, na základě 30 upozornění, pocházející z nespravovaný produkt: 192.168.190.2. Byl zjištěn pokus o získání nebo udržení perzistence možného škodlivého objektu v upozornění RunKeyWritten, na spravované aktiva: DEMO-DAN. V rámci 31 upozornění bylo zjištěno více pokusů o komunikaci od 2 nespravovaná aktiva do 5 spravovaná aktiva.

PŘÍČINA

Incident byl vyvolán pokusem o zneužití pocházejícím z nespravovaný produkt: 192.168.190.2 a zahrnujícím nespravovaný produkt: 192.168.190.254, a 5 spravovaná aktiva.

ATT&CK TAKTIKY A TECHNIKY

Initial Access	T1190	Exploit Public-Facing Application
Discovery	T1046	Network Service Discovery
Reconnaissance	T1595	Active Scanning
Command and Control	T1571	Non-Standard Port
	T1071	Application Layer Protocol
Credential Access	T1110	Brute Force
Defense Evasion	T1553	Subvert Trust Controls
	T1134	Access Token Manipulation
	T1112	Modify Registry
Lateral Movement	T1021	Remote Services
Execution	T1059	Command and Scripting Interpreter
Privilege Escalation	T1134	Access Token Manipulation
	T1547	Boot or Logon Autostart Execution
	T1037	Boot or Logon Initialization Scripts
Persistence	T1547	Boot or Logon Autostart Execution
	T1037	Boot or Logon Initialization Scripts

DOPAD NA ORGANIZACI

ENTITY

7 | 1 | 1

ZDROJE

12

HIGHLIGHTS

Exploit.PentestingTool.HTTP.1 | Počáteční přístup

Severity: Nízký

Network Probe has detected a pentesting activity performed in your network.
Detekováno senzorem: *Síť* dne 18 Bře 2024 v 19:35:18

2

+ 17 OTHER POČÁTEČNÍ PŘÍSTUP ALERTS

Exploit.DCOM.FileExplorer | Postranní pohyb

Severity: Střední

Network Probe has detected the creation of a remote File Explorer process (using the DCOM network protocol), which could lead to remote code execution.
Detekováno senzorem: *Síť* dne 18 Bře 2024 v 20:59:41

2

+ 21 OTHER POSTRANNÍ POHYB ALERTS

Attack.Bruteforce.RDP | Udělení přístupu

Severity: Nízký

Network Probe has detected a large number of login attempts that are usually associated with a bruteforce attack.
Detekováno senzorem: *Síť* dne 18 Bře 2024 v 20:30:40

2

+ 29 OTHER UDĚLENÍ PŘÍSTUPU ALERTS

RunKeyWritten | Trvání

Severity: Nízký

A Startup item registry key(HKCU\\SOFTWARE\\Microsoft\\Windows\

RESPONSE

Poslední aktualizace 22:17:35

ACTION NEEDED (7) | EXECUTED

UZAVŘENÍ

4 Koncové body k izolaci

VIEW DETAILS

VYTVRZOVÁNÍ

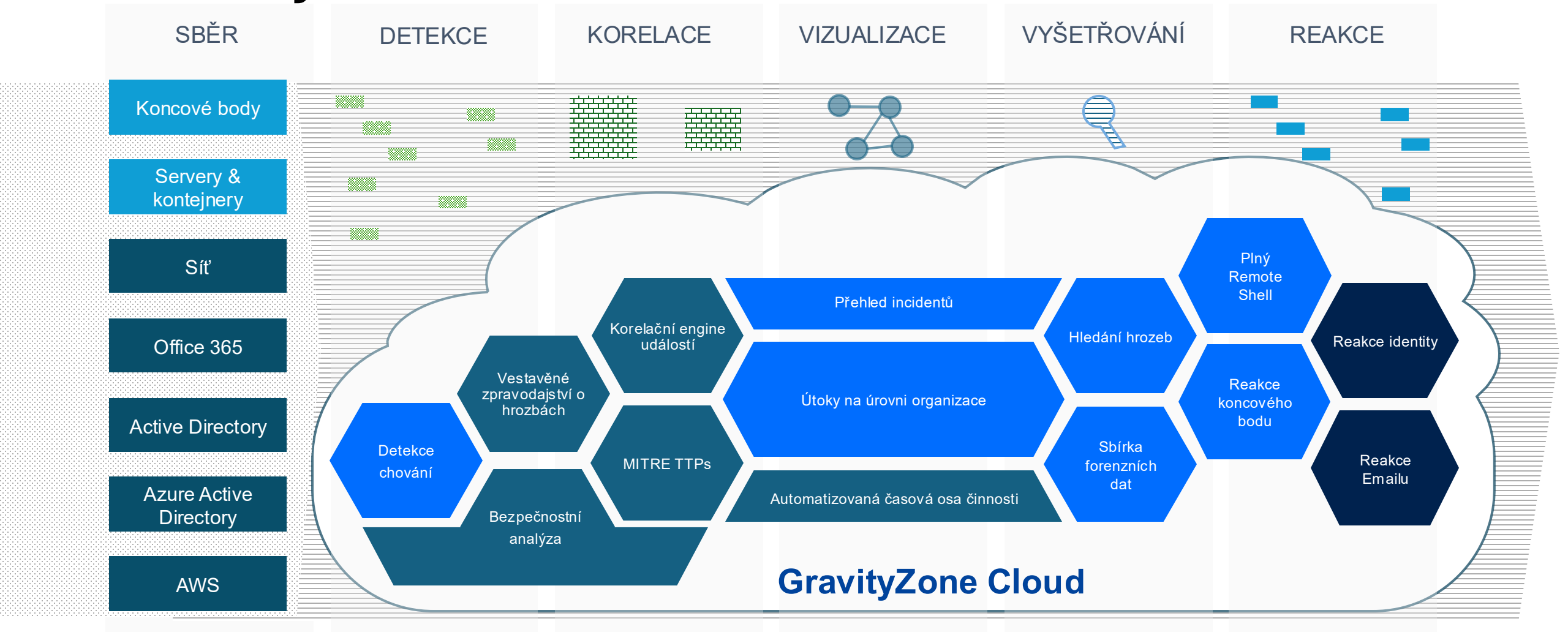
3 Aktiva ke správě

VIEW DETAILS

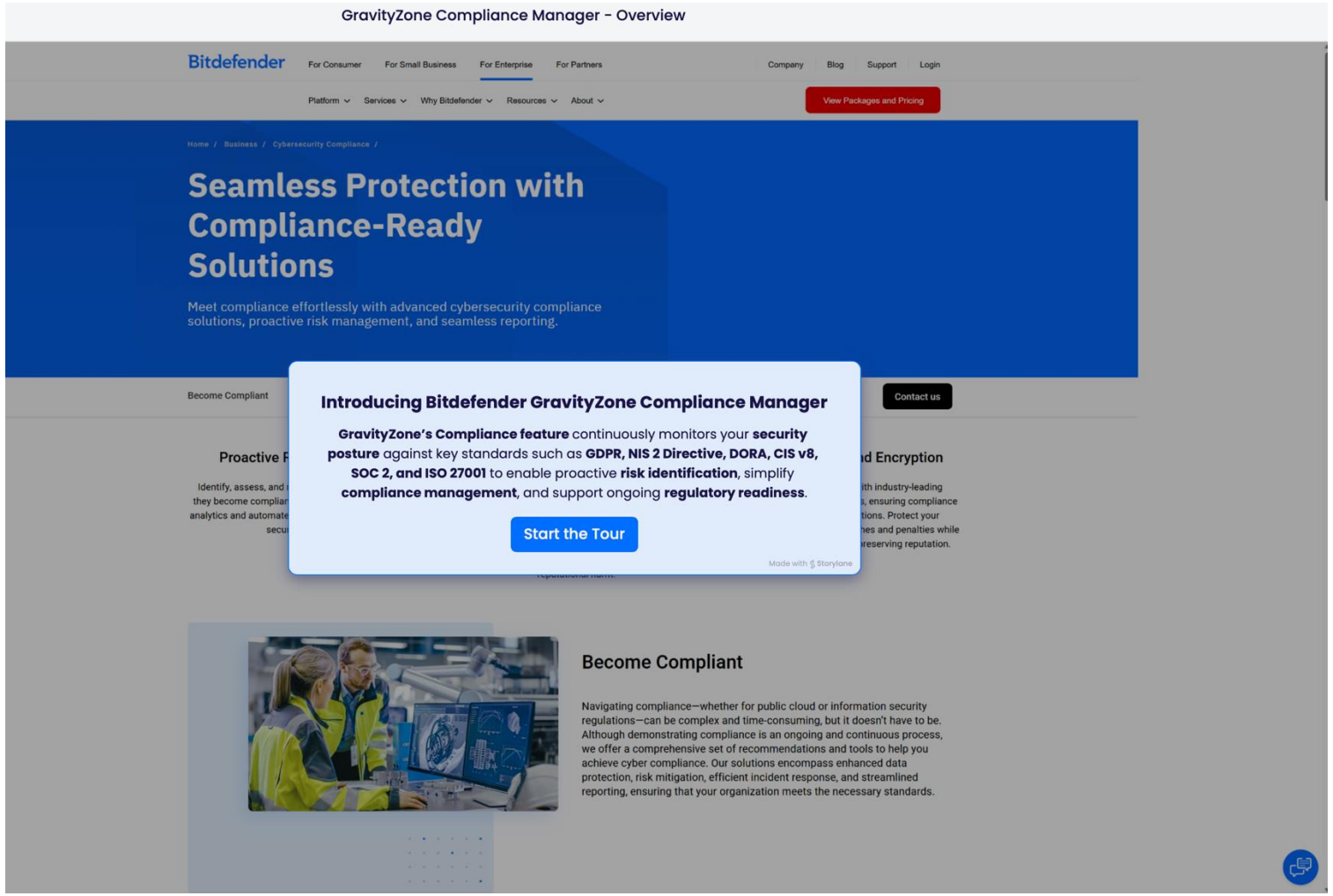
(AI) INCIDENT ADVISOR vám AUTOMATICKY poví :

- **co se vůbec stalo?**
- **kdy to začalo?**
- **kam se to rozšířilo?**
- **jak reagovat?**
- **proč to bylo vůbec možné?**
- **jak to můžete vyřešit?**
- **jak můžete zamezit dalšímu šíření útoku?**

GravityZone XDR



Nový Bitdefender GravityZone Compliance Manager velký pomocník pro splnění nejen **NIS2** ale i pro DORA, SOC2, SOC 2, ISO270001, GDPR atd.



Umožnuje monitorovat a řídit shodu s klíčovými legislativními bezpečnostními směrnicemi:

NIS2
DORA
CIS V8
SOC 2
ISO 27001
GDPR atd.

Podívejte se na Bitdefender Compliance Manager DEMO zde: https://demo.bitdefender.com/share/crtpbgulfvsq

Policy Manager je dostupný jako addon pro Bitdefender GravityZone již od základní Business Security

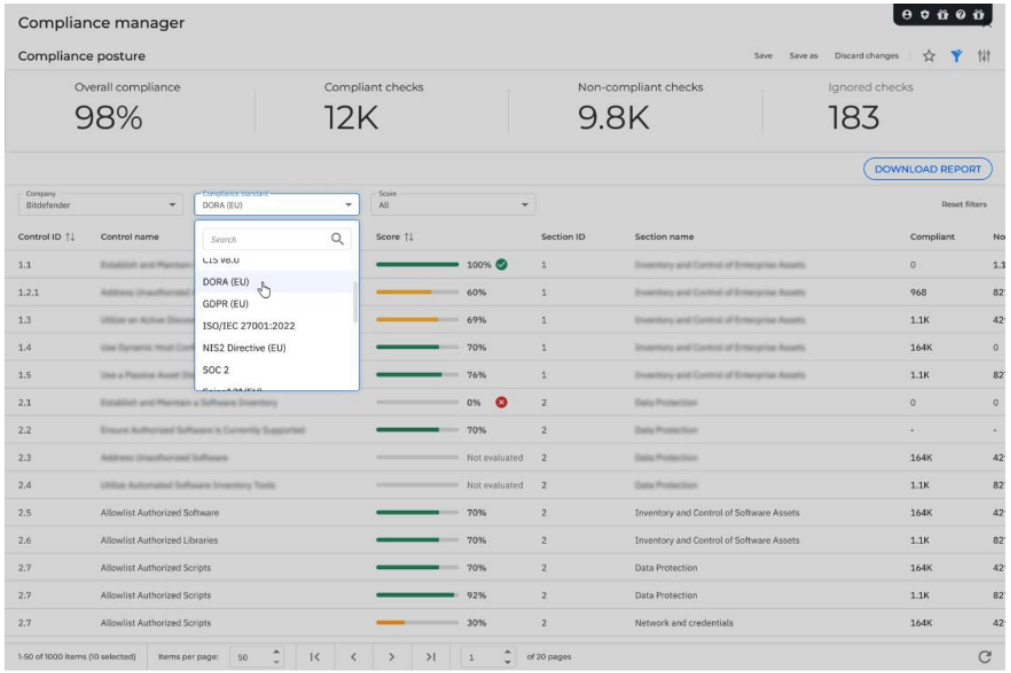
GravityZone Compliance Manager

Available as an Add-on License

- Available to both Yearly and Monthly
- Unlocks full access to standards such as GDPR, PCI DSS, SOC 2, DORA *(Advanced Standards)*

Available as an add-on with all base licenses, excluding *Small Business Security*.

- GravityZone Business Security (BS)
- Business Security Premium (BSP)
- Business Security Enterprise (BSE)
- GravityZone EDR Cloud
- GravityZone Cloud MSP Security
- Bitdefender MDR



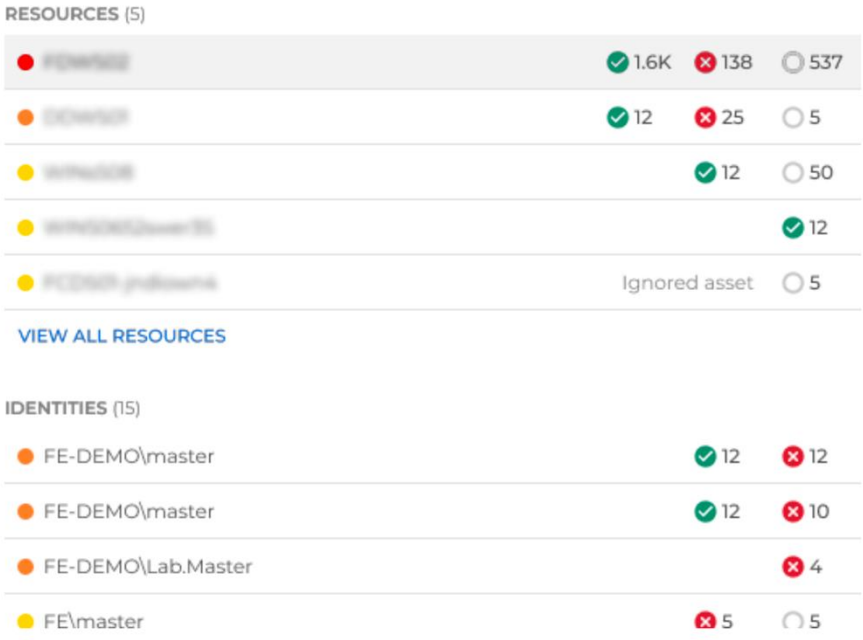
Umožňuje přehledy v reálném čase,
Vytváří automaticky audity a reporty během minut

Bitdefender

Key Capabilities

From Months to Minutes: Automated, Audit-ready Reports

- ✓ **Supports Multiple Compliance Standards**
  Out-of-the-box support for major compliance standards such as GDPR, PCI DSS, NIS 2 Directive, CISv8, SOC 2, HIPAA and ISO 27001.
- ✓ **Real-time Insights**
  Real-time visibility into risks, affected assets, and overall compliance posture for both cloud and on-premises endpoints to help accelerate processes and reduce time-to-compliance.
- ✓ **Close Identified Compliance Gaps**
  Quickly fix detected gaps – reducing risk, saving time, and streamlining remediation.
- ✓ **Comprehensive Report Generation**
  Generate detailed reports that consolidate all relevant data, reducing complexity, saving time, and minimizing the need for specialized expertise.

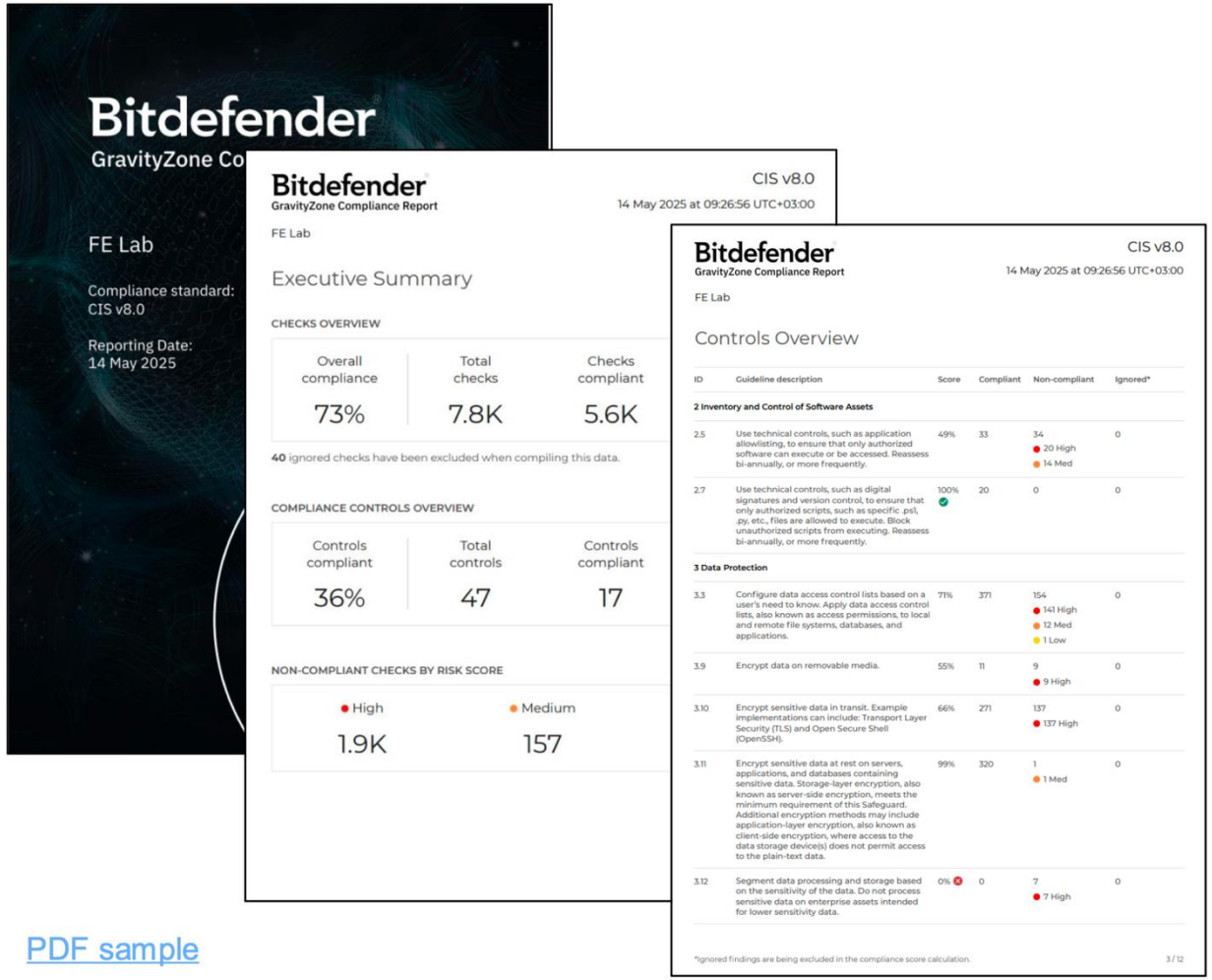


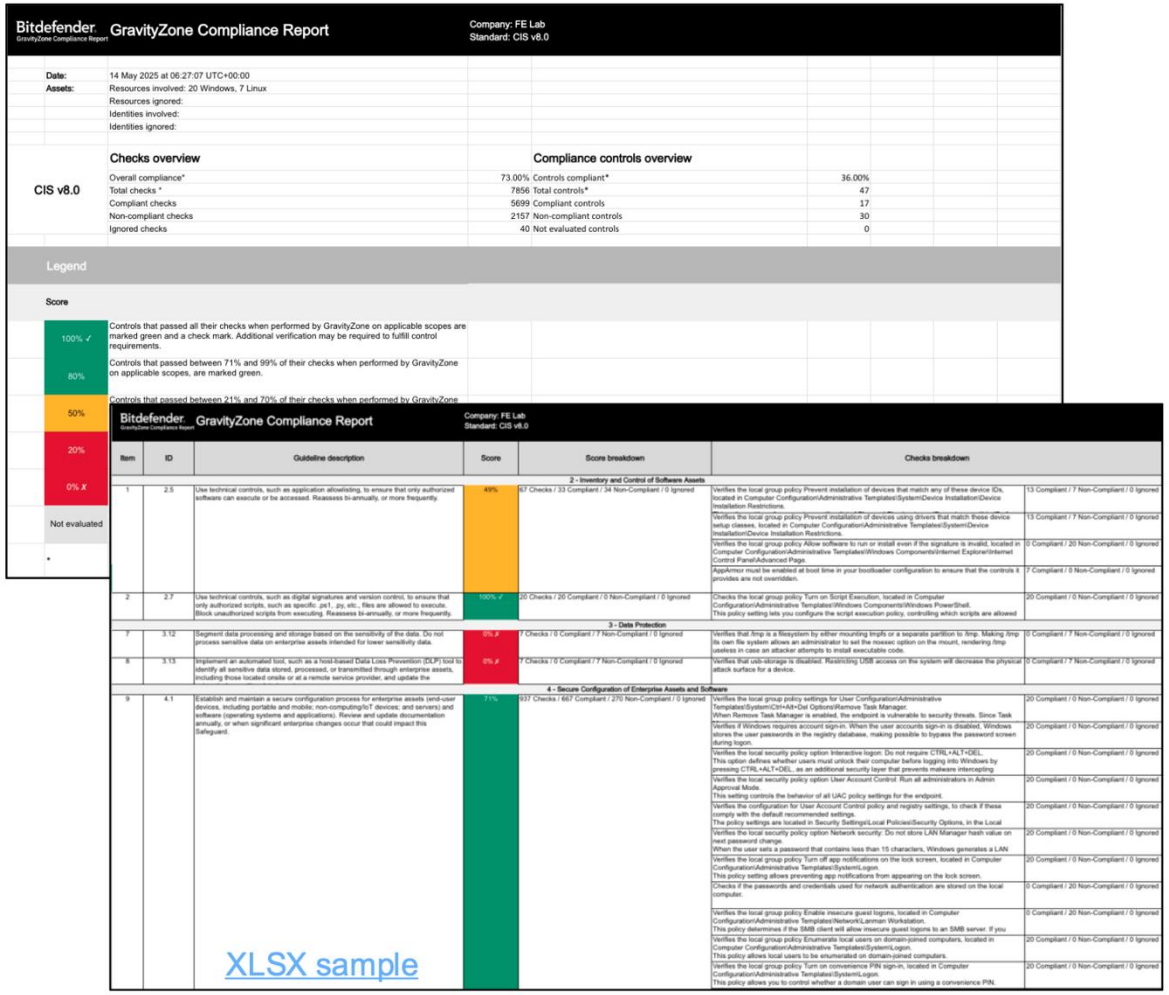
** Legal Notice
Bitdefender's GravityZone Cloud Security compliance features and reports are designed to help organizations with compliance-related security activities, in particular with assessing and helping maintain compliance with its listed standards and baselines, but can neither fully replace internal efforts nor guarantee that an organization will pass a compliance audit. Bitdefender recommends you work with an approved auditor to obtain any official compliance certifications.

Bitdefender

GravityZone Compliance Manager - Reports

Audit-ready reports available in **PDF** and **XLSX** formats





[PDF sample]

[XLSX sample]

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 Praha, Olomouc, Bratislava**

www.bitdefender.cz