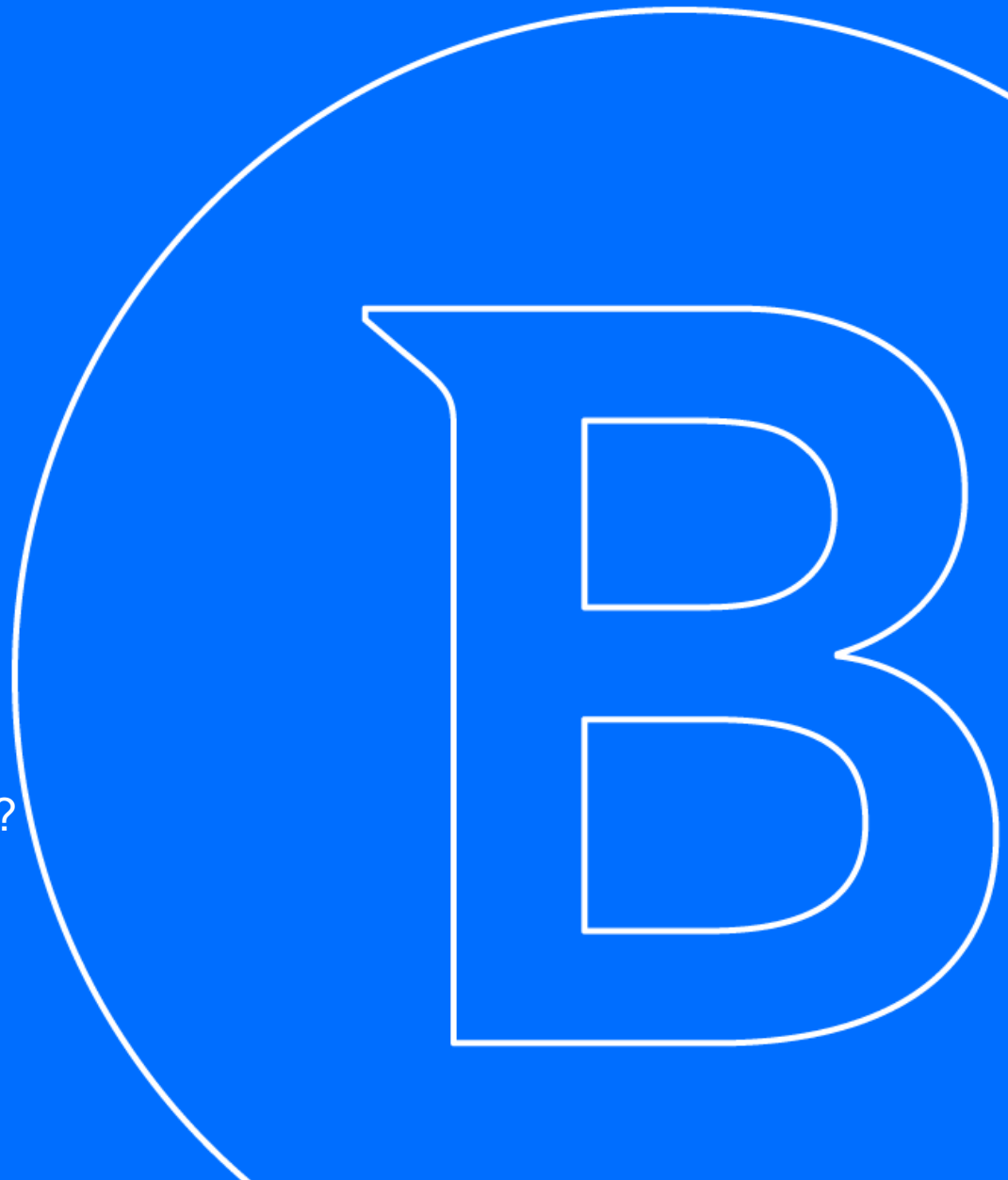
Global Leader In
Cybersecurity

Bitdefender®

ŠKODLIVÝ KÓD = VIRUS -
JE VŮBEC V DOBĚ AI JEŠTĚ ZAPOTŘEBÍ?

Jiří Hasala– Sales Director, Bitdefender CZ&SK



Bitdefender

GLOBAL
CYBERSECURITY COMPANY

Založena v roce 2001
1800+ zaměstnanců

Centrála a vývoj v Europe
HQ Rumunsko, USA
17 regionalních poboček napříč Evropou, USA, Asií a Austrálií

35,000+ distributorů, prodejců

TRUSTED
SECURITY TECHNOLOGY PROVIDER

180+ technologických OEM partnerů

Spolupráce s bezpečnostními složkami ve **27** zemích, včetně Europol a FBI

Gartner Peer Insights **Customers' Choice** for Voc EPP in EMEA

CRN 5-star 9 let v řadě za sebou

AV-Comparatives 20 let partnerství

INNOVATIVE
ENDPOINT SECURITY

+16 roků AI Inovací

487+ patentů

32+ zveřejněných ransomware decryptorů. **$1.6B** ušetřeno obětem ransomware

AWARDED
INDUSTRY LEADER

Bitdefender

Bitdefender GravityZone Packages

GRAVITYZONE DEFENSE XDR

GRAVITYZONE BUSINESS SECURITY ENTERPRISE

GRAVITYZONE BUSINESS SECURITY PREMIUM

GRAVITYZONE BUSINESS SECURITY

- WEB AND CONTENT CONTROL & FILTERING
- DEVICE CONTROL
- APPLICATION CONTROL
- ENDPOINT & USER RISK ANALYSIS
- CLOUD SECURITY POSTURE MANAGEMENT ADD-ON
- PHASR ADD-ON
- COMPLIANCE MANAGER ADD-ON
- EASM ADD-ON
- PATCH MANAGEMENT ADD-ON
- FULL DISK ENCRYPTION ADD-ON
- RANSOMWARE MITIGATION
- EXPLOIT DEFENSE
- PROCESS PROTECTION
- NETWORK ATTACK DEFENSE
- FILELESS ATTACK DEFENSE
- SANDBOX ANALYSIS
- TUNABLE MACHINE LEARNING
- ATTACK FORENSICS
- SECURITY FOR EMAIL ADD-ON
- SECURITY FOR MOBILE ADD-ON
- SECURITY FOR CONTAINERS ADD-ON
- SECURITY FOR STORAGE ADD-ON
- INTEGRITY MONITORING ADD-ON
- INCIDENT ADVISOR
- INCIDENT VISUALIZATION
- GUIDED RESPONSE
- LIVE SEARCH
- ANOMALY DEFENSE
- EXTENDED DETECTION AND RESPONSE
  - IDENTITY
  - PRODUCTIVITY
  - NETWORK
- XDR SENSORS
  - CLOUD ADD-ON
  - BUSINESS APPS (ATLASIAN) ADD-ON
- MANAGED DETECTION AND RESPONSE
- PREMIUM SUPPORT SERVICES
- ADVISORY AND DEPLOYMENT SERVICES

PREVENTION | PROTECTION | DETECTION AND RESPONSE

DATA ANALYTICS & RETENTION | LOCAL & CLOUD MACHINE LEARNING | MALWARE DETECTION | ANOMALY DETECTIONS | THREAT INTELLIGENCE | CONFIGURATION MANAGEMENT | VULNERABILITY IDENTIFICATION | AUTOMATION & ORCHESTRATION | DASHBOARDS & REPORTING | INTEGRATION APIs

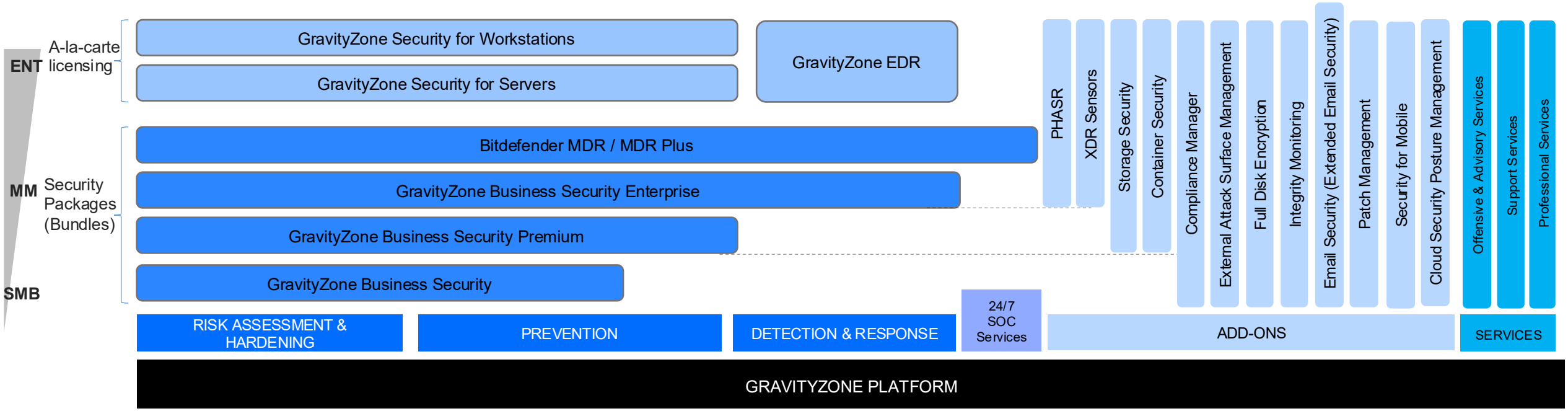
GRAVITYZONE PLATFORM

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

Produkty

	Business Security	Business Security Premium	Business Security Enterprise
PREVENTION & PROTECTION CAPABILITIES			
Endpoint Risk Analytics	V cloud only	V cloud only	V cloud only
Web Threat Protection	V	V	V
Device Control	V	V	V
Application Control (Black-listing)	V	V	V
Application Control (Whitelis-ting)	V	V on-premise only	V on-premise only
Firewall for Windows Endpoints	V	V	V
Local and Cloud Machine Learning	V	V	V
Exploit Defense	V	V	V
Automatic Disinfection and Removal	V	V	V
Network Attack Defense	V	V	V
Process Protection	V	V	V
Ransomware Mitigation	V	V	V
Fileless Attack Defense	X	V	V
HyperDetect (Tunable Machine Learning)	-	V	V
Sandbox Analysis	-	V	V
Attack Forensics	-	V	V
ENDPOINT DETECTION AND RESPONSE CAPABILITIES			
Cross-endpoint correlation	-	-	V
Anomaly Defense	-	-	V
Endpoint Incident Visualization	-	V (limited)	V
Live and Historical Search	-	-	V
MITRE Event Tagging (TTPs)	-	-	V
Response recommendations	-	-	V
Endpoint response	-	-	V
EXTENDED DETECTION AND RESPONSE CAPABILITIES			
Cross-source event correlation	-	-	+ Requires XDR (cloud only)
Organization-level incident visualization	-	-	+ Requires XDR (cloud only)
Incident Advisor	-	-	+ Requires XDR (cloud only)
Cross-organization response	-	-	+ Requires XDR (cloud only)

