



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**



LEGEND

- ATTACKS
- INFECTIONS
- SPAM

LIVE ATTACKS

TIME	ATTACK	ATTACK TYPE	ATTACK COUNTRY	TARGET COUNTRY
FRI 6 SEP 8:11:4...	?TABTIP.EXE:0000...	INFECTION	ROMANIA	N/A
FRI 6 SEP 8:11:5...	N/A	SPAM	UNITED STATES	N/A
FRI 6 SEP 8:11:4...	GEN:ILLUSION.PUP...	INFECTION	UNITED STATES	N/A
FRI 6 SEP 8:11:4...	?REGSVR32.EXE:00...	INFECTION	UNITED STATES	N/A
FRI 6 SEP 8:11:4...	?SIGNAL.EXE:0000...	INFECTION	UNITED KINGDOM	N/A
FRI 6 SEP 8:11:4...	APPLICATION.HACK...	INFECTION	BRAZIL	N/A
FRI 6 SEP 8:11:5...	N/A	ATTACK	UNITED STATES	UNITED STATES

LOCATIONS

- UNITED STATES
- ROMANIA
- FRANCE
- BRAZIL
- GERMANY
- CANADA
- UNITED KINGDOM
- MEXICO
- INDIA

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)



In the past, cyber attackers acted like burglars

Jejich podezřelé nástroje a chování tak spouštěly POPLACH ...



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



Today, attackers don't break in
but log in using stolen credentials

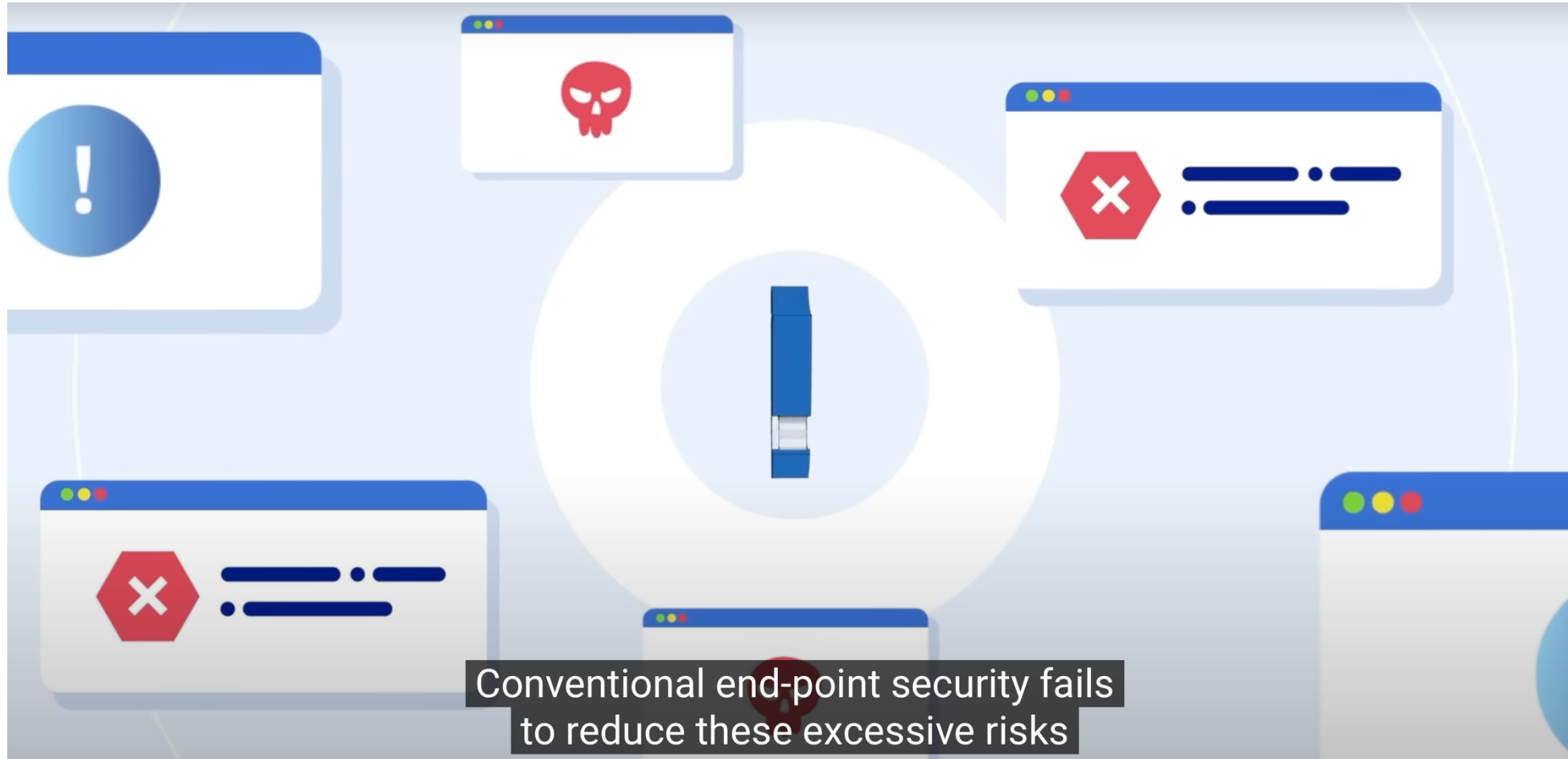
Využívají legitimní nástroje OS a běžné aplikace správy IT
84% útoků probíhá dnes za pomoci těchto nástrojů ... (LOTL)



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 výjimky 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 pokročilé 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 společností Bitdefender. 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..

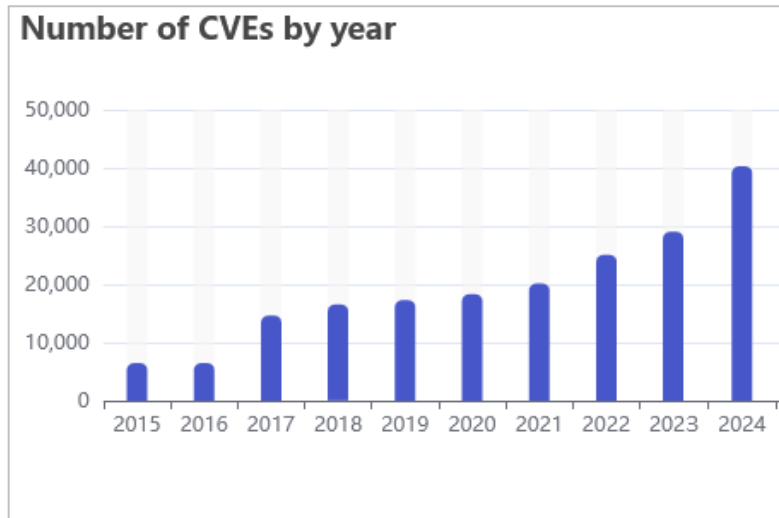


Bitdefender
PHASR



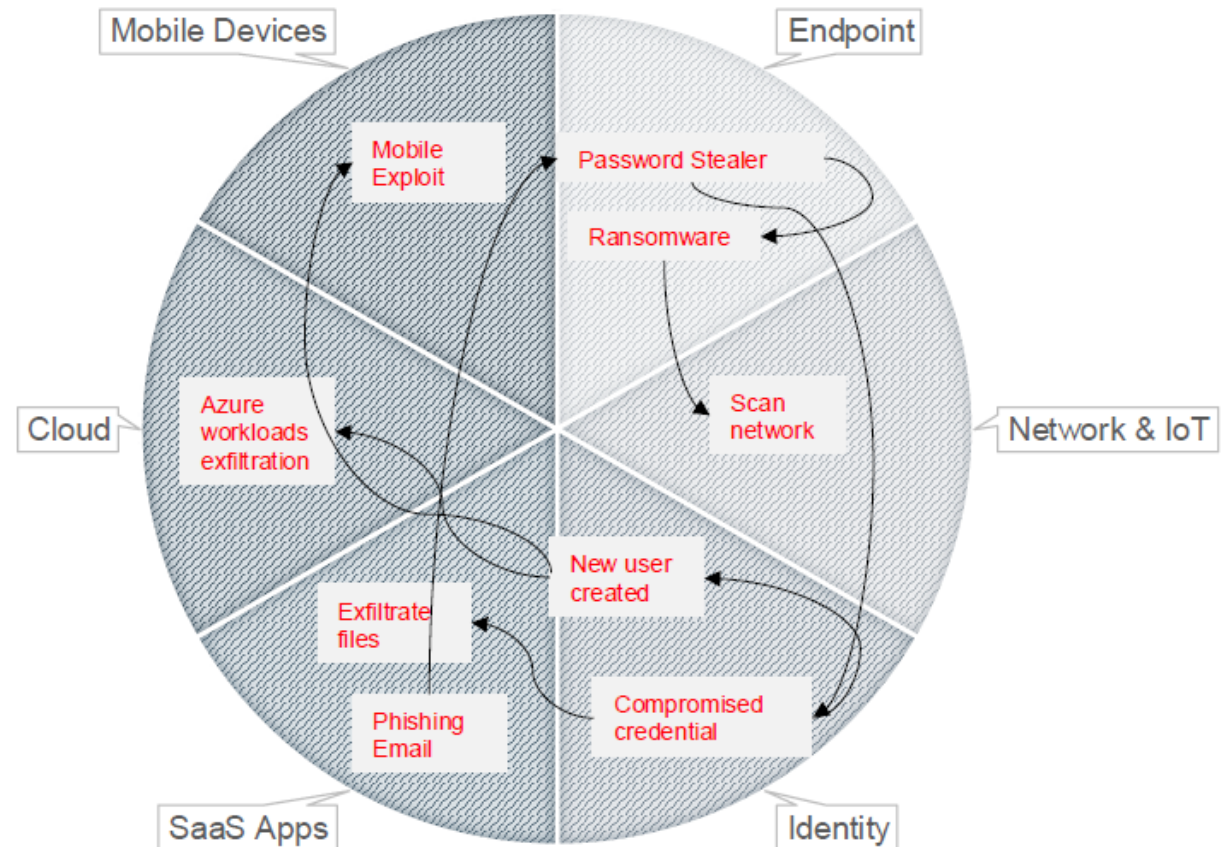
Vulnerabilities and Attack Surfaces Are Rapidly Increasing

More Vulnerabilities, faster exploitation



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

Expanding attack surface



Proč vznikl PHASR

Bitdefender®

Unnecessary attack vectors

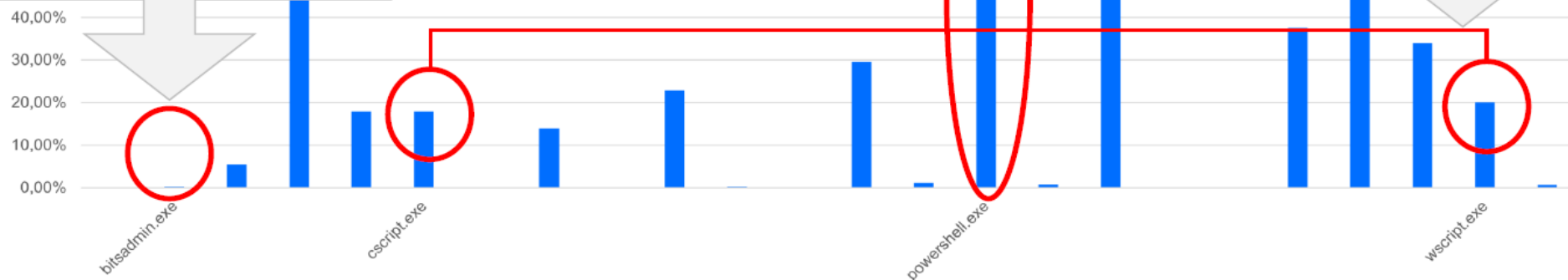
REAL-WORLD EXAMPLES

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.

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.

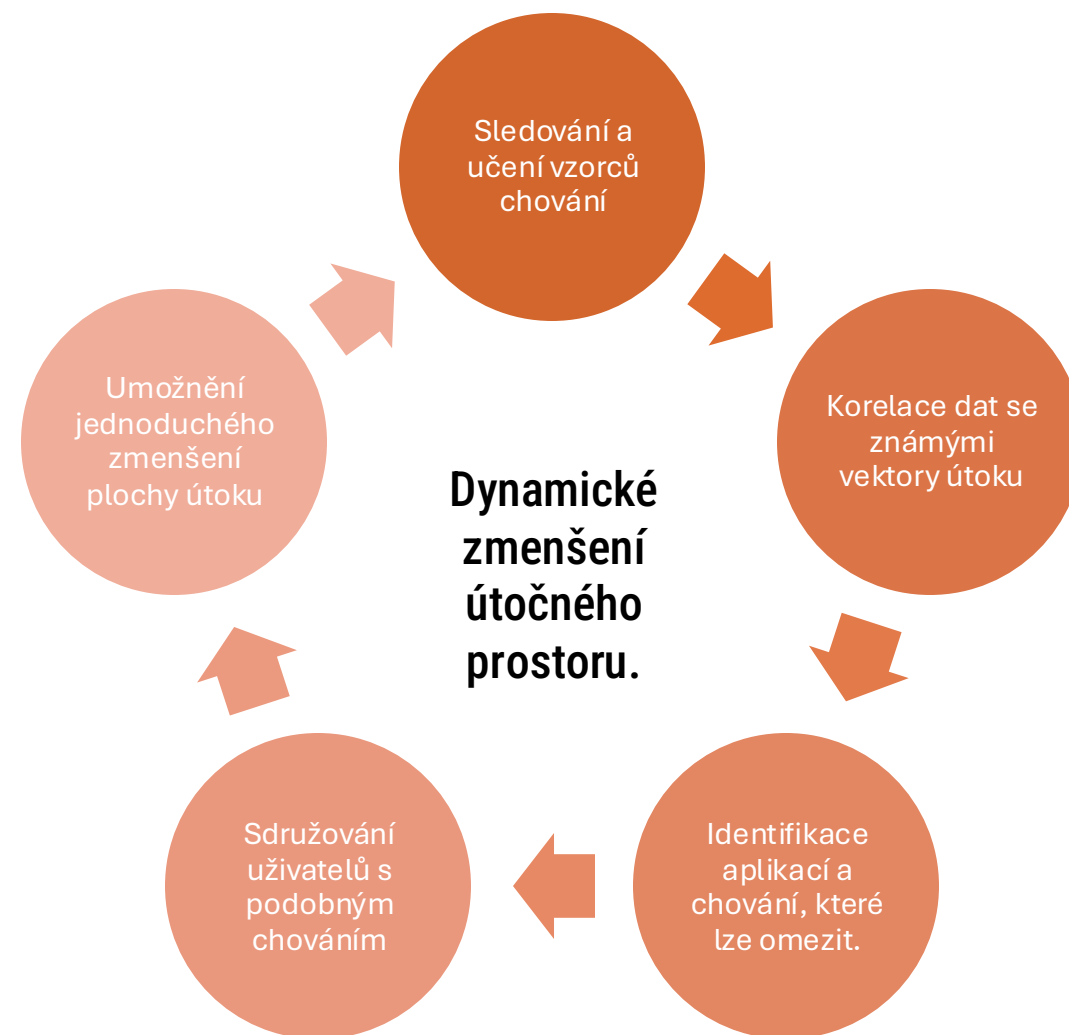
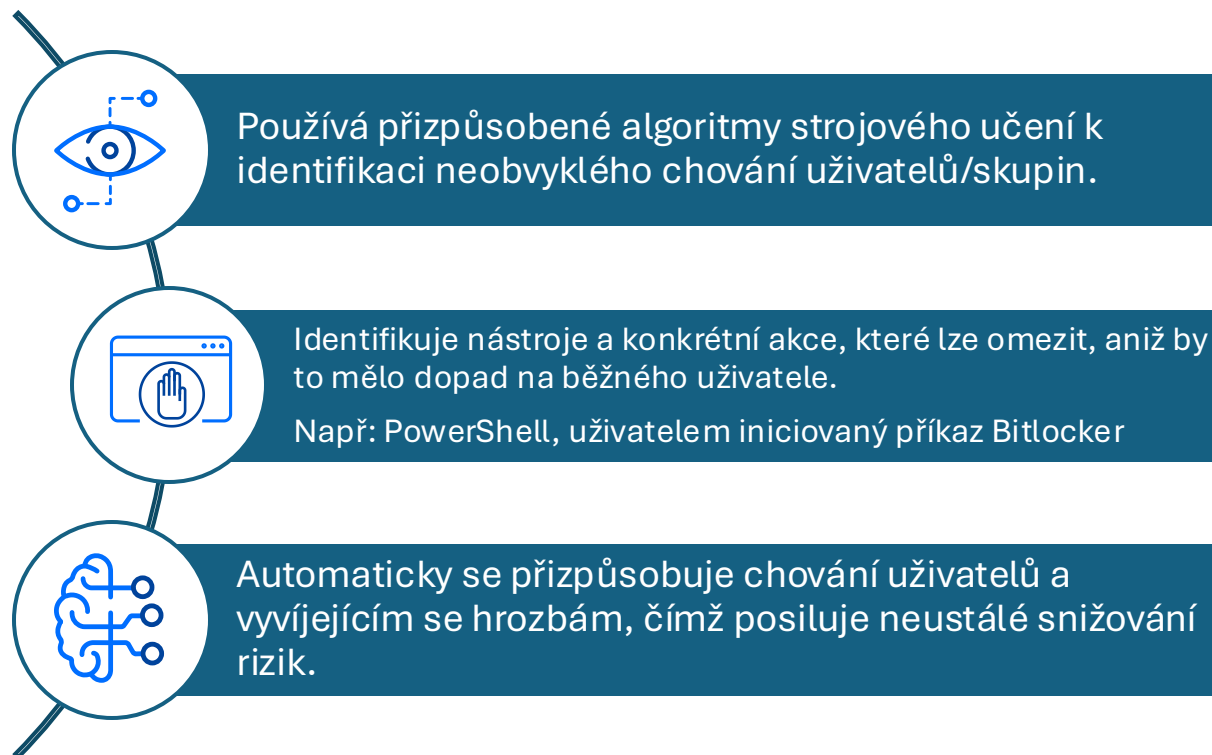
cscript and **wscript** have rarely any restrictions on Windows machines, but less than 20% of organizations actually use these tools. This leaves an **80%** attack surface where this utilities can be exploited by attackers.



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?



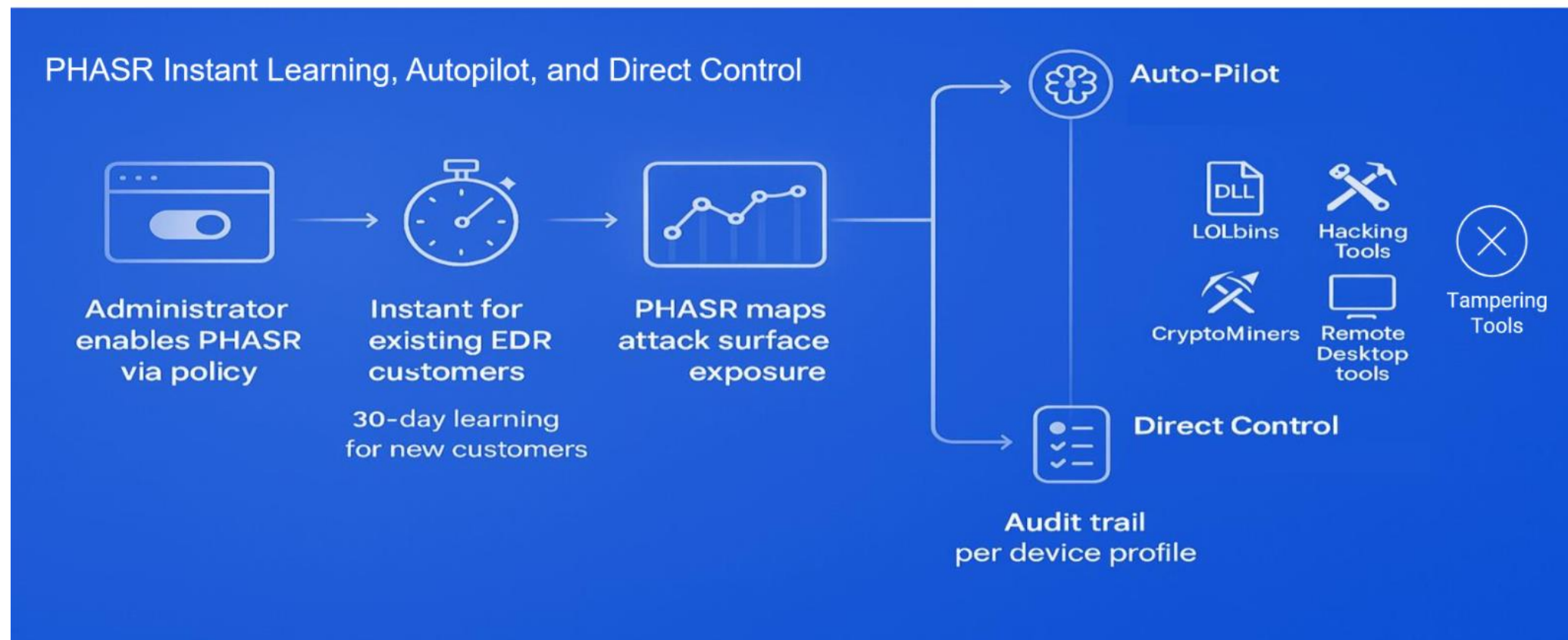
Jak probíhá sběr informací?

- Sběr informací probíhá jak z chování uživatele – user behavior díky modulu Endpoint 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 zařízením v rámci domény
- Pokud používáte v rámci domény roli AD Integrátor i ten je zdrojem informací pro konfiguraci PHASR (u)

Jak PHASR funguje - jednoduše

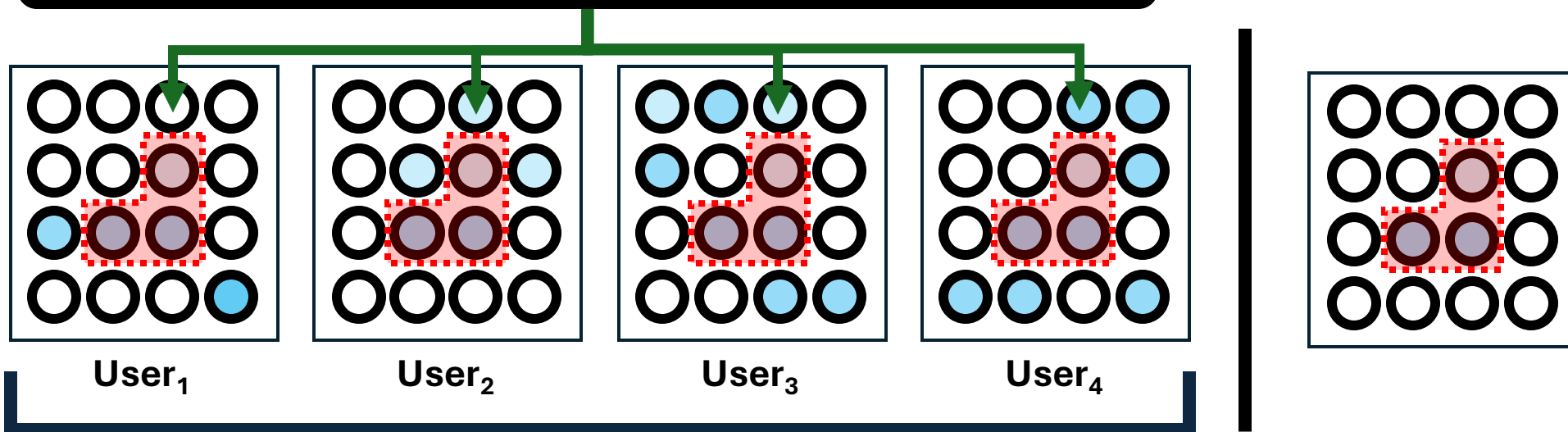
Bitdefender GravityZone PHASR

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.



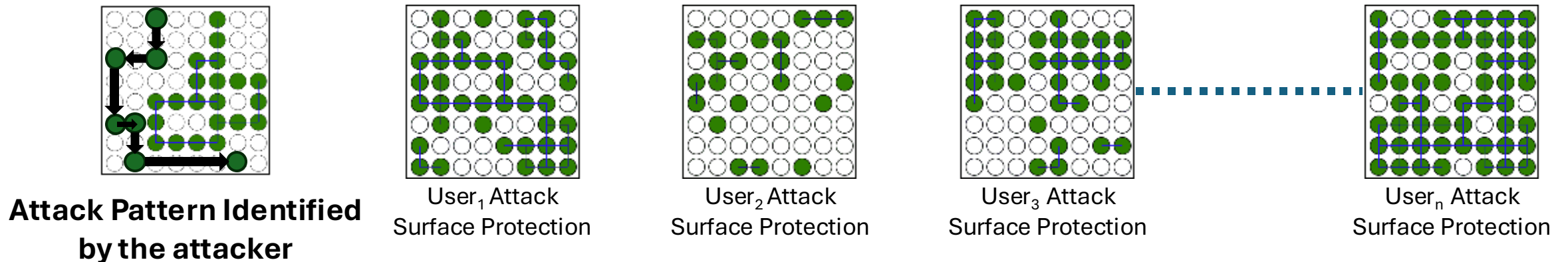
PHASR používá pro každého uživatele jinou detekci, která se dynamicky mění a je pro daného uživatele nejvhodnější (ne pro všechny).

Ostatní

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 pomocí 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.



Shrnutí požadavků pro instalaci PHASR

- Je nutné mít produkt s EDR tzn. GravityZone Business Security Enterprise nebo a la carte + 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 neznámá, 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 začne 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 tím pádem se odvíjí od původní licence BSE či součtu a la carte + EDR . Ohledně ceny budete muset kontaktovat Vámi přiděleného obchodníka.

