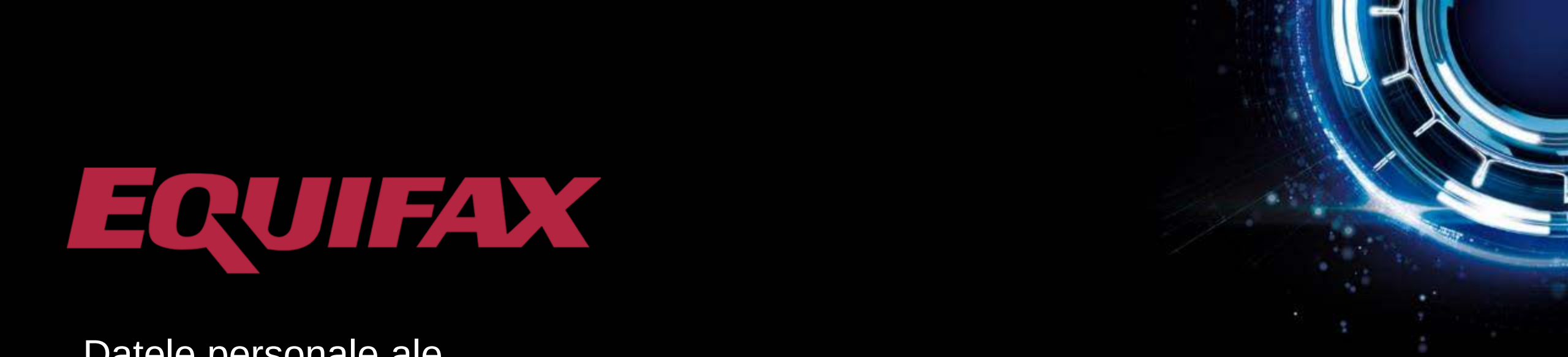
Bitdefender NextGen Endpoint Protection

Catalina Husanu, Product Manager Bitdefender



Datele personale ale

143.000.000 cetateni ai SUA

Expuse in unul din cele mai grave atacuri informatice

CE POTI SA FACI CA SI CETATEAN AFECTAT?

Pasul 1: Sa te inrolezi in programul de verificare al Equifax

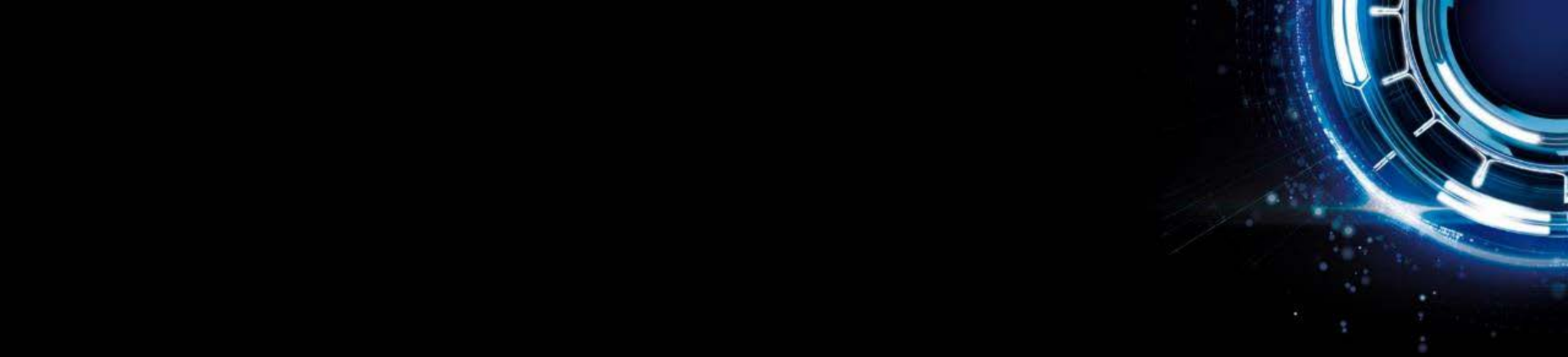
Pasul 2: Sa verifici rapoartele de credit

Pasul 3: Sa blochezi acordarea de credite pe numele tau

Pasul 4: Sa setezi o alerta de frauda

Pasul 5: Sa repeti procesul pentru cei din familie

Pas bonus: Fii foarte atent in sezonul de taxe



GDPR

UN CADRU LEGISLATIV COERENT SI UNITAR LA NIVEL UE PENTRU PROTECTIA DATELOR CU CARACTER PERSONAL

Bitdefender

BITDEFENDER AJUTA COMPANIILE SA ISI PROTEJEZE DATELE

Protectie impotriva furtului de date – Atacuri targetate

- HyperDetect, Sandbox Analyzer

Imbunatatirea vizibilitatii asupra incidentelor de securitate

- Endpoint Security HD Insights
- Security Analytics planificate pentru xDR

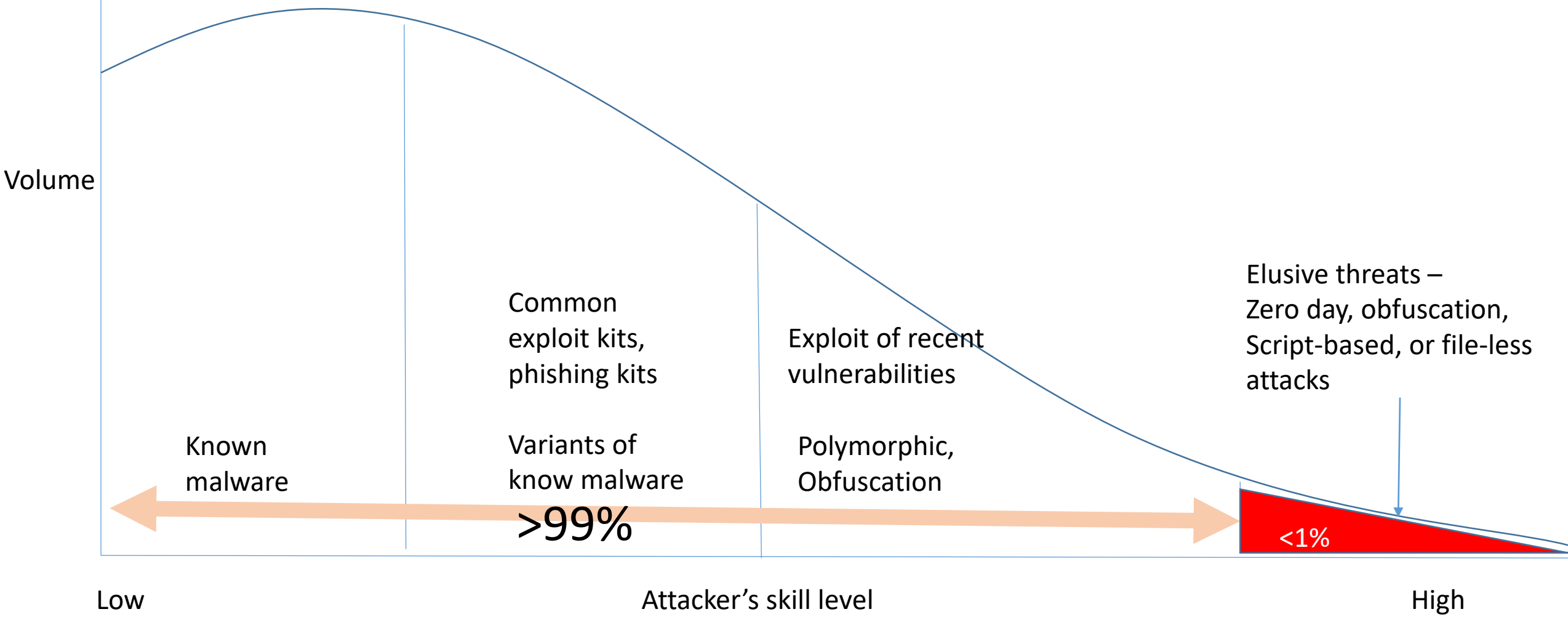
Protectie impotriva pierderii de date – Dispozitive furate si/sau pierdute

- Full Disk Encryption

PROTECTIE IMPOTRIVA FURTULUI DE DATE – ATACURI TARGETATE

Bitdefender

The Evolving Threat Landscape



AUGUST

Bitdefender

Need help with ordering on [redacted].Com - Message (Plain Text)

File | Message

From: [redacted].au>
Sent: Tue 11/8/2016 5:43 AM
To: [redacted]
Cc:
Subject: Need help with ordering on [redacted].Com

Message | [redacted].Com.doc (53 KB)

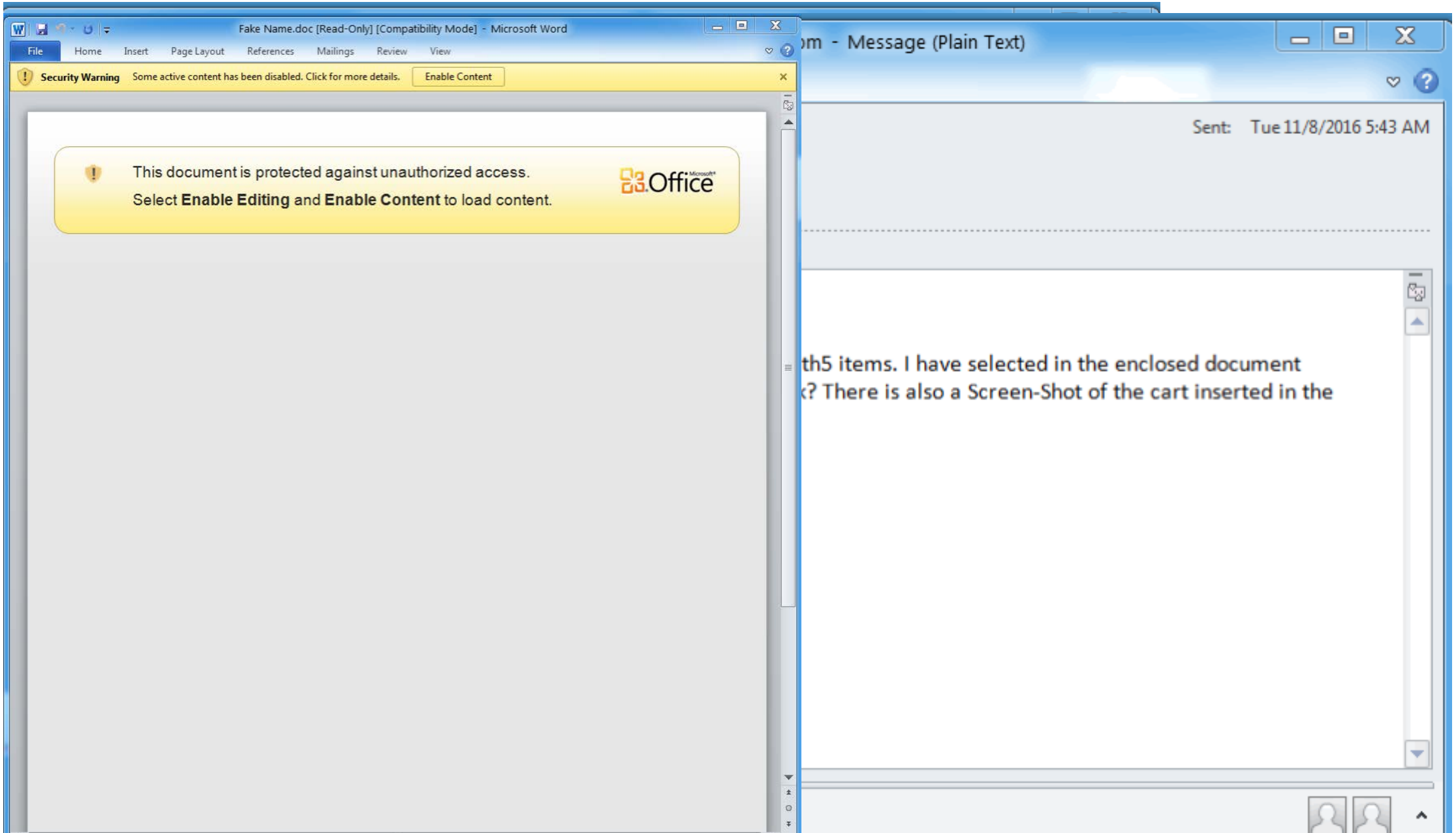
Dear Sir/Madam,

I am getting ready to place an order on [redacted].Com, but having issues with5 items. I have selected in the enclosed document everything I want to buy, can you take a look and confirm if you have it in stock? There is also a Screen-Shot of the cart inserted in the document.

I appreciate your help.

Cheers!
[redacted]

August malware attack



August malware attack

Phishing email with word/excel attachment

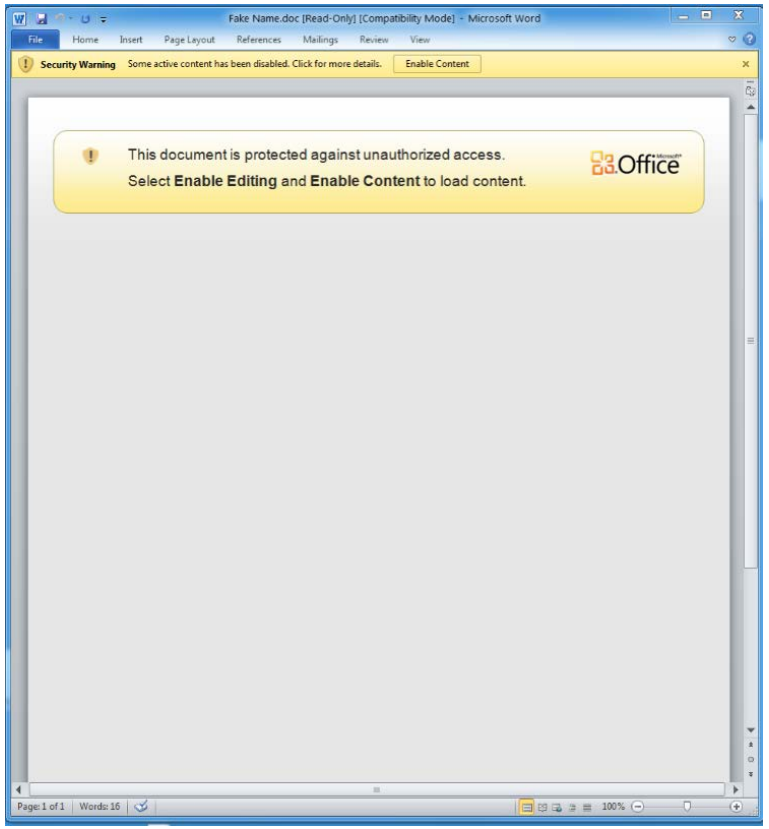
User enable Macro

Macro launches PowerShell commends

PowerShell download and execute malicious file-less malware

Credential theft

Data theft



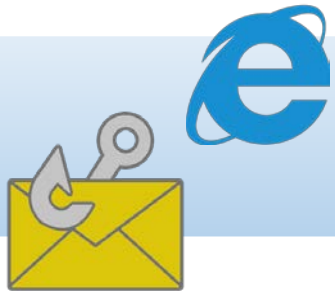
Detect, Prevent, Disrupt File-less Attacks

Channel

Infection/Exploitation Techniques

Payload Techniques

Objectives



PowerShell
WMI

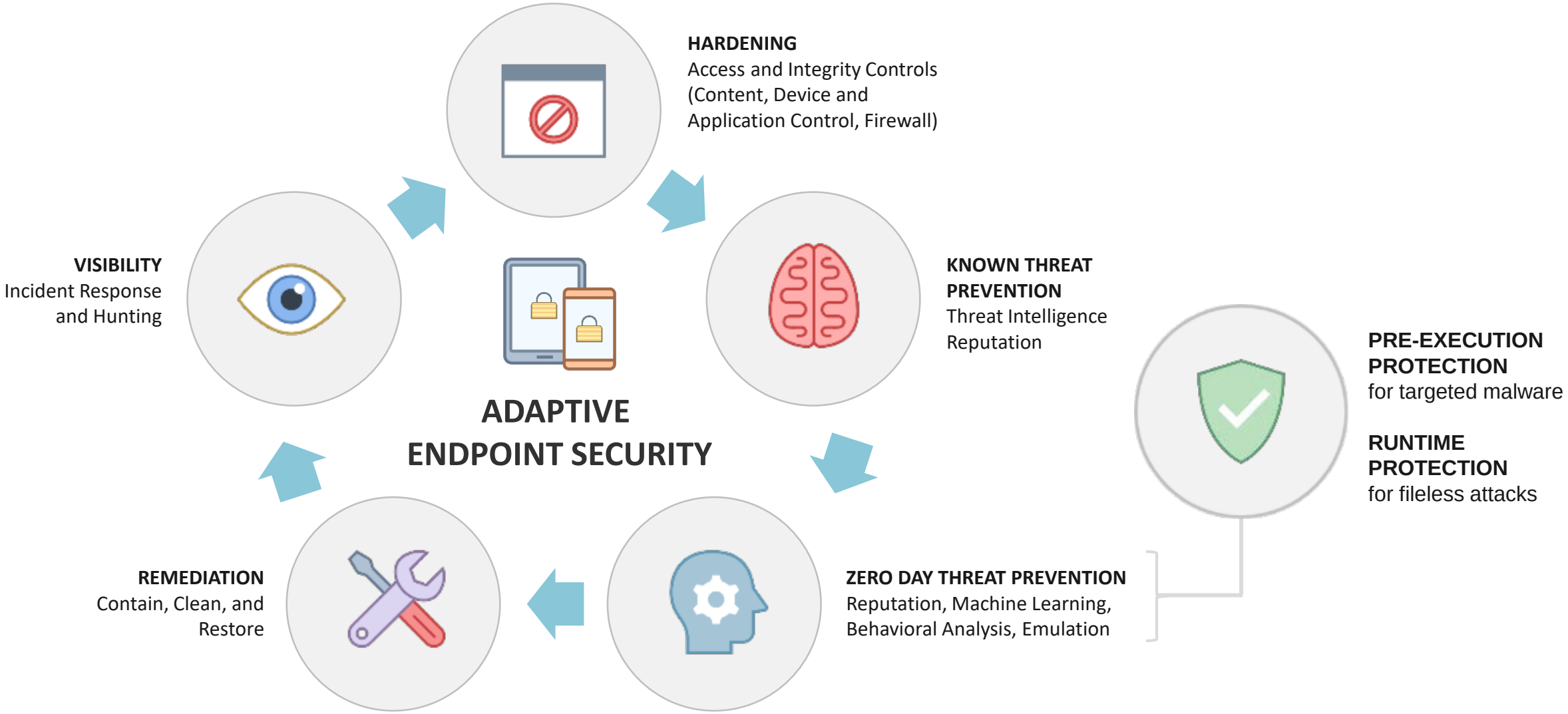
HyperDetect

- Command line Analyzer
- Malicious scripts
- Anti-exploit

Process inspector –

- Zero trust, follows every single running process
- Terminate process

Procesul de securitate



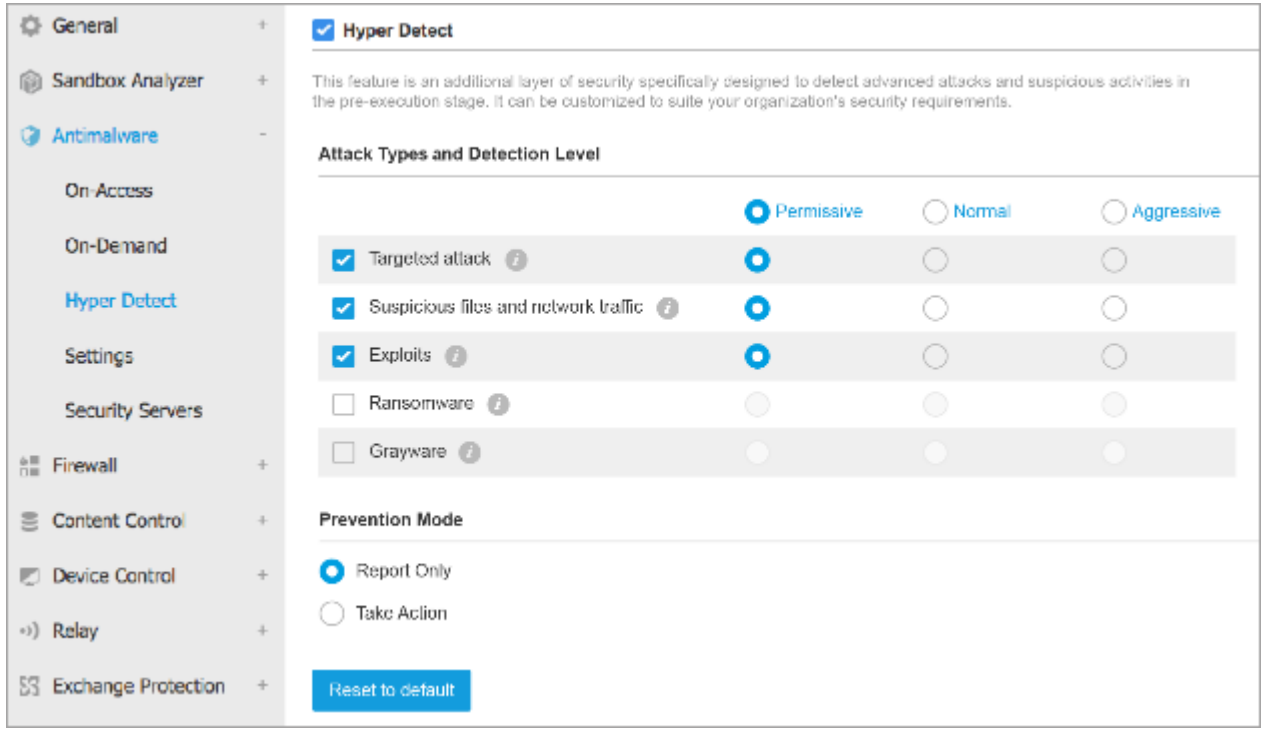
Bitdefender

HYPERDETECT

DETECTEAZA ATACURI SOFISTICATE IN FAZA DE PRE-EXECUTIE

New in GZ Elite

- Preventie in faza de pre-execution
- Non-signature based - Machine learning + euristici avansate
- Blocheaza amenintari avansate (PowerShell, file-less attacks, ransomware necunoscut)
- Atacuri targetate, instrumente de hacking, anti-exploit, ransomware, PUA, trafic web suspicios
- Setari flexibile pentru optimizarea agresivitatii protectiei
- Vizibilitate asupra amenintarilor potentiale

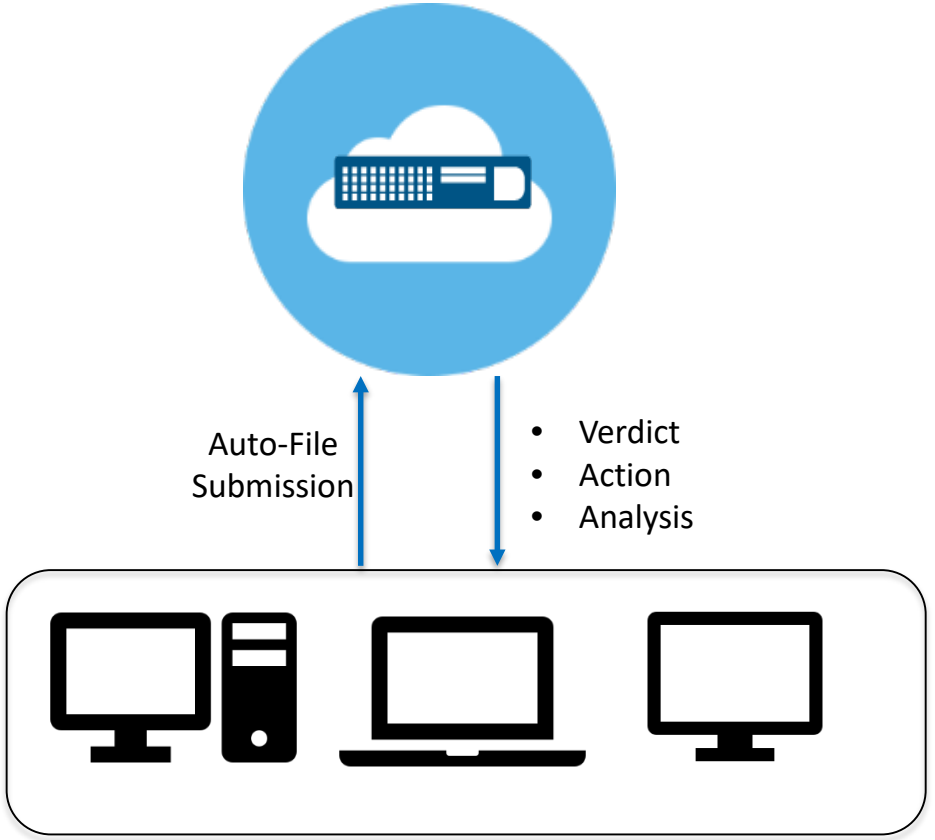


New in GZ Elite

SANDBOX ANALYZER

PROTEJEAZA IMPOTRIVA ATACURILOR TARGETATE SI A AMENINTARILOR NECUNOSCUTE

- Trimite automat fisierele suspicioase pentru a fi analizate in sandbox
- Optiuni de monitorizare si blocare
- Verdict in timp preal
- Informatii detaliate cu privire la comportamentul fisierelor necunoscute
- Analizeaza o singura date iar rezultatul este disponibil pentru intreaga organizatie



VIZIBILITATE ASUPRA AMENINTARILOR SI INCIDENTELOR DE SECURITATE

Bitdefender

VIZIBILITATE IMBUNATATITA ASUPRA AMENINTARILOR SI INCIDENTELOR

Endpoint Security HD Insight

- Detonare remote (Sandbox)
- Vizibilitate asupra contextului amenintarii
- Conecteaza amenintarea cu actiunile acesteia
- Vizibilitate suplimentara pentru analize si actiuni viitoare
- Expune amenintarile (software) suspecte (HD Reports)

Security Analytics planuite pentru xDR

- Detecteaza varfurile de activitate de tip Malware
- Detecteaza conexiunile de tip Botnet/C&C
- Detecteaza downloadul de fisiere suspecte (Atacuri targetate)
- Detecteaza procesele suspecte (atacuri file-less)
- Detecteaza comportamentul anormal al aplicatiilor sau sistemului de calcul (Data Exfiltration & Lateral Movement)
- Detectecteaza amenintarile din interior (User rau intentionat sau conturi de utilizator compromise)

Bitdefender

PROTECTIE IMPOTRIVA PIERDERII DE DATE – DISPOZITIVE PIERDUTE SI/SAU FURATE

Bitdefender

STATISTICI DATE PIERDUTE IN 2016

554 milioane de inregistrari in prima jumatate a 2016

45% din incidentele din healthcare

Source: Verizon 2016 Data Breach Investigations Report

Bitdefender

GRAVITYZONE FULL DISK ENCRYPTION

GravityZone Full Disk Encryption foloseste mecanismele puse la dispozitie de Windows (Bitlocker) si Mac (FileVault), beneficiind de nivelul excelent de compatibilitate si performanta oferite de aceste mecanisme native.
Nu este necesara instalarea unui agent additional si nici a unui server de key management.

- ☑ Managementul criptarii folosind aceeasi consola cloud/on-premise utilizata la management solutiei de securitate pentru endpoints
- ☑ Utilizeaza mecanismele native pentru Windows (BitLocker) si Mac (FileVault) evitand astfel problemele de performanta si compatibilitate
- ☑ Simplu de instalat Full Disk Encryption pe endpoints; simplu de administrat si de recuperat cheile de criptare folosind consola
- ☑ Ofera rapoarte specifice cu privire la criptare pentru a dovedi conformitatea
- ☑ Fortarea autentificarii utilizatorului inainte de pornirea calculatorului

Bitdefender

Q&A

Bitdefender