Bundles & Add-ons



Ostatní:

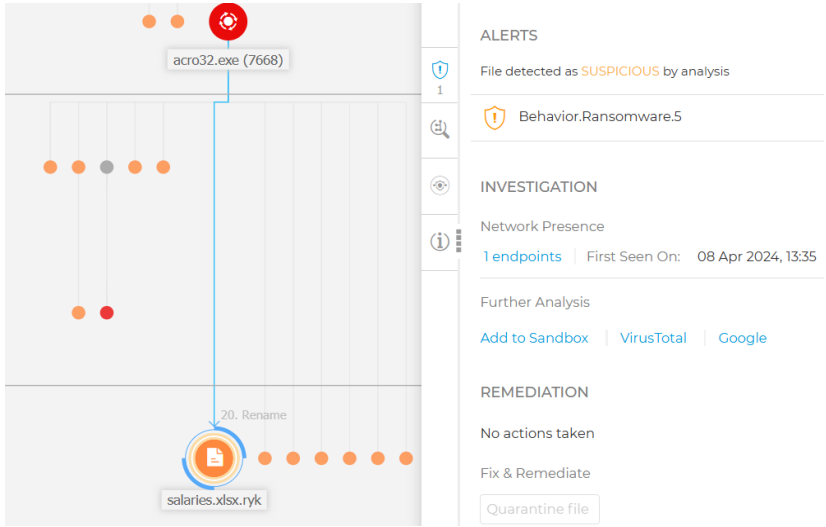
- Thread Intelligence (TI) / IntelliZone for B2B.
- Security for AWS.

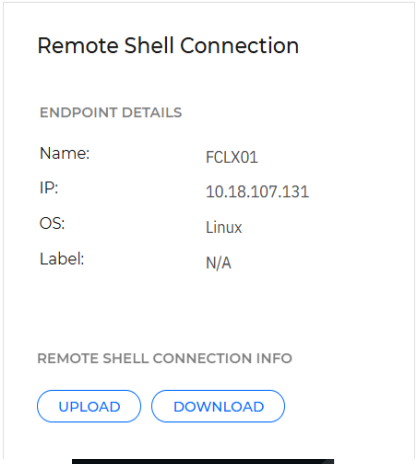
Bitdefender

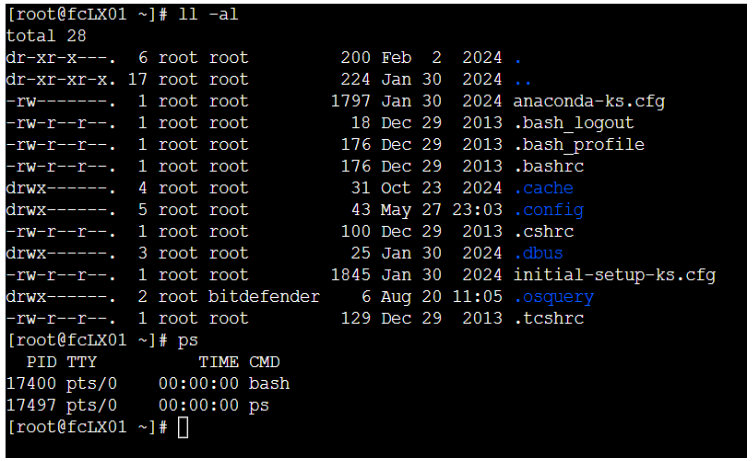
GravityZone EDR

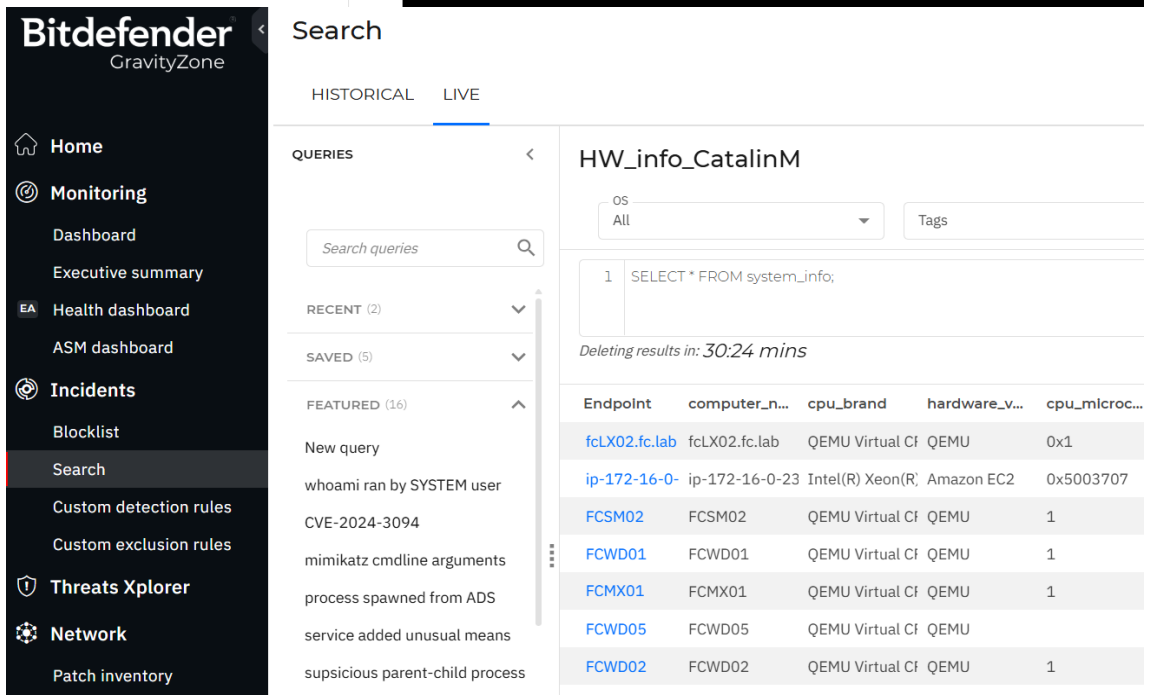
KOMPLEXNÍ ŘEŠENÍ ÚTOKŮ A JEJICH SPRÁVA

ENDPOINT DETECTION AND RESPONSE CAPABILITIES
Cross-endpoint correlation
Anomaly Defense
Endpoint Incident Visualization
Live and Historical Search
MITRE Event Tagging (TTPs)
Response recommendations
Endpoint response





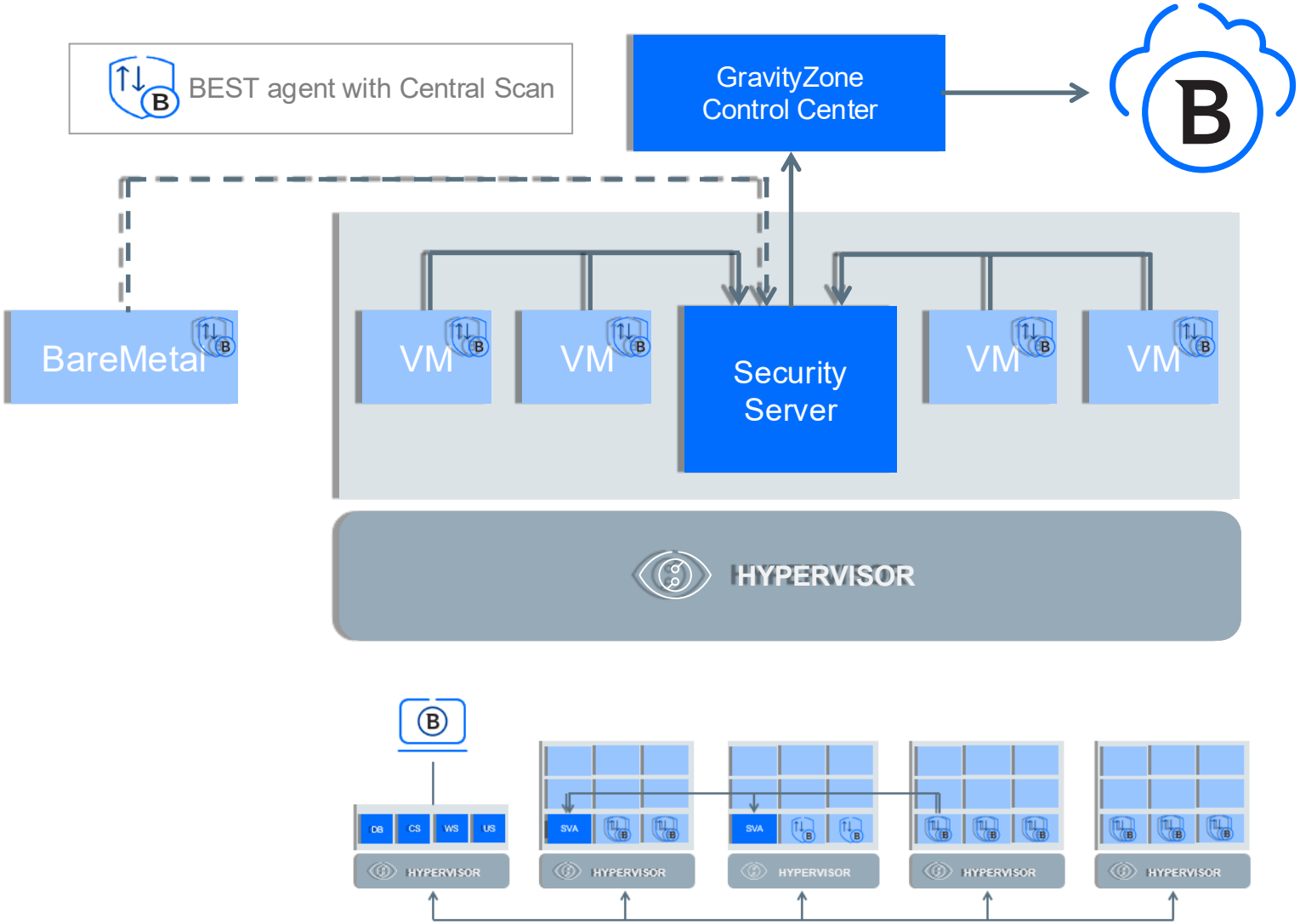




Anomaly Defense Tato funkce je součástí naší technologie strojového učení a umělé inteligence v rámci řešení pro detekci a reakci na hrozby v koncových bodech (EDR). Využíváme různé algoritmy založené na strojovém učení a statistice, přičemž trénování modelu pro **ochranu před anomáliemi probíhá převážně v prostředí zákazníka** (na koncových bodech a serverech). **V zásadě má každý zákazník svůj vlastní model, který se v průběhu času vyvíjí** (a je tedy průběžně přizpůsobován).

Bitdefender

Security for Virtualized Env.



- Bitdefender oceňovaná technology (ML/AI, AM, HyperDetect)
- **Central Scan** slouží ke snížení zatížení VMs, chytrá ochrana virtualizace a HW slabých strojů)
- Nízký dopad na výkon
- Předcházení AV bouřím
- Kompletní ochrana virtualizovaných farem
- Podpora více platforem & flexibilní nasazení architektury

ŠKODLIVÝ KÓD
=
VIRUS

JE VŮBEC V DOBĚ AI JEŠTĚ ZAPOTŘEBÍ ?

Proč by měl útočník vymýšlet nový virus, když má v operačním systému dost nástrojů na to, aby jejich pomocí útok provedl a „nebyl“ odhalen

LIVING OFF THE LAND

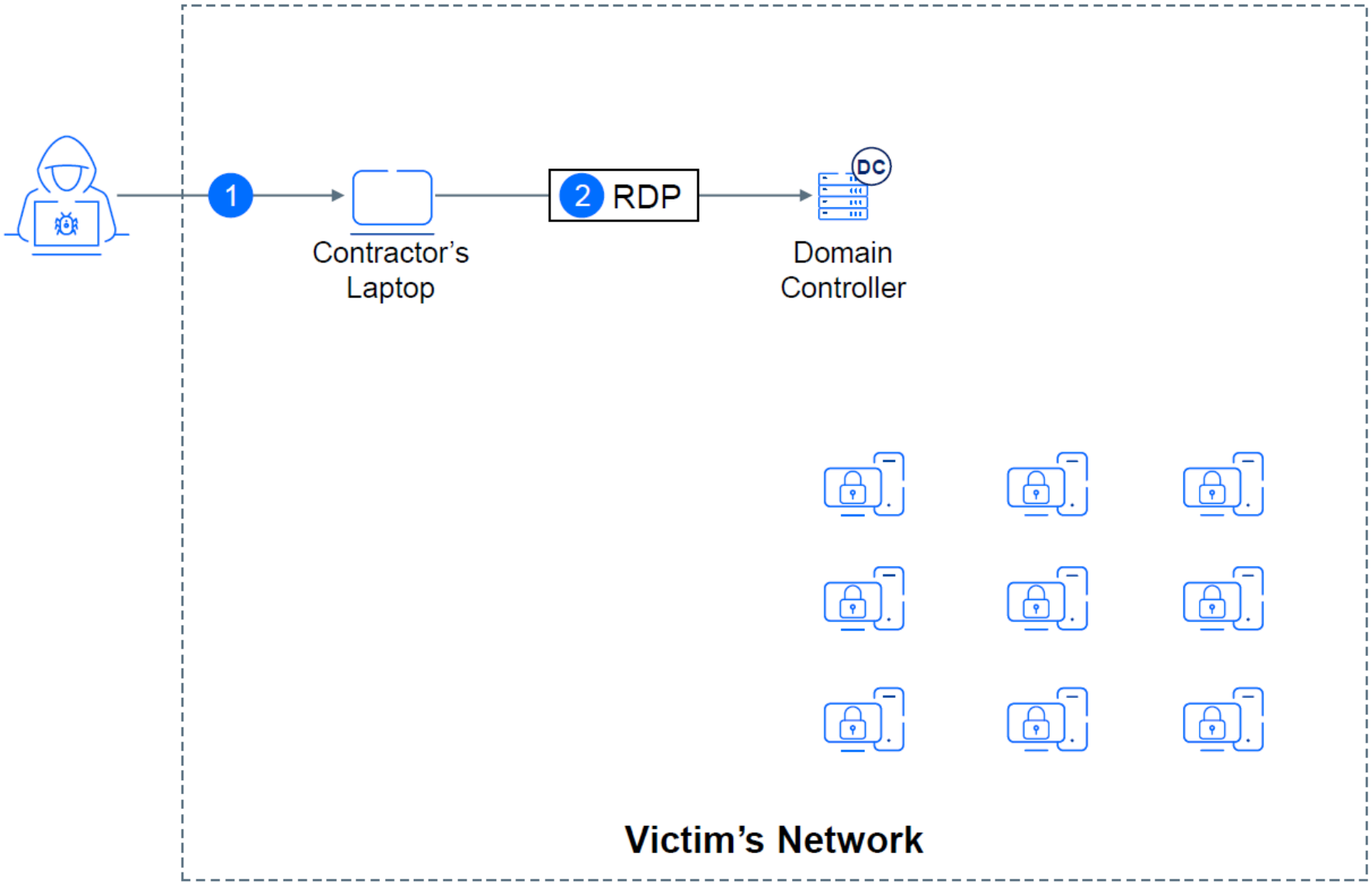
Shrinklocker

Ransomware

Case Study

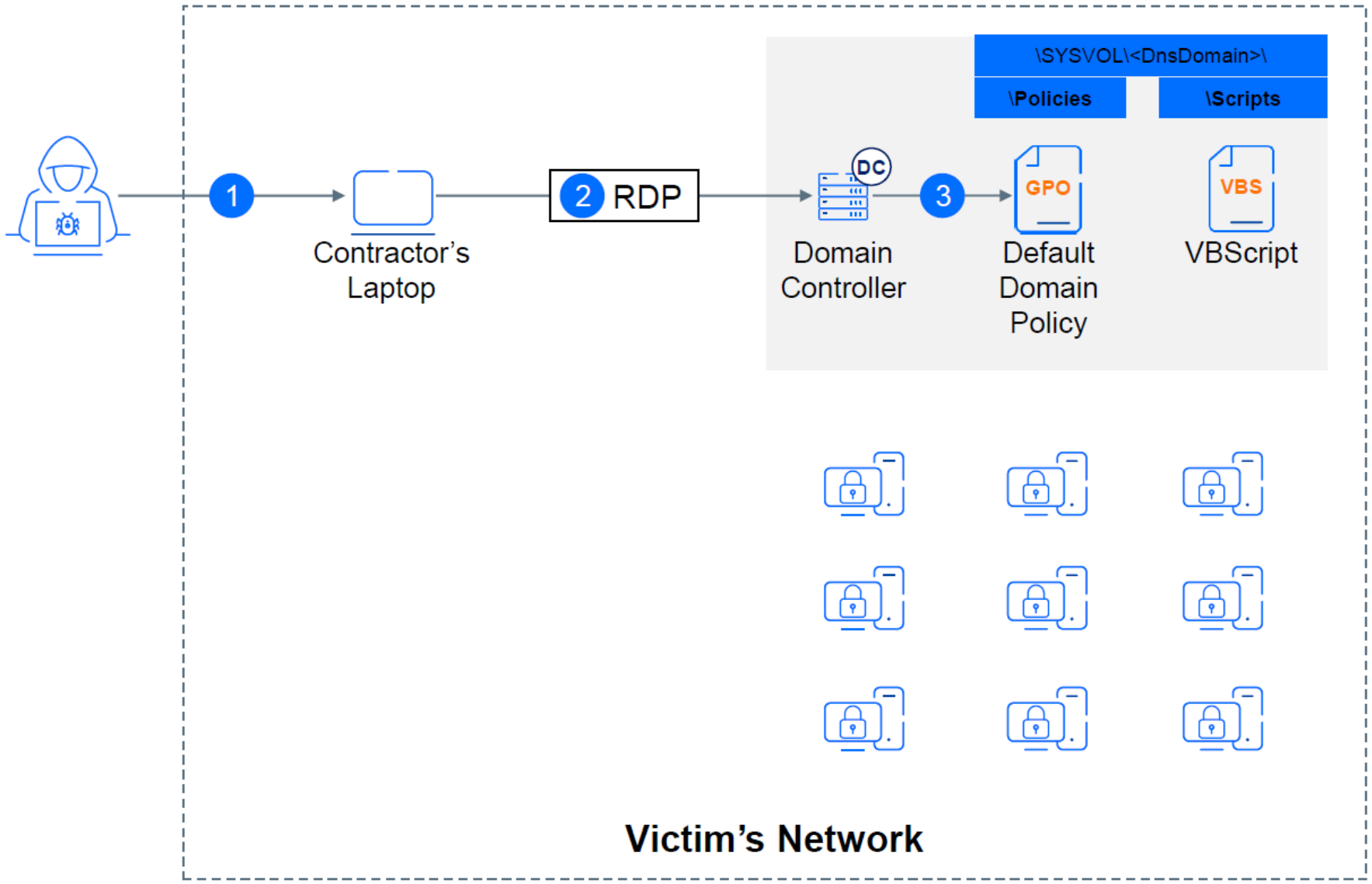
Bitdefender

Bitdefender



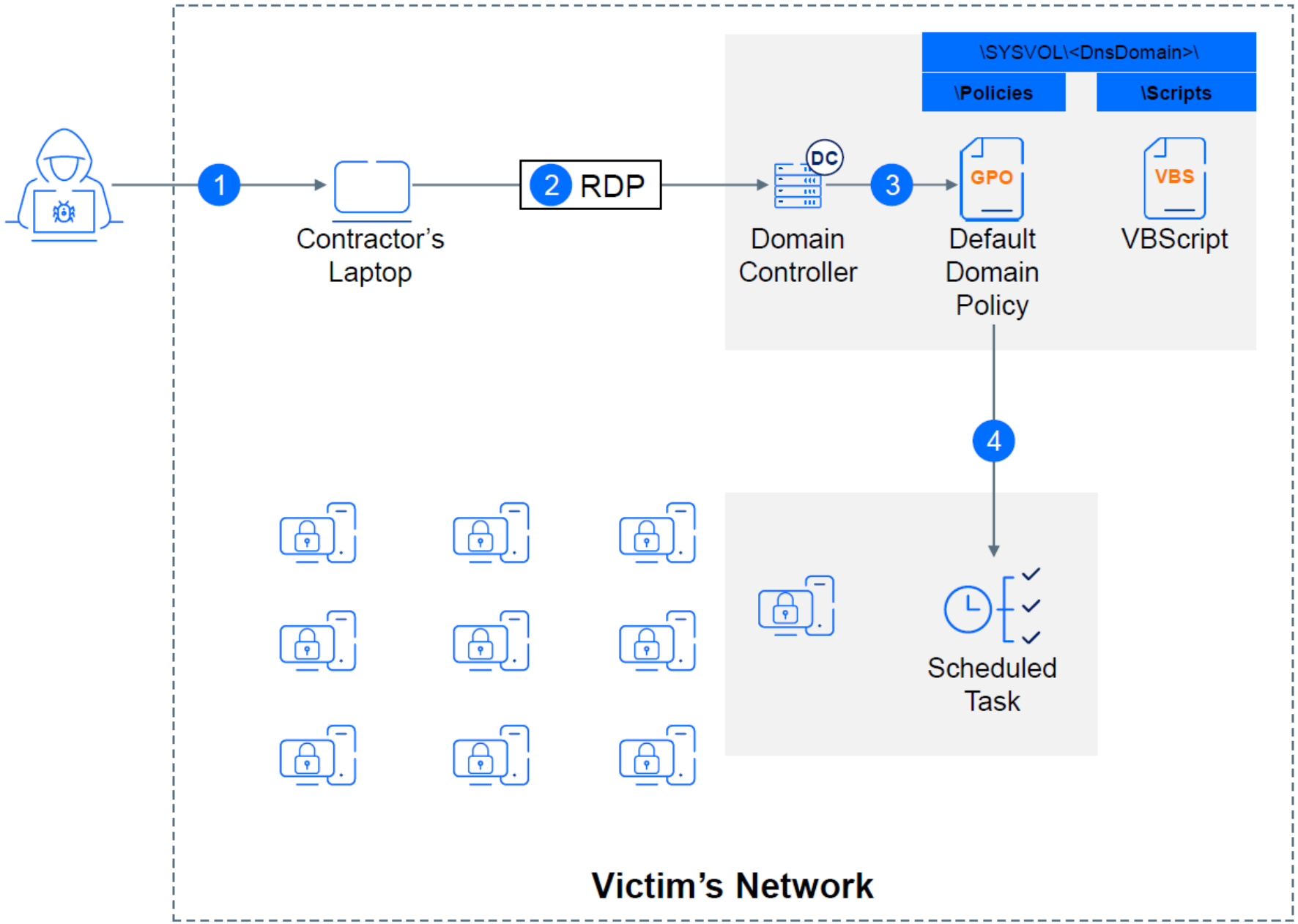
1. Attackers gained access to a contractor's laptop.
2. Using stolen credentials, attackers compromised the Domain Controller.

Bitdefender



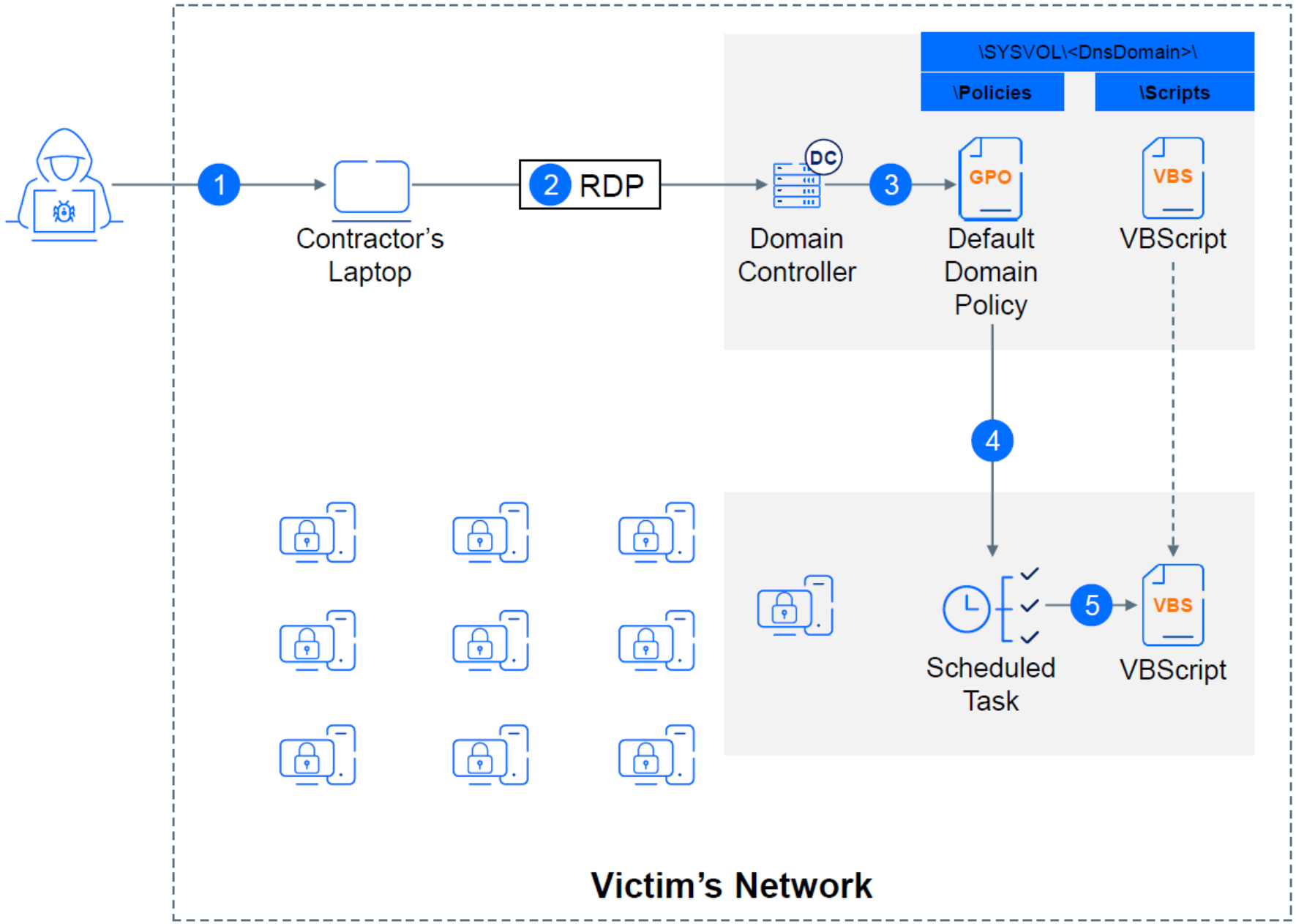
1. Attackers gained access to a contractor's laptop.
2. Using stolen credentials, attackers compromised the Domain Controller.
3. Attackers modified domain policies and deployed scripts to a shared location.

Bitdefender



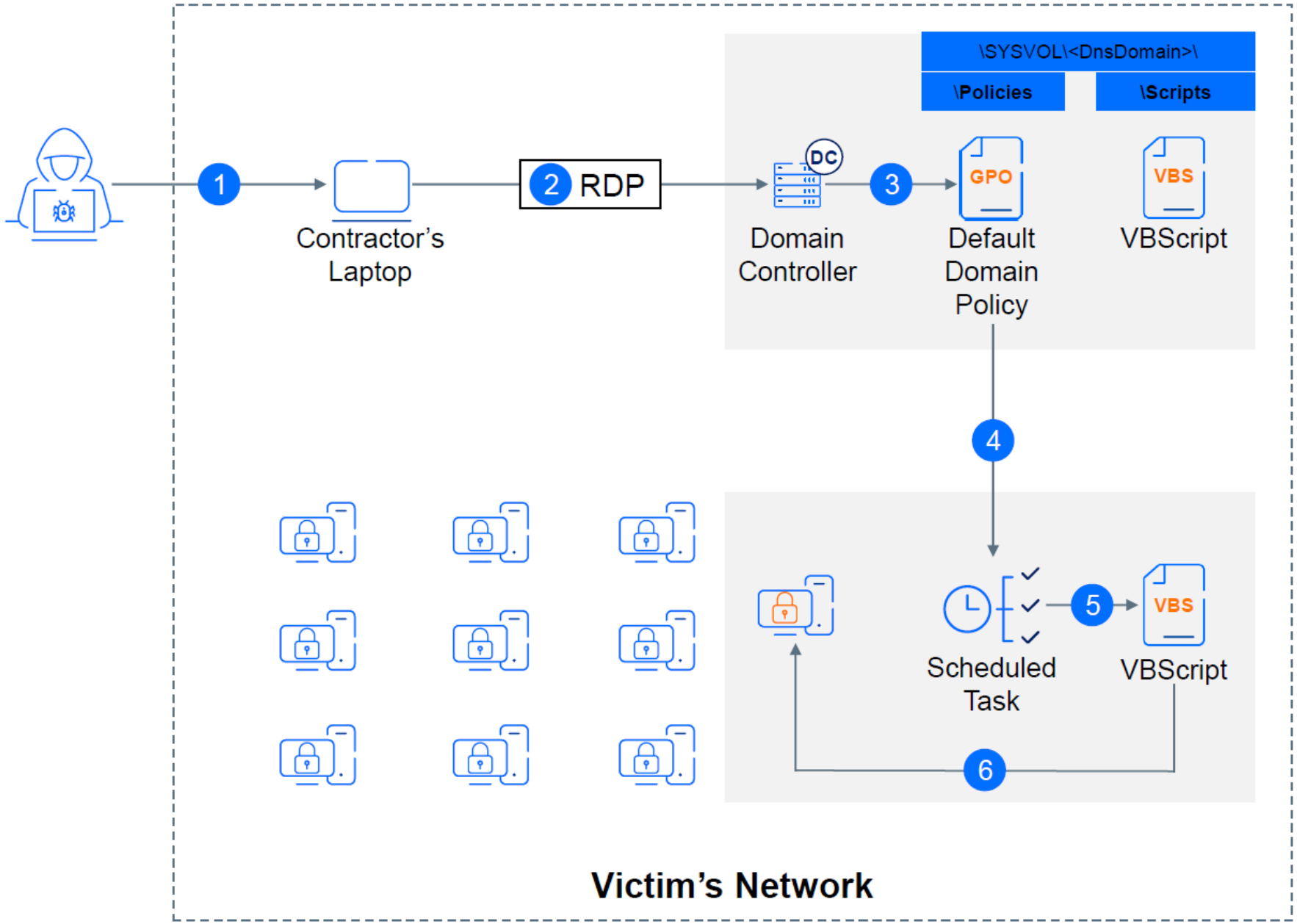
1. Attackers gained access to a contractor's laptop.
2. Using stolen credentials, attackers compromised the Domain Controller.
3. Attackers modified domain policies and deployed scripts to a shared location.
4. GPO policy created scheduled tasks on all domain machines.

Bitdefender



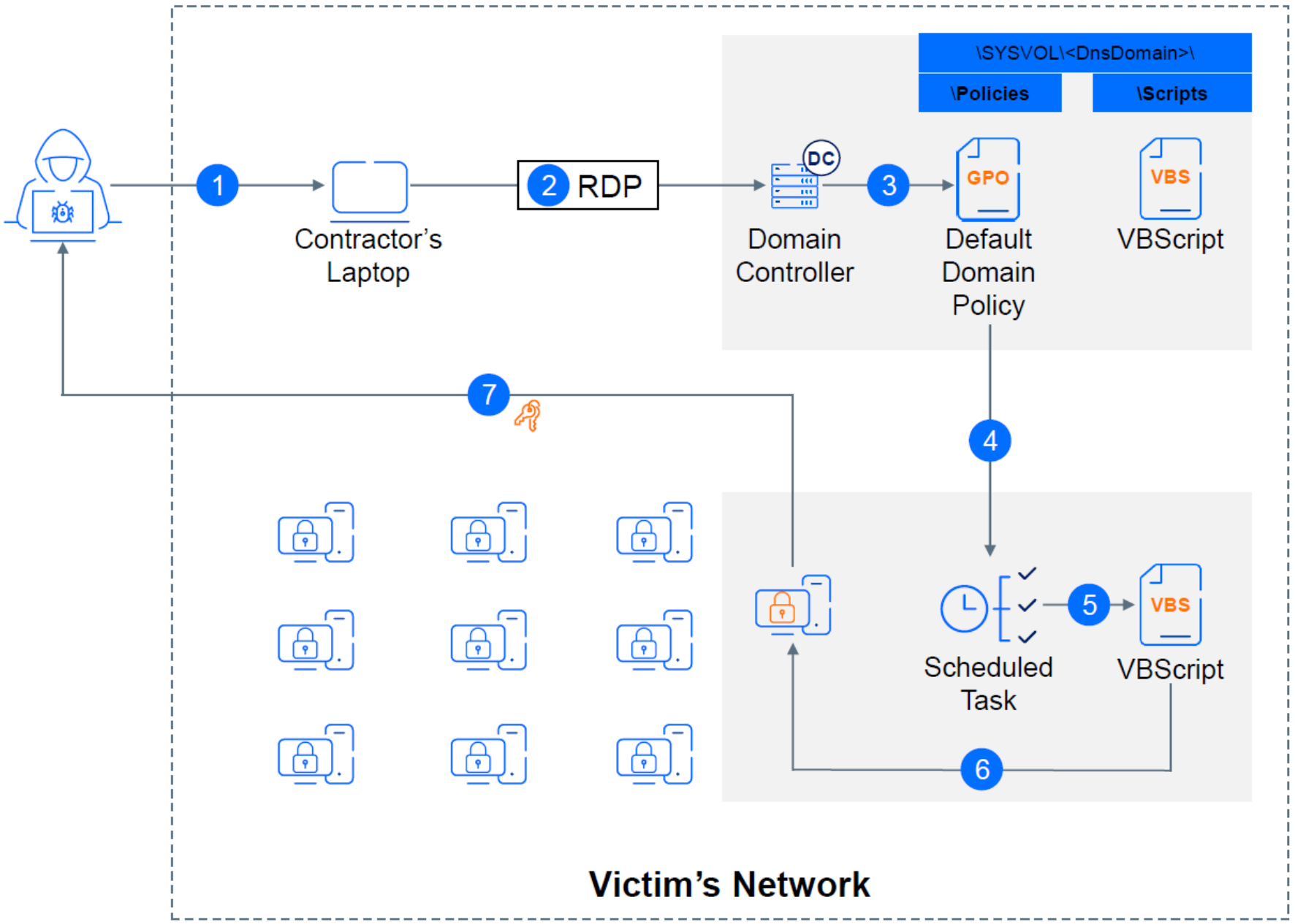
1. Attackers gained access to a contractor's laptop.
2. Using stolen credentials, attackers compromised the Domain Controller.
3. Attackers modified domain policies and deployed scripts to a shared location.
4. GPO policy created scheduled tasks on all domain machines.
5. Scheduled tasks executed the scripts locally.

Bitdefender



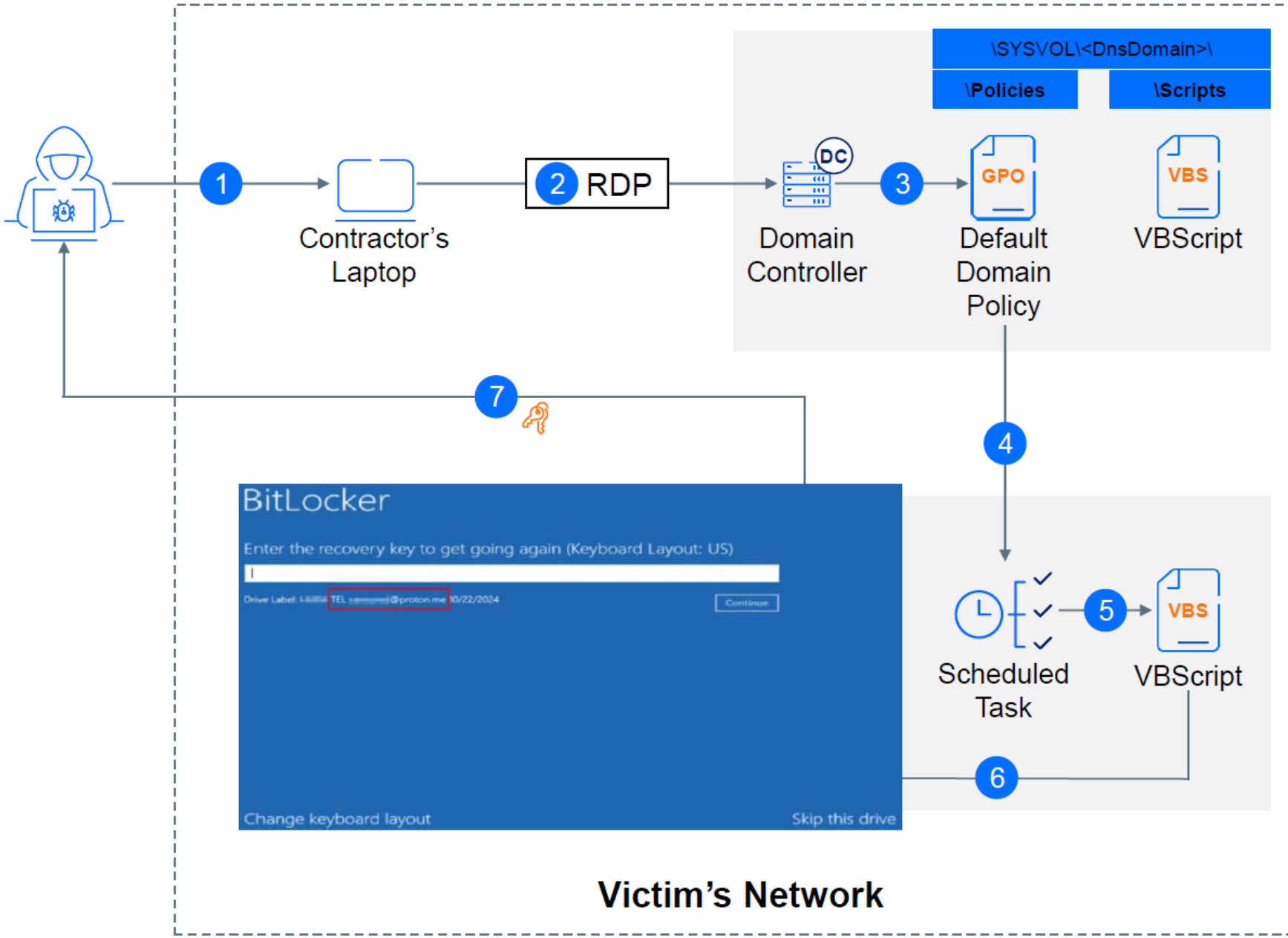
1. Attackers gained access to a contractor's laptop.
2. Using stolen credentials, attackers compromised the Domain Controller.
3. Attackers modified domain policies and deployed scripts to a shared location.
4. GPO policy created scheduled tasks on all domain machines.
5. Scheduled tasks executed the scripts locally.
6. Scripts reset **BitLocker** encryption and changed passwords to random string.

Bitdefender



1. Attackers gained access to a contractor's laptop.
2. Using stolen credentials, attackers compromised the Domain Controller.
3. Attackers modified domain policies and deployed scripts to a shared location.
4. GPO policy created scheduled tasks on all domain machines.
5. Scheduled tasks executed the scripts locally.
6. Scripts reset **BitLocker** encryption and changed passwords to random string.
7. The new passwords are uploaded to a command-and-control (C2) server.

Bitdefender



1. Attackers gained access to a contractor's laptop.
2. Using stolen credentials, attackers compromised the Domain Controller.
3. Attackers modified domain policies and deployed scripts to a shared location.
4. GPO policy created scheduled tasks on all domain machines.
5. Scheduled tasks executed the scripts locally.
6. Scripts reset **BitLocker** encryption and changed passwords to random string.
7. The new passwords are uploaded to a command-and-control (C2) server.

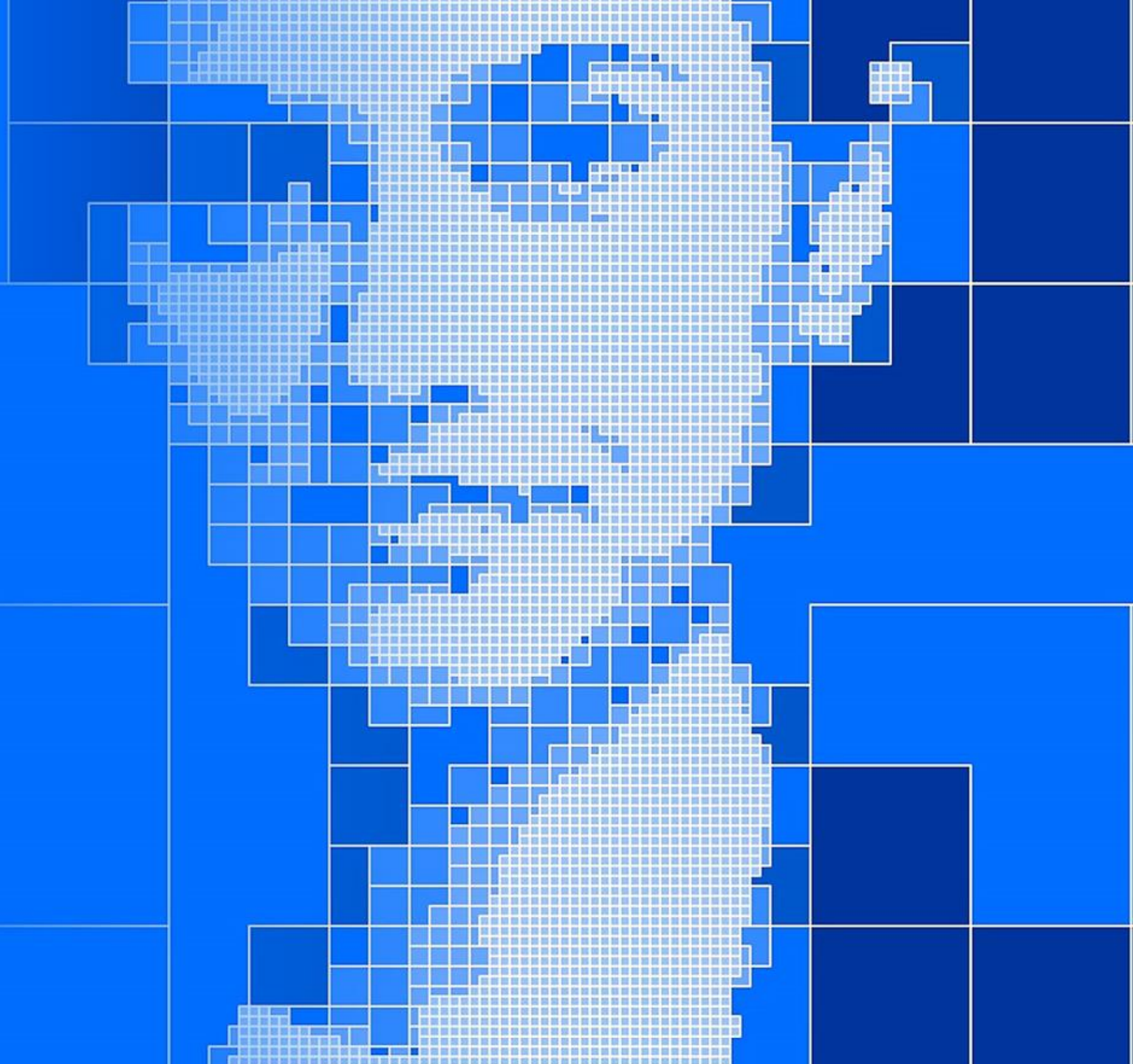
Ochrání vás proti těmto typům útoku antivirus ?

NE

Bitdefender Global Leader In Cybersecurity

Představujeme GravityZone

PHASR



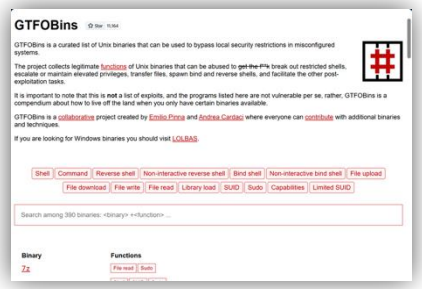
Bitdefender

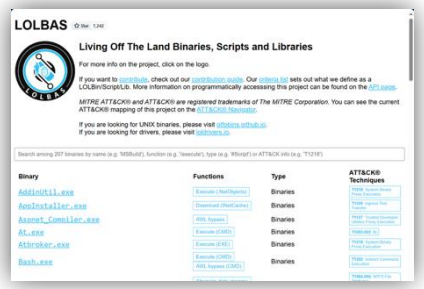
Útočníci využívají legitimní nástroje operačních systémů

84% závažných incidentů se nyní týká Living off the Land (LotL) – technika, při které útočníci zneužívají legitimní nástroje, které jsou již v systému k dispozici

Útočníci opakovaně používají úspěšné vzorce útoků v různých systémech

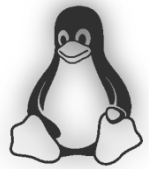
Zbytečná útočná plocha – stovky rizikových legitimních nástrojů, které uživatelé nevyužívají, ale které využívají útočníci





200+

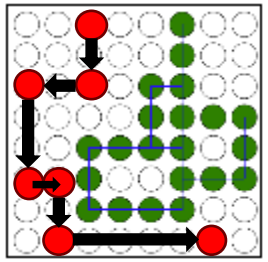
Binárních souborů Windows zneužité útočníky



Bitdefender

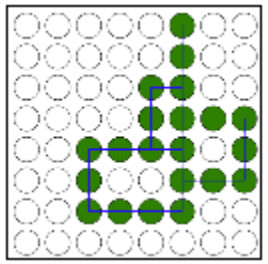
PHASR konkurenční výhoda

Útočník

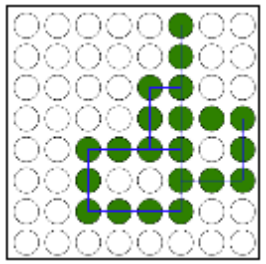


Vzor útoku identifikovaný útočníkem

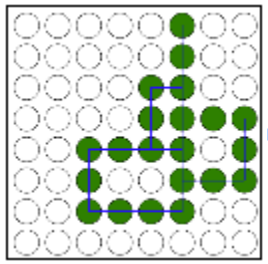
Společnost X chráněna produktem A



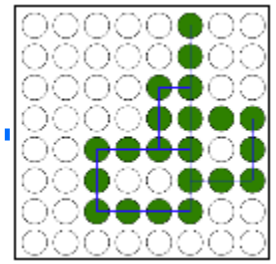
Ochrana potenciální oblasti útoku uživatel 1



Ochrana potenciální oblasti útoku uživatel 2

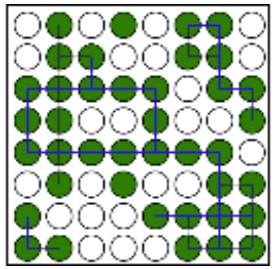


Ochrana potenciální oblasti útoku uživatel 3

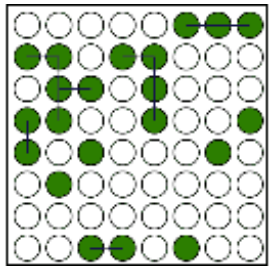


Ochrana potenciální oblasti útoku uživatele

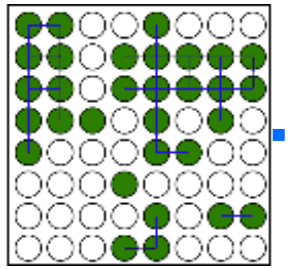
Společnost X chráněna PHASR



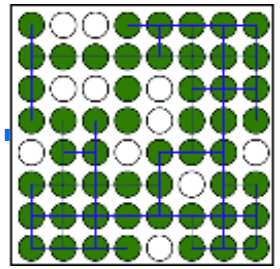
Ochrana potenciální oblasti útoku uživatel 1



Ochrana potenciální oblasti útoku uživatel 2



Ochrana potenciální oblasti útoku uživatel 3

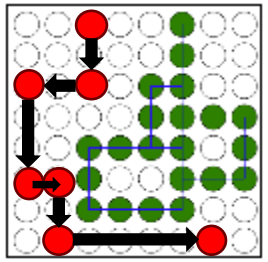


Ochrana potenciální oblasti útoku uživatele

Bitdefender

PHASR konkurenční výhoda

Útočník



Vzor útoku identifikovaný útočníkem

Company X protected by Product A

Takto vypadá PHASR v realitě
(neustále se mění a vyvíjí)

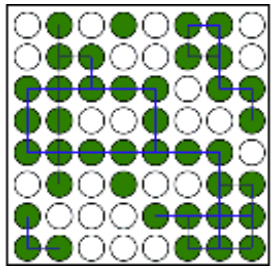
$User_1$ Attack Surface Protection

$User_2$ Attack Surface Protection

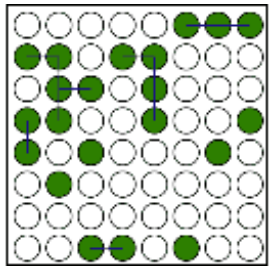
$User_3$ Attack Surface Protection

$User_n$ Attack Surface Protection

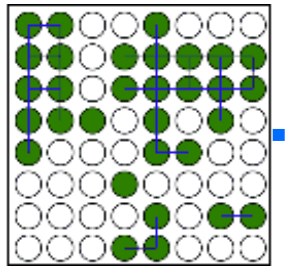
Company X protected by PHASR



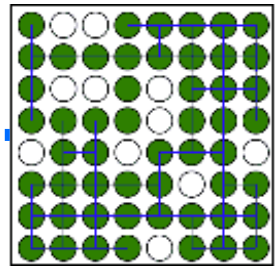
Ochrana potenciální oblasti útoku uživatel 1



Ochrana potenciální oblasti útoku uživatel 2



Ochrana potenciální oblasti útoku uživatel 3

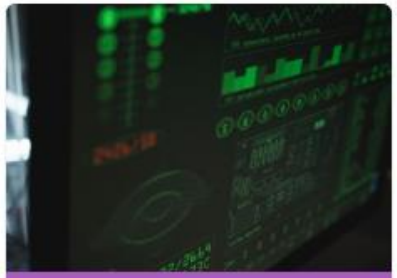


Ochrana potenciální oblasti útoku uživatele

Bitdefender

PHASR
Monitored categories of tools

- **LoLBin**
- **Tampering Tools**
- **Remote Admin Tools**
- **Crypto Miners**
- **HackTools**



Living Off the Land Binaries

Living off the land binaries are tools that exploit existing software and systems for malicious purposes. They leverage legitimate applications to carry out attacks without detection.

Understanding Tampering Tools

Tampering tools in software are programs used to modify or analyze applications. While they can serve legitimate purposes, they are often linked to malicious activities like cracking and code injection.

Exploring Hack Tools

Hack tools are software applications designed to exploit vulnerabilities in systems. They can be used for both ethical hacking and malicious purposes, depending on the user's intent.

Cryptocurrency Miners Overview

Cryptocurrency miners are specialized software or hardware that solve complex mathematical problems to validate transactions on a blockchain. They are essential for generating new coins.

Remote Administration Tools

Remote administration tools allow users to control computers from a distance. While they can be used for legitimate remote support, they are also exploited for unauthorized access.

Other categories will come …

Autopilot (ML/AI) or Direct control operating modes

Od kolika zařízení se Phasr licencuje?

500

5

100

300

Co je potřeba pro nasazení Phasr ?

- musím mít platnou licencí Enterprise s EDR ?
- musím být zákazníkem Bitdefenderu ?
- co když mám antimalware od jiného výrobce ?

Bitdefender

GravityZone Compliance Manager

Klíčové Vlastnosti

Z MĚSÍCŮ NA MINUTY: AUTOMATIZOVANÉ ZPRÁVY PŘIPRAVENÉ K AUDITU

- ✓ Podporuje Různé Compliance Standardy

  Připravená podpora hlavních standardů shody, jako jsou například GDPR, PCI DSS, NIS 2 Directive, CISv8, SOC 2, HIPAA and ISO 27001

- ✓ Informace V Reálném Čase

  Přehled v reálném čase o rizicích, dotčených aktivech a celkovém stavu dodržování předpisů u koncových zařízení v cloudu i v lokálním prostředí, který pomáhá urychlit procesy a zkrátit dobu potřebnou k dosažení souladu s předpisy

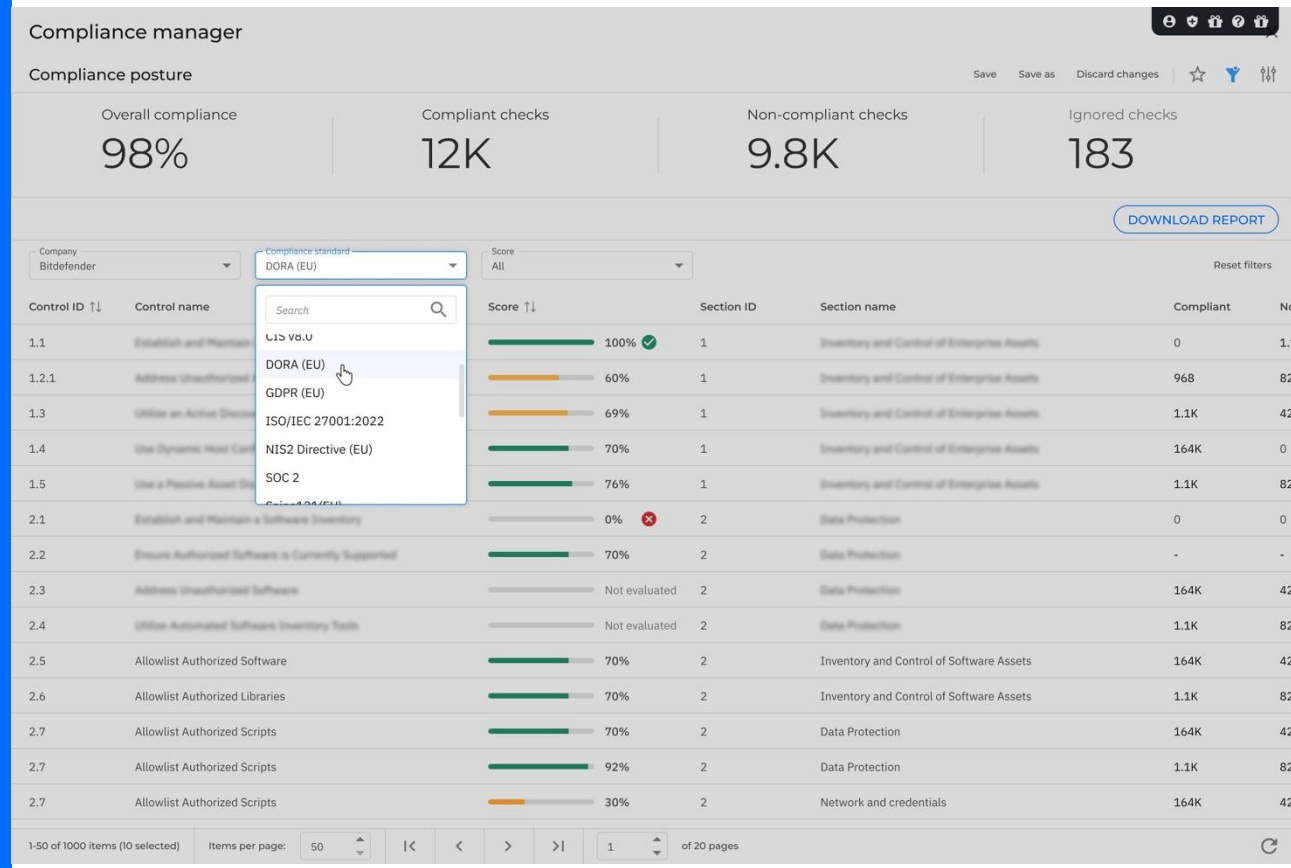
- ✓ Odstraní Zjištěné Nedostatky

  Zjištěné chyby rychle opravte jediným kliknutím – snížíte tak riziko, ušetříte čas a zefektivníte nápravná opatření

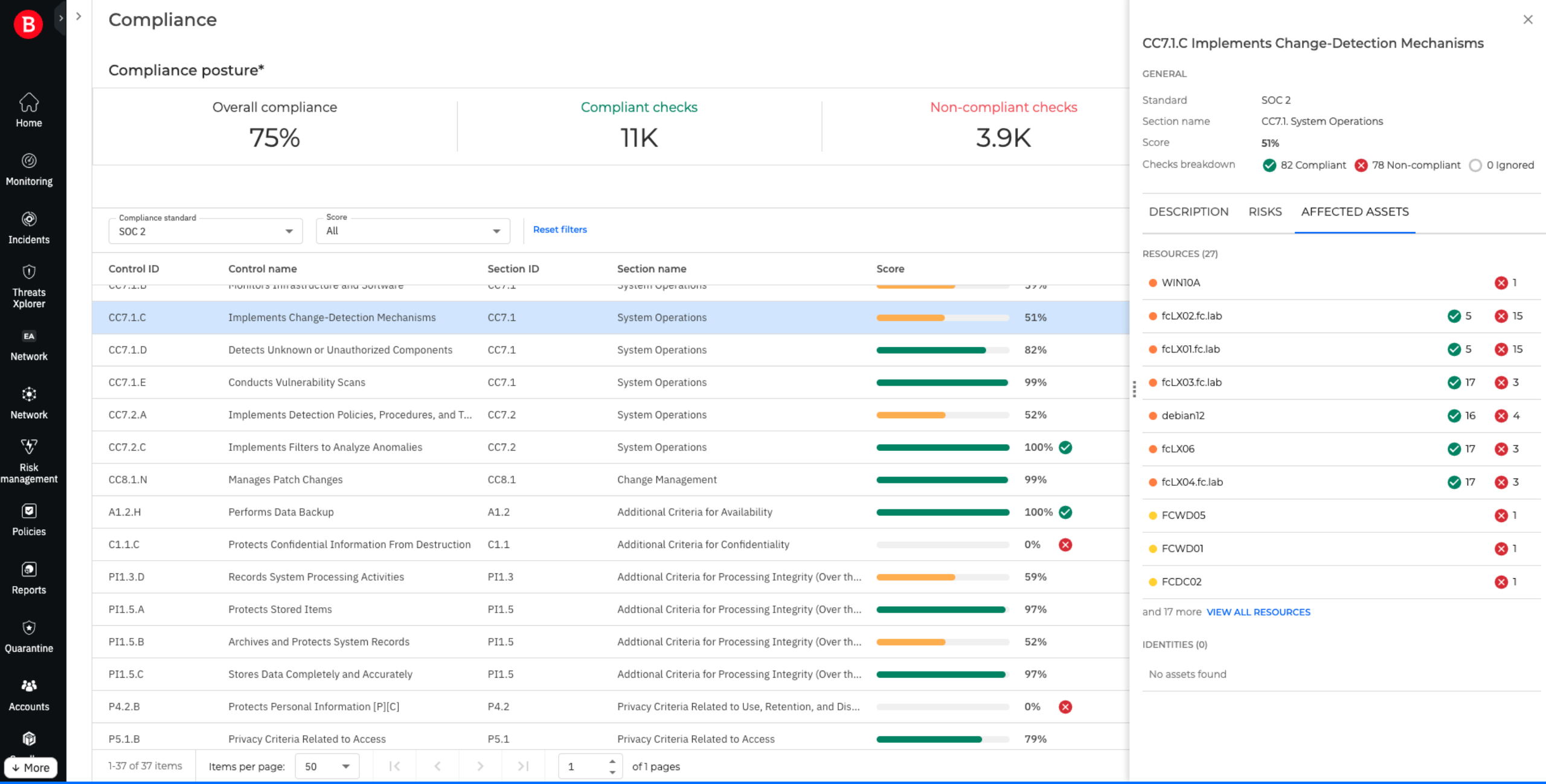
- ✓ Vytváří Rozsáhlé Reporty

  Vytvářejte podrobné zprávy, které shrnují všechna relevantní data, čímž snižují složitost, šetří čas a minimalizují potřebu specializovaných odborných znalostí

Compliance Made Real Simple.



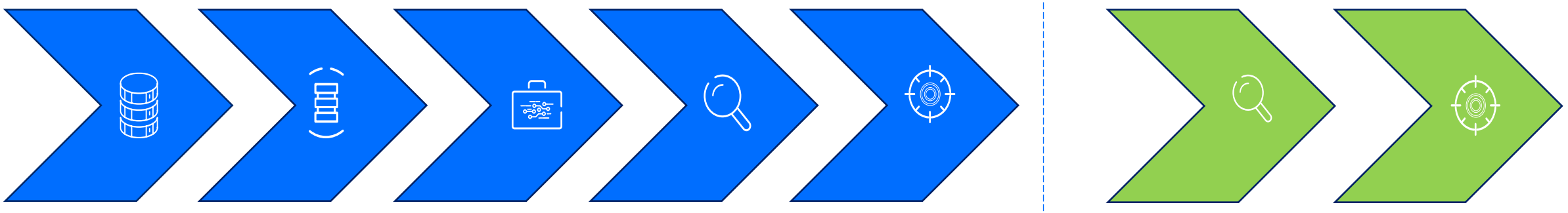
European Parliament · PCI · CISA · ISO · CIS · AICPA SOC



Plný přístup ke všem standardům shody (základní a pokročilé) - Zobrazí všechny podrobnosti a umožní exportovat do PDF nebo XLS

Bitdefender

Data Lake - Jak to funguje



Collect

Přenášejte protokoly ze svých nástrojů, aplikací a cloudu

Ingest & Normalize

Převeďte data do jednotného schématu pro snadnou korelaci

Route & Store

Live-archive pro úschovu dat s optimalizovanými náklady

Search & Retrieve

Live search pro rychlé vyhledávání a investigací dat

Detect & Act

Přehledové panely a upozornění mapují rizika v reálném čase

Investigate

Data z klíčových bezpečnostních nástrojů 3rd stran se načtou pro potřeby třídění a vyšetřování

Respond

Opatření a doporučení přijatá za účelem zmírnění rizik

Bitdefender

MDR Operations Overview

Global Team: 3 x Security Operations Centra: San Antonio, Texas & Bucharest, Romania & Singapore

Expertise:

- 40+ SANS certifications; Incident Handling, Forensics, SIEM with Tactical Analysts, Cyber Threat Intelligence .
- Cloud Admins, System Administrators, IT (školství, státní správa, zdravotnictví)
- Military Intelligence (U.S. Air Force, U.S. Navy, British Intelligence, NSA, NATO, etc.)

Threat Intelligence

Zabývá se výzkumem kybernetických hrozeb, geopolitického dění a trendů v datech specifických pro jednotlivá odvětví a tyto poznatky aplikuje v prostředích zákazníků

24/7 Monitoring & Response

Odstraňuje provozní zátěž spojenou se správou bezpečnostních výstrah a událostí a poskytuje taktická i strategická doporučení s cílem snížit míru vystavení zákazníků rizikům

Threat Hunting

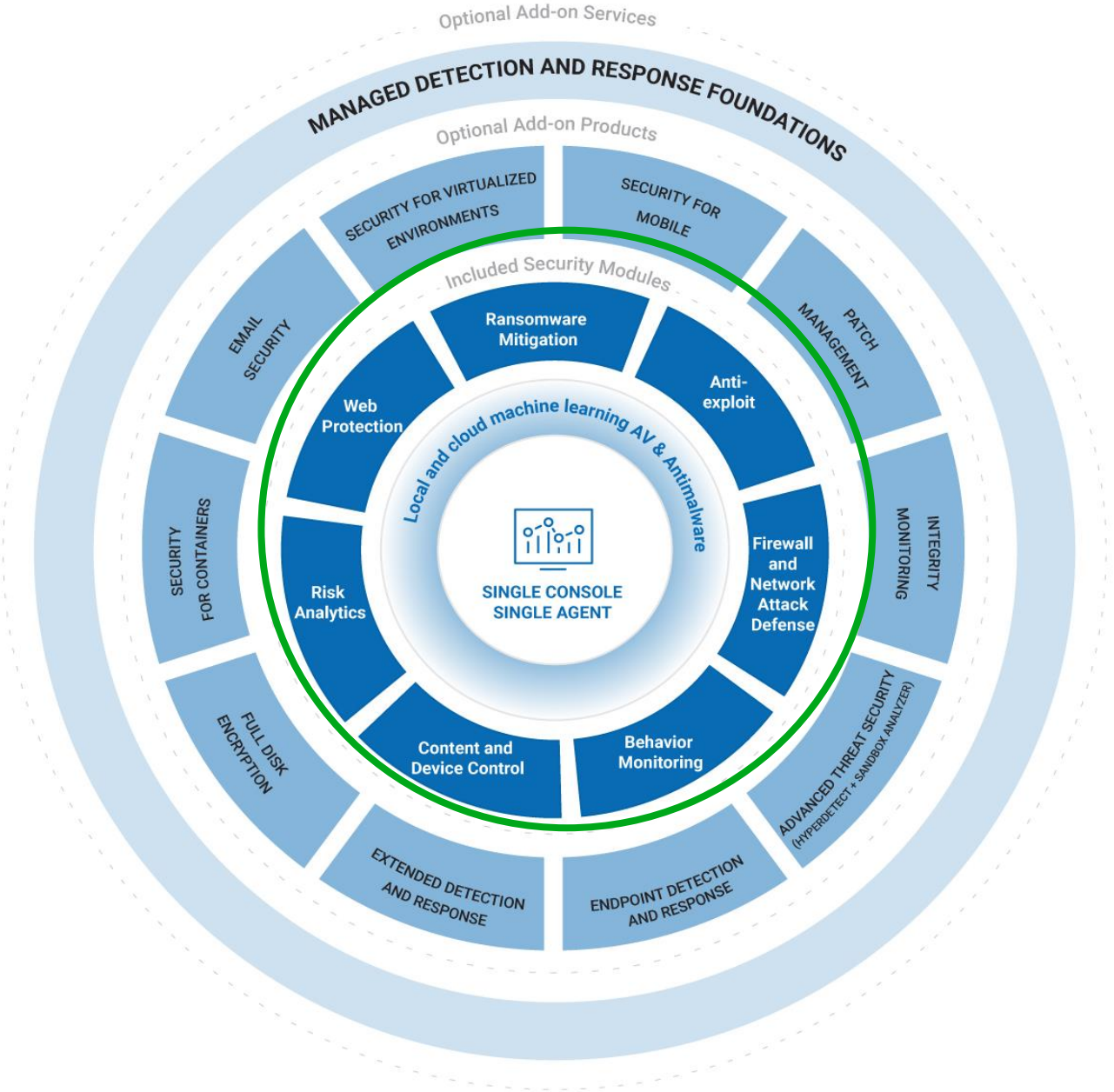
Neustále sledujeme globální situaci v oblasti hrozeb a získané poznatky využíváme k vyhledávání hrozeb v systémech našich zákazníků

Bitdefender

Existing Cloud Security

" Přizpůsobte si svou kyberbezpečnost pomocí řešení GravityZone Cloud Security – špičková ochrana, maximální kontrola."

- **Účinné řešení kyberbezpečnosti** pro poskytovatele spravovaných služeb s pokročilou prevencí, posílením zabezpečení, detekcí a reakcí.
- **Flexibilní,** komplexní a přizpůsobené vašim jedinečným požadavkům.
- Naše řešení vám dává svobodu vybrat si pouze ty **bezpečnostní funkce**, které potřebujete, a poskytuje tak špičkovou ochranu při současném optimalizování vašich **provozních nákladů**.



Bitdefender

Cloud Security Solutions

SECURE

MSP Core
ATS
EDR

SECURE PLUS

MSP Core
ATS
EDR
MDR

SECURE EXTRA

MSP Core
ATS
EDR
MDR
XDR Identity providers
XDR Productivity apps

Bundles!

A LA CARTE

Existing multilayered security solution

ATS *(Advanced Threat Security):*

- *HyperDetect*
- *Fileless Attack Defense*
- *Sandbox Analyzer*

EDR *(Endpoint Detection and Response)*

- *Cross-endpoint correlation*
- *Anomaly Defense*
- *Endpoint Incident Visualization*
- *Live and Historical Search*
- *MITRE Event Tagging (TTPs)*
- *Response recommendations*
- *Endpoint response*

MDR *(Managed Detection and Response)*

- *24x7 Monitoring & Respond*
- *Threat Hunting*
- *Reporting*
- *Recommendations*

XDR *(eXtended Detection and Response)*

Global Leader In
Cybersecurity

Bitdefender®