Závěrem

Užitečné linky:

PHASR

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

MasterClass -> Jedná se o krátké webináře, kde naleznete On-Boarding, Best Practices, Troubleshooting, instalace, investigaci incidentů popř. vysvětlení DEMO incidentu 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 podrobnostmi o nalezených zranitelnostech v rámci produktů BD

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

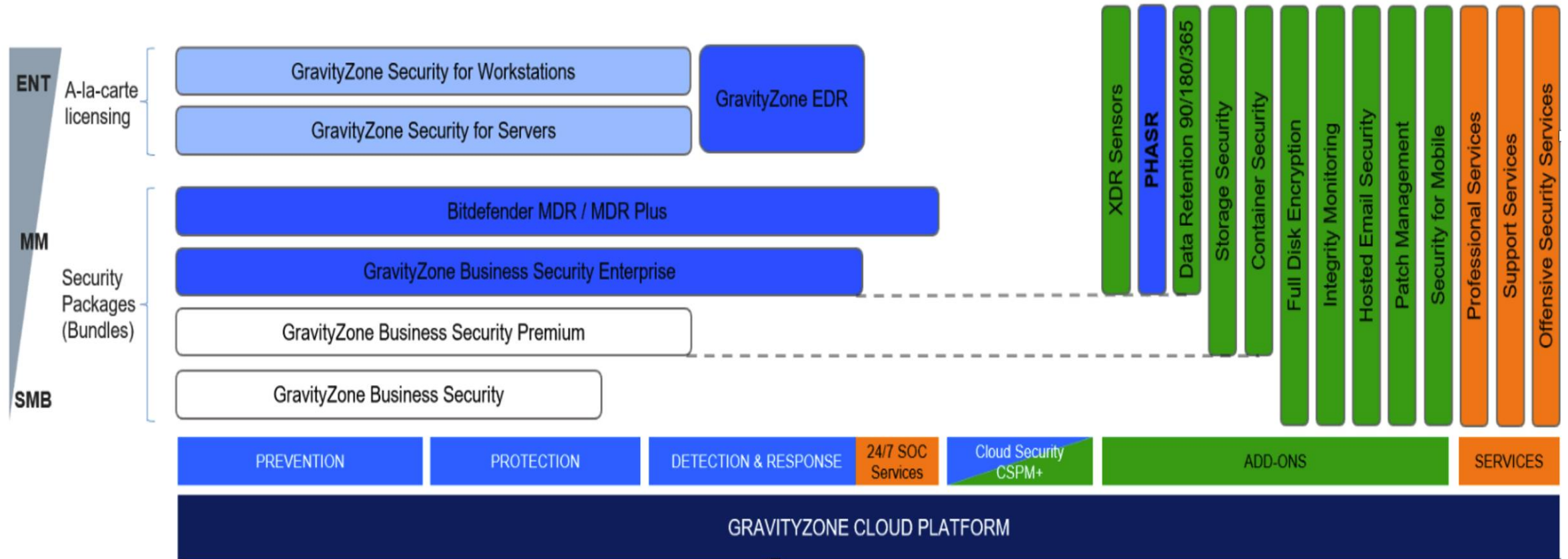
TechZone - detailnější technické informace o vybraných produktech

<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

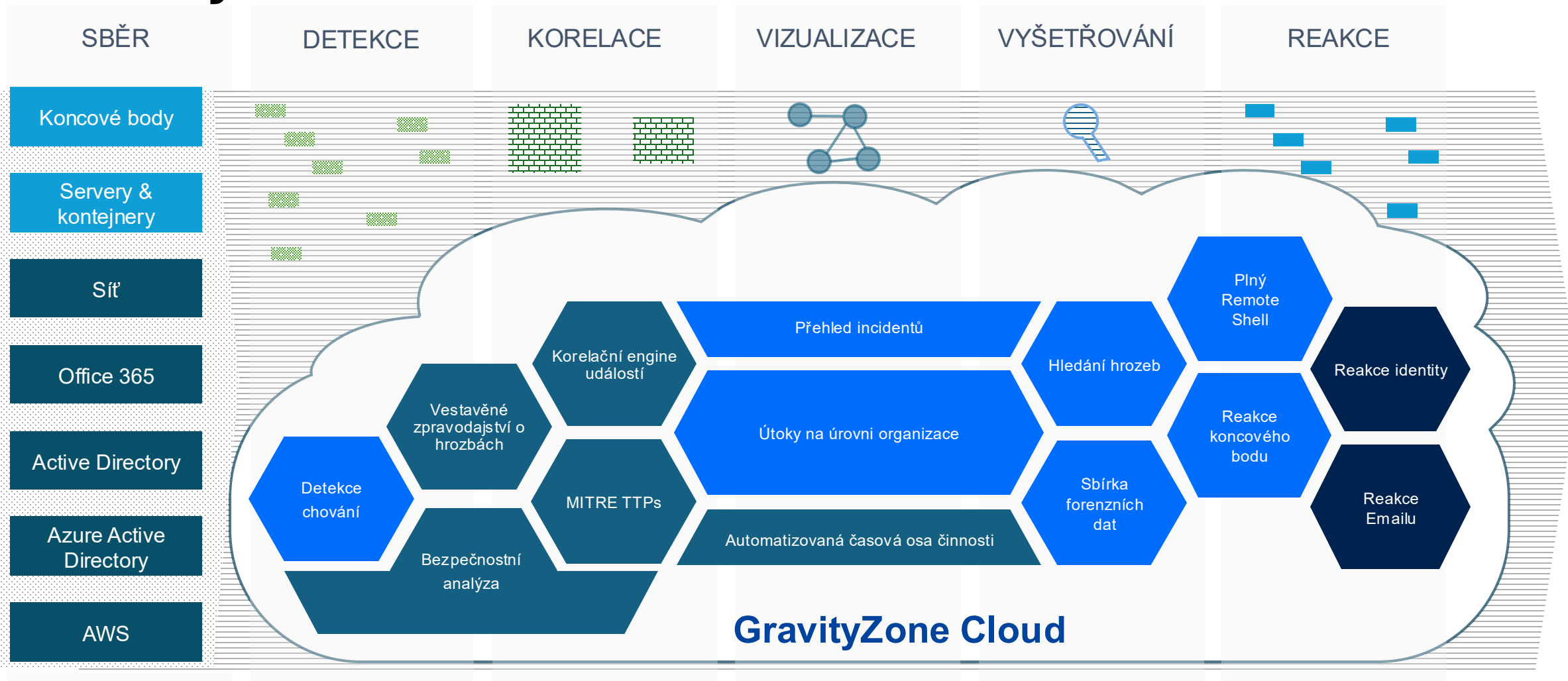


Automatická detekce incidentů , forenzní analýza útoků a korelace napříč celou organizací

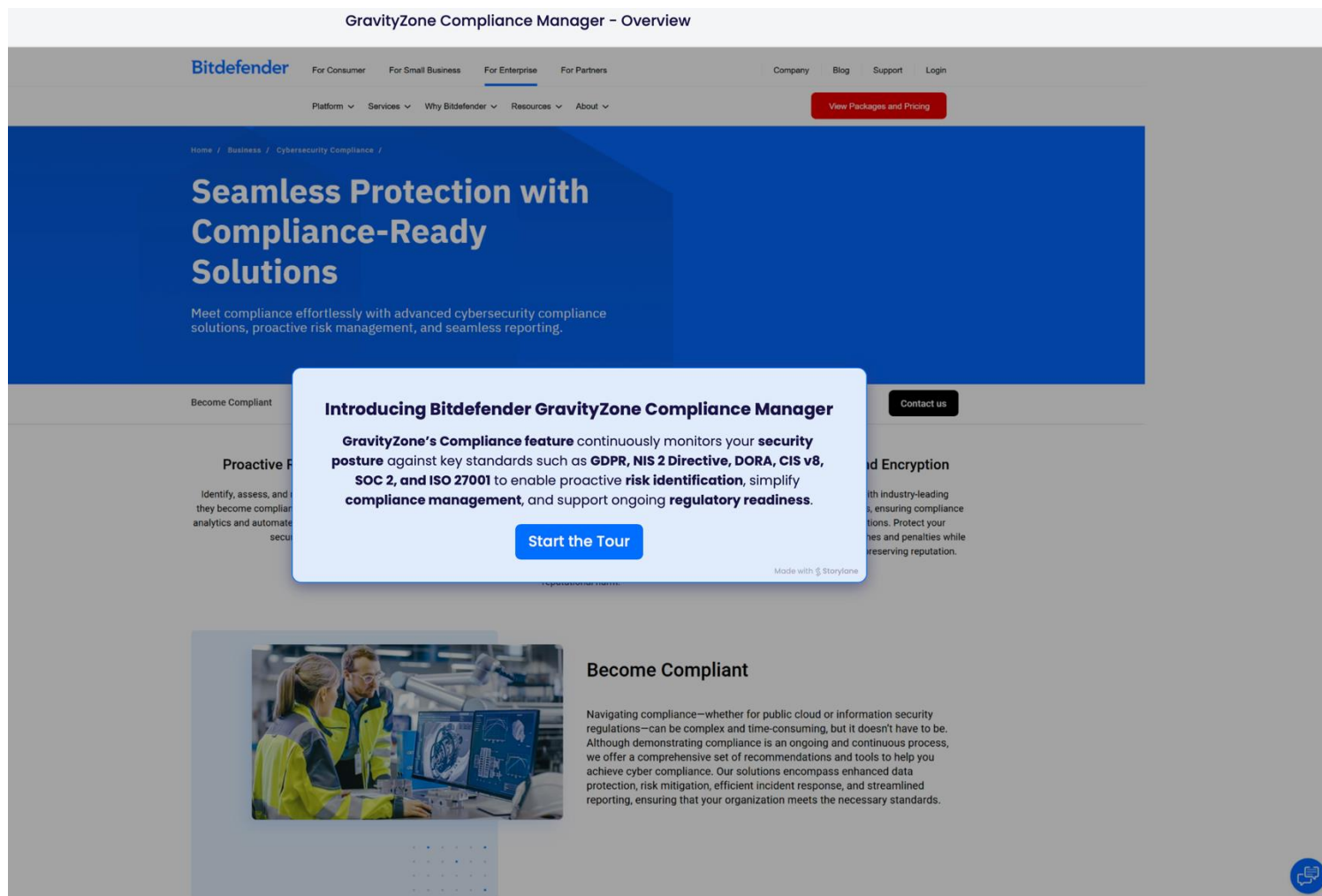
The screenshot displays a comprehensive security dashboard with the following components:

- Incidents List:** A table on the left lists 13 incidents from April 12, 2023, at 16:37. Key incidents include 'Suspicious Email Received', 'VB:Trojan.Valyria.447', 'Suspicious File Write', 'Trojan.Metasploit.A', 'DoubleExtensionExecutableHTTP Query', 'SuspiciousHttpQuery', 'Suspicious HTTP Query', 'SuspiciousDownload', 'ATC.Malicious', 'Generic.Exploit.Shellcode.2.7E50A F52', 'Generic.Exploit.Shellcode.2.2DB5 E90E', 'Exploit.HTTP.ReverseMeterpreter Console.2', and another 'ATC.Malicious' entry.
- Threats Explorer:** A central visualization showing a network of entities and their interactions. Entities include email addresses like 'gesteban.cloud@...', 'alice@bitdefender...', and 'bob@bitdefender...', as well as IP addresses '100.0.0.101' and '204.79.197.203' under 'EXIT POINTS'. Alerts are represented by colored dots and lines indicating relationships, such as 'Suspicious Email Received', 'SuspiciousDownload', 'KerberosBruteForce', and 'Suspicious Login'.
- Alerts and Interactions:** On the right, a panel shows 'ALERTS (0)' with 'No alerts available'. Below it, 'INTERACTIONS WITH (3)' lists entities with their alert counts: 'bob-pc.bitdefender.demo' (2 Alerts), 'gesteban.cloud@gmail.com' (3 Alerts), and 'bob@bitdefenderdemo01.onmicrosoft.com' (4 Alerts).
- Remediation:** A section with buttons for 'Disable User', 'Force credentials reset', and 'Mark user as compromised'.
- Details:** Information for the selected user 'alice@bitdefenderdemo01.onmic...' is shown, including 'Entity type: Azure AD user' and 'Platform: Microsoft Azure Active Directory'.
- Azure User Risk Info:** Shows the 'Level' as 'N/A'.

GravityZone XDR



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



Umožňuje 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

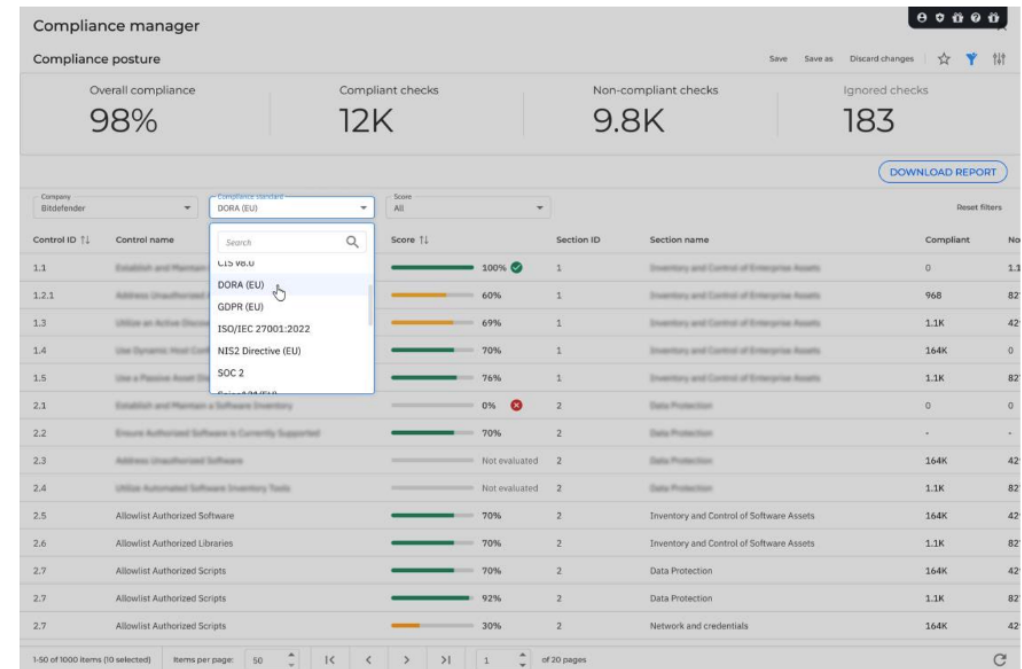
GravityZone Compliance Manager

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



The screenshot displays the 'Compliance manager' interface. At the top, it shows 'Compliance posture' with a summary: Overall compliance 98%, 12K Compliant checks, 9.8K Non-compliant checks, and 183 Ignored checks. Below this is a table of controls. A search dropdown is open, showing options like 'DORA (EU)', 'GDPR (EU)', 'ISO/IEC 27001:2022', 'NIS2 Directive (EU)', and 'SOC 2'. The table columns include Control ID, Control name, Score, Section ID, Section name, Compliant status, and a 'No' column. The table lists various controls such as 'Establish and Maintain a Software Inventory', 'Ensure Authorized Software is Currently Supported', and 'Allowlist Authorized Software', each with a corresponding score and status.

Control ID	Control name	Score	Section ID	Section name	Compliant	No
1.1	Establish and Maintain a Software Inventory	100%	1	Inventory and Control of Enterprise Assets	0	13
1.2.1	Address Unauthorized Software	60%	1	Inventory and Control of Enterprise Assets	968	82
1.3	Utilize an Active Process	69%	1	Inventory and Control of Enterprise Assets	1.1K	42
1.4	Use Dynamic Host Configuration	70%	1	Inventory and Control of Enterprise Assets	164K	0
1.5	Use a Passive Asset Discovery	76%	1	Inventory and Control of Enterprise Assets	1.1K	82
2.1	Establish and Maintain a Software Inventory	0%	2	Data Protection	0	0
2.2	Ensure Authorized Software is Currently Supported	70%	2	Data Protection	-	-
2.3	Address Unauthorized Software	Not evaluated	2	Data Protection	164K	42
2.4	Utilize Automated Software Inventory Tools	Not evaluated	2	Data Protection	1.1K	82
2.5	Allowlist Authorized Software	70%	2	Inventory and Control of Software Assets	164K	42
2.6	Allowlist Authorized Libraries	70%	2	Inventory and Control of Software Assets	1.1K	82
2.7	Allowlist Authorized Scripts	70%	2	Data Protection	164K	42
2.7	Allowlist Authorized Scripts	92%	2	Data Protection	1.1K	82
2.7	Allowlist Authorized Scripts	30%	2	Network and credentials	164K	42

Umožňuje přehledy v reálném čase, Vytváří automaticky audits 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.

PROPRIETARY AND CONFIDENTIAL

Internal Use Only

RESOURCES (5)

FORWARD	✓ 1.6K	✗ 138	○ 537
DISPATCH	✓ 12	✗ 25	○ 5
INTEGRATE	✓ 12		○ 50
INTERMEDIATE			✓ 12
FEEDBACK		Ignored asset	○ 5

[VIEW ALL RESOURCES](#)

IDENTITIES (15)

FE-DEMO\master	✓ 12	✗ 12
FE-DEMO\master	✓ 12	✗ 10
FE-DEMO\Lab.Master		✗ 4
FE\master	✗ 5	○ 5

** 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.

GravityZone Compliance Manager - Reports

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

	Bitdefender GravityZone Compliance Report CIS v8.0 14 May 2025 at 09:26:56 UTC+03:00 FE Lab Compliance standard: CIS v8.0 Reporting Date: 14 May 2025																																																																														
	Executive Summary CHECKS OVERVIEW <table> <tr> <th>Overall compliance</th><th>Total checks</th><th>Checks compliant</th></tr> <tr> <td>73%</td><td>7.8K</td><td>5.6K</td></tr> </table> 40 ignored checks have been excluded when compiling this data. COMPLIANCE CONTROLS OVERVIEW <table> <tr> <th>Controls compliant</th><th>Total controls</th><th>Controls compliant</th></tr> <tr> <td>36%</td><td>47</td><td>17</td></tr> </table> NON-COMPLIANT CHECKS BY RISK SCORE <table> <tr> <th>High</th><th>Medium</th></tr> <tr> <td>1.9K</td><td>157</td></tr> </table>	Overall compliance	Total checks	Checks compliant	73%	7.8K	5.6K	Controls compliant	Total controls	Controls compliant	36%	47	17	High	Medium	1.9K	157	Controls Overview CIS v8.0 14 May 2025 at 09:26:56 UTC+03:00 FE Lab <table> <thead> <tr> <th>ID</th><th>Guideline description</th><th>Score</th><th>Compliant</th><th>Non-compliant</th><th>Ignored*</th></tr> </thead> <tbody> <tr> <td colspan="6">2 Inventory and Control of Software Assets</td></tr> <tr> <td>2.5</td><td>Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.</td><td>49%</td><td>33</td><td>34 20 High 14 Med </td><td>0</td></tr> <tr> <td>2.7</td><td>Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.</td><td>100%</td><td>20</td><td>0</td><td>0</td></tr> <tr> <td colspan="6">3 Data Protection</td></tr> <tr> <td>3.3</td><td>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</td><td>71%</td><td>371</td><td>154 141 High 12 Med 1 Low </td><td>0</td></tr> <tr> <td>3.9</td><td>Encrypt data on removable media.</td><td>55%</td><td>11</td><td>9 9 High </td><td>0</td></tr> <tr> <td>3.10</td><td>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).</td><td>66%</td><td>271</td><td>137 137 High </td><td>0</td></tr> <tr> <td>3.11</td><td>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.</td><td>99%</td><td>320</td><td>1 1 Med </td><td>0</td></tr> <tr> <td>3.12</td><td>Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.</td><td>0% </td><td>0</td><td>7 7 High </td><td>0</td></tr> </tbody> </table> *Ignored findings are being excluded in the compliance score calculation.	ID	Guideline description	Score	Compliant	Non-compliant	Ignored*	2 Inventory and Control of Software Assets						2.5	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	49%	33	34 20 High 14 Med	0	2.7	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	100%	20	0	0	3 Data Protection						3.3	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	71%	371	154 141 High 12 Med 1 Low	0	3.9	Encrypt data on removable media.	55%	11	9 9 High	0	3.10	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	66%	271	137 137 High	0	3.11	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	99%	320	1 1 Med	0	3.12	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	0% 	0	7 7 High	0	
Overall compliance	Total checks	Checks compliant																																																																													
73%	7.8K	5.6K																																																																													
Controls compliant	Total controls	Controls compliant																																																																													
36%	47	17																																																																													
High	Medium																																																																														
1.9K	157																																																																														
ID	Guideline description	Score	Compliant	Non-compliant	Ignored*																																																																										
2 Inventory and Control of Software Assets																																																																															
2.5	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	49%	33	34 20 High 14 Med	0																																																																										
2.7	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	100%	20	0	0																																																																										
3 Data Protection																																																																															
3.3	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	71%	371	154 141 High 12 Med 1 Low	0																																																																										
3.9	Encrypt data on removable media.	55%	11	9 9 High	0																																																																										
3.10	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	66%	271	137 137 High	0																																																																										
3.11	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	99%	320	1 1 Med	0																																																																										
3.12	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	0% 	0	7 7 High	0																																																																										

PDF sample

3 / 12

Bitdefender GravityZone Compliance Report		Company: FE Lab Standard: CIS v8.0											
CIS v8.0	Date:	14 May 2025 at 06:27:07 UTC+00:00											
	Assets:	Resources involved: 20 Windows, 7 Linux											
		Resources ignored:											
		Identities involved:											
		Identities ignored:											
Checks overview		Compliance controls overview											
Overall compliance*		73.00% Controls compliant*		36.00%									
Total checks *		7856 Total controls*		47									
Compliant checks		5699 Compliant controls		17									
Non-compliant checks		2157 Non-compliant controls		30									
Ignored checks		40 Not evaluated controls		0									
Legend													
Score													
100% ✓	Controls that passed all their checks when performed by GravityZone on applicable scopes are marked green and a check mark. Additional verification may be required to fulfill control requirements.												
80%	Controls that passed between 71% and 99% of their checks when performed by GravityZone on applicable scopes, are marked green.												
50%	Controls that passed between 24% and 70% of their checks when performed by GravityZone												
25%													
0% ✗													
Not evaluated													
*													
Bitdefender GravityZone Compliance Report		Company: FE Lab Standard: CIS v8.0											
				Score Breakdown		Checks Breakdown							
Item	ID	Outline description	Score	2 - Inventory and Control of Software Assets									
1	2.5	Use technical controls, such as application whitelisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	80% ✓	27 Checks / 33 Compliant / 38 Non-Compliant / 3 Ignored		Verifies the local group policy Prevent installation of devices that match any of these device IDs, located in Computer Configuration\Administrative Templates\SystemDevice Installation\Device Installation Restrictions.	13 Compliant / 7 Non-Compliant / 0 Ignored						
						Verifies the local group policy Prevent installation of devices using drivers that match these device setup classes, located in Computer Configuration\Administrative Templates\SystemDevice Installation\Device Installation Restrictions.	13 Compliant / 7 Non-Compliant / 0 Ignored						
						Verifies the local group policy Allow software to run or install even if the signature is invalid, located in Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Pages.	9 Compliant / 20 Non-Compliant / 0 Ignored						
						AppLocker must be enabled at all times in your build configuration to ensure that the controls it provides are not overridden.	7 Compliant / 8 Non-Compliant / 0 Ignored						
2	2.7	Use technical controls, such as digital signatures and version controls, to ensure that only authorized scripts, such as specific .ps1, .ps2, etc. files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	100% ✓	28 Checks / 30 Compliant / 0 Non-Compliant / 0 Ignored		Checks the local group policy Turn on Script Execution, located in Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell.	20 Compliant / 0 Non-Compliant / 0 Ignored						
						This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run.							
7	3.12	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	0% ✗	3 - Data Protection		Verifies that BitLocker is configured by either mounting implicitly or a separate partition to hmg. Making hmg is on the system allows an administrator to set the recovery option on the mount, rendering time useless in case an attacker attempts to install executable code.	0 Compliant / 0 Non-Compliant / 0 Ignored						
8	3.13	Implement an automated tool, such as a Host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located on-site or at a remote service provider, and update the	0% ✗	7 Checks / 0 Compliant / 7 Non-Compliant / 0 Ignored		Verifies that USB-connections is disabled. Restricting USB access on the system will decrease the physical attack surface for a device.	0 Compliant / 7 Non-Compliant / 0 Ignored						
9	4.1	Establish and maintain a secure configuration process for enterprise assets (per-server devices, including portable and mobile, non-computing/IOT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Subgroup.	24% ✓	4 - Secure Configuration of Enterprise Assets and Software		Verifies the local group policy settings for User Configuration\Administrative Templates\System\Computer\Task Manager\Task Manager.	20 Compliant / 0 Non-Compliant / 0 Ignored						
						When Windows Task Manager is enabled, the endpoint is vulnerable to security threats. Since Task Manager is Windows requires account sign-in. When the user accounts control is disabled, Windows stores the user passwords in the registry database, making possible to bypass the password screen during login.	20 Compliant / 0 Non-Compliant / 0 Ignored						
						Verifies the local security policy interactive logon. Do not require CTRL+ALT+DEL. This option defines whether users must enter their computer before logging into Windows by pressing CTRL+ALT+DEL, as an additional security layer that prevents malware intercepting	20 Compliant / 0 Non-Compliant / 0 Ignored						
						Verifies the local security policy option User Account Control. Run all administrators in Admin Approval Mode.	20 Compliant / 0 Non-Compliant / 0 Ignored						
						This setting controls the behavior of all UAC policy settings for the endpoint.							
						Verifies the configuration for User Account Control policy and registry settings, to check if they comply with the default recommended settings.	20 Compliant / 0 Non-Compliant / 0 Ignored						
						The policy settings are located in Security\Background\Policy\Security Options, in the Local							



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

Bitdefender[®]
BUILT FOR RESILIENCE

ChannelWorld

číslo 2 - červen 2024 | ročník XVI | cena: 100 Kč / 4,3 €

Časopis pro resellery a VAR

Stavíme na důvěře a hodnotách

René Pospíšil z IS4 security
o budování bezpečnostního
ekosystému

Čtete na straně 10

Kulatý stůl: Lepší zůstanou

Vymodlené oživení trhu PC

Katalog distributorů

+ Resellerův průvodce
s přehledem ICT distributorů v ČR a SR