Bitdefender
Global Leader
In Cybersecurity

Bitdefender®

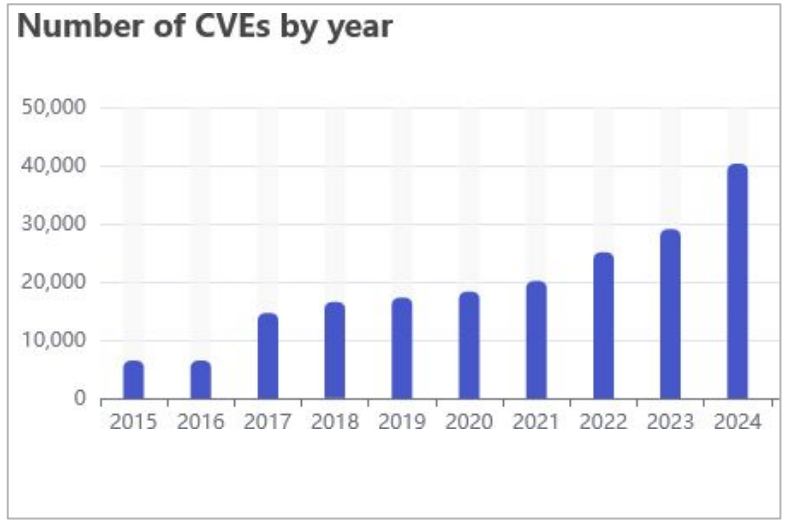
Bitdefender rivoluziona la sicurezza con PHASR: ogni utente, una protezione dedicata

AVANGATE by ELOVADE

Bitdefender

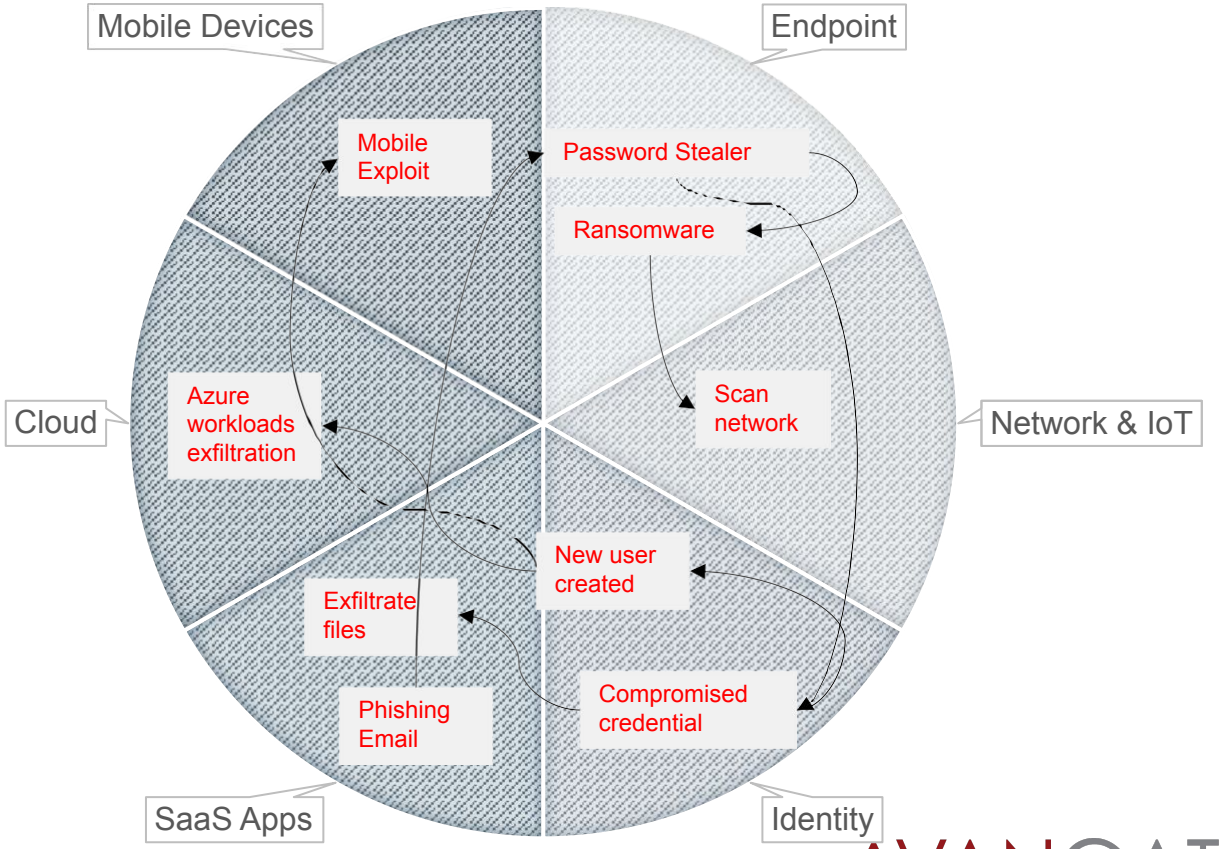
Le vulnerabilità e le superfici di attacco sono in rapido aumento

More Vulnerabilities, faster exploitation



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

Expanding attack surface



AVANGATE by ELOVADE

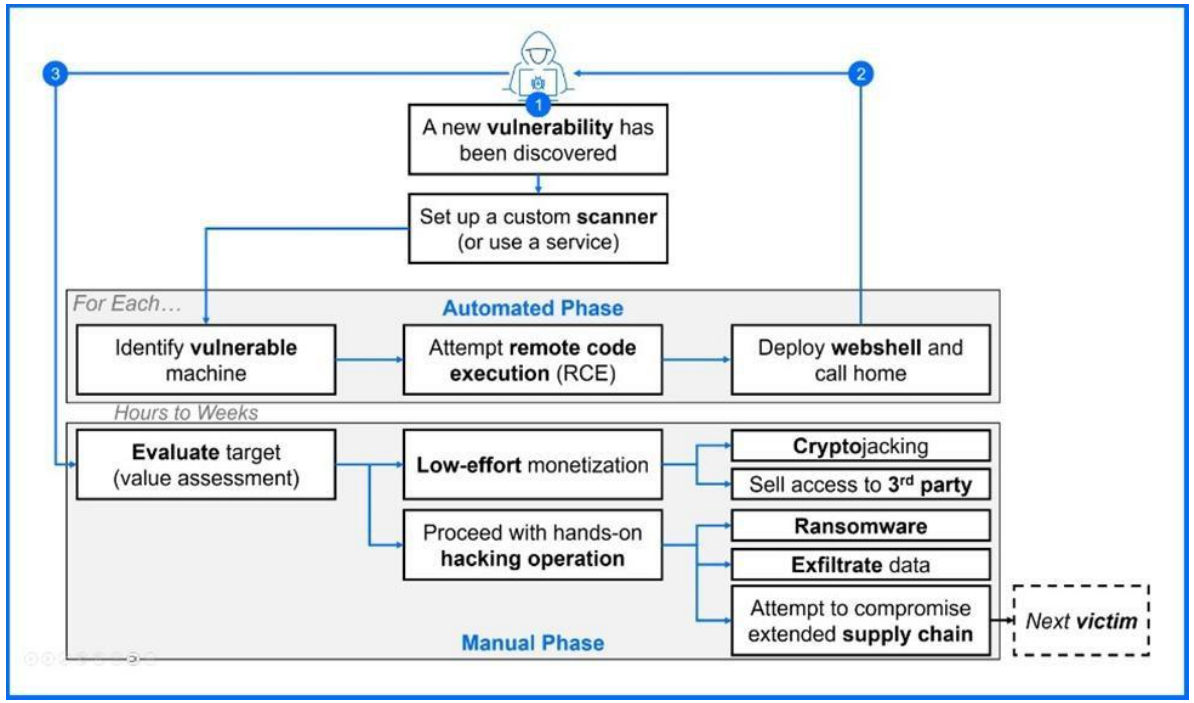
Bitdefender

Meno di 24 ore dopo la divulgazione pubblica della vulnerabilità ,
i cyber criminali avviano scanner automatici che scandagliano Internet
e stabiliscono l'accesso remoto ai sistemi vulnerabili.

Dopo il blitz di accesso iniziale,
i criminali avviano la seconda fase dell'attacco:
l'**hacking manuale delle vittime**.

Questa seconda fase **richiede tempo**.

In genere utilizzando tecniche di
"Living Off the Land"
per eludere il rilevamento.



Bitdefender

ATTACCHI **LOTL**:

Living **O**ff **T**he **L**and

Negli attacchi LOTL
gli aggressori sfruttano strumenti legittimi già disponibili sul sistema di destinazione:

- nessun tempo per lo sviluppo di tool (malware)
- nessun file maligno rilevabile con firme
- nessuna traccia permanente dell'attacco

L'attacco ha ottime possibilità di NON essere intercettato ed arrestato nelle fasi iniziali della killchain.

68% Degli incidenti gravi coinvolgono LOTL

AVANGATE by ELOVADE

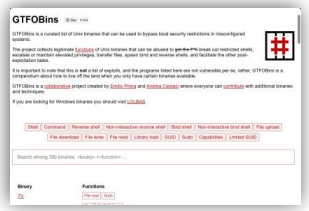
LOLTools

Living **O**ff the **L**and **T**ools

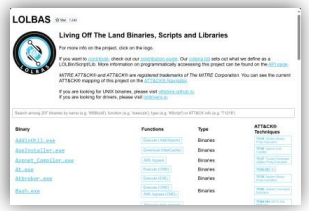
200+

Windows binaries abused by threat actors

I LOLBin (Living Off the Land Binaries) sono eseguibili legittimi che gli aggressori utilizzano impropriamente per attività dannose. Questi binari integrati spesso hanno privilegi elevati e sono considerati affidabili dagli strumenti di sicurezza, il che li rende efficaci per l'esecuzione stealth.



- **PowerShell** : esegue script offuscati per scaricare malware, modificare le impostazioni di sistema ed eludere il rilevamento.
- **MSHTA.exe** – Esegue script HTML Application (HTA) , spesso utilizzati per la distribuzione iniziale di malware.
- **Rundll32.exe** – Carica ed esegue DLL dannose tramite dirottamento di DLL (binary planting).
- **Certutil.exe** : un'utilità di certificazione legittima, comunemente utilizzata dagli autori delle minacce per scaricare e decodificare il malware.
- **Attività pianificate (Schtasks.exe, At.exe)** : automatizza l'esecuzione di script dannosi a intervalli stabiliti per garantire la persistenza.
- **BITSAdmin** – Utilizzato per scaricare ed eseguire furtivamente i payload.
- WMIC (Windows Management Instrumentation Command-line): esegue comandi e script remoti, spesso utilizzati per la ricognizione del sistema.



AVANGATE by ELOVADE

Bitdefender

Vettori di attacco superflui

Sulla base di una ricerca di Bitdefender, **solo lo 0,22% delle organizzazioni** utilizza **Bitsadmin**.

quindi potrebbe essere **disabilitato per il 99,8%** delle organizzazioni

Meno del 20% delle organizzazioni utilizza effettivamente **cscript** e **wscript**

quindi potrebbe essere **disabilitato per il 80%** delle organizzazioni

PowerShell,viene **utilizzato dall'83,6% delle aziende**.

Il **17% delle aziende** può eseguire potenziali payload dannosi **senza alcuna ragione**.

Il **90% dell'utilizzo di PowerShell include gli account amministratore**

quindi potrebbe essere disabilitato per tutti gli altri utenti.

AVANGATE by ELOVADE

Bitdefender

Ogni organizzazione e ogni utente sono diversi. Così come la loro superficie di attacco.

Bitdefender

Un’azienda: diversi utenti, diversi ruoli

Jessica
Risorse Umane

Riccardo
Software Engineer

Andrea
SysAdmin

Attacco Ransomware

AVANGATE by ELOVADE

Bitdefender

Quale superficie possiamo ridurre per Jessica?

Attacco Ransomware

Jessica
Risorse Umane

Email, Adobe, MS Office?
Servono per il suo lavoro.

Non ha bisogno di eseguire **macro** ne script **Powershell**.
Possiamo bloccarli.

Servirebbero **eccezioni** per permettere ad **amministratori** di eseguire **Powershell** sul suo computer.

AVANGATE by ELOVADE

Bitdefender

Le esigenze cambiano, in funzione dell'utente e del dispositivo.

	 **Jessica** Notebook Aziendale	 **Riccardo** Notebook Aziendale	 **Andrea** Gestione Server
Email	☑ Necessario	☑ Necessario	✗ ☑ Non sui server
Office & Adobe	☑ Necessario	☑ Necessario	✗ ☑ Non sui server
Powershell, wscript	✗	☑ Necessario	☑ Necessario
Macros in documents	✗	☑ Necessario	✗ ☑ Non sui server

NON ESISTE UNA SICUREZZA PER TUTTI

AVANGATE by ELOVADE

Bitdefender

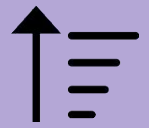
La sfida: obbiettivi e varibili

Obbiettivi

Hardening

Small Attack Surface

Usability



No/low impact to business operations

Manageability

Practical to implement

X

Variabili

LOLTools

200+

Users

tens to thousands

Endpoint

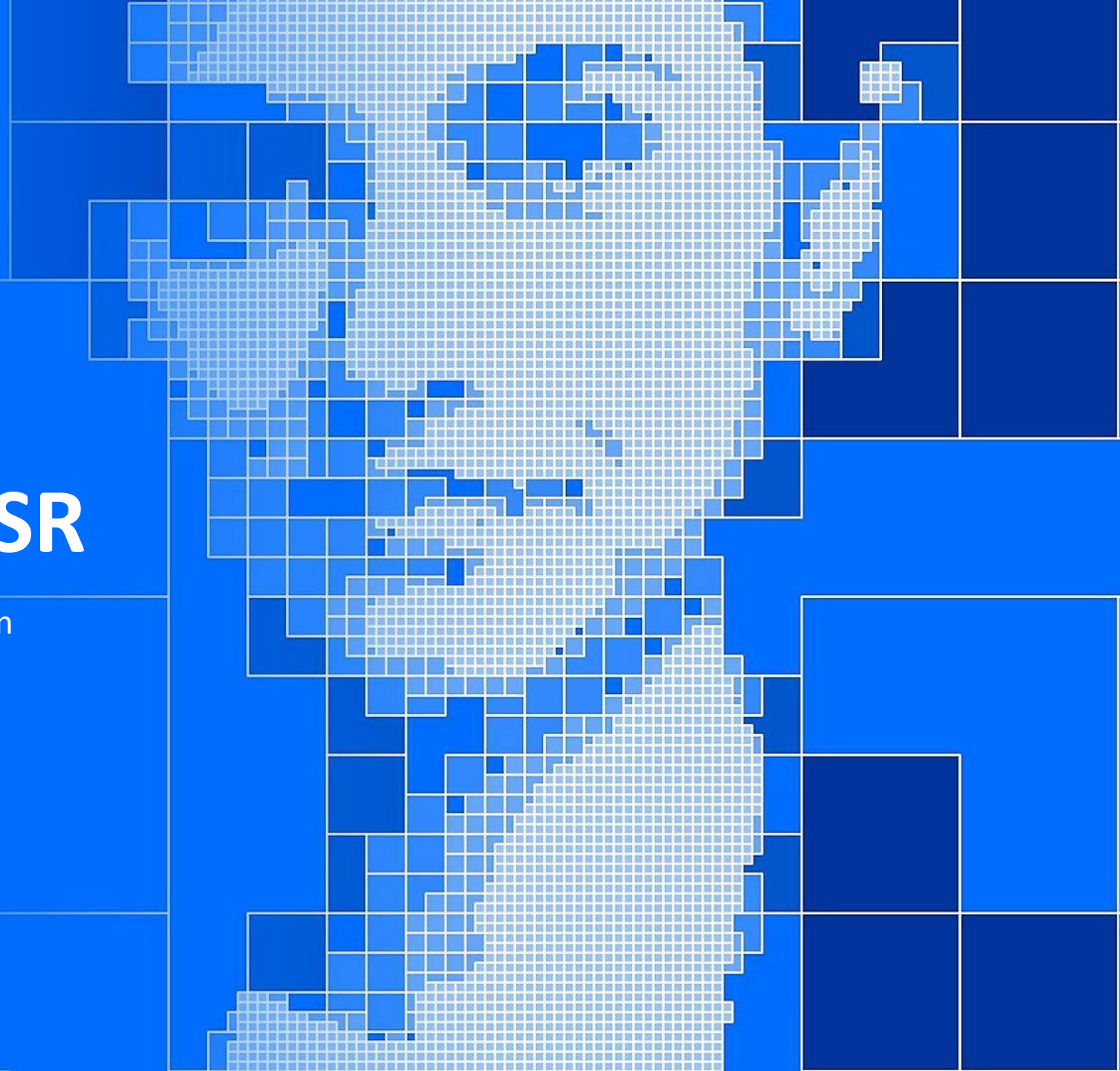
tens to thousands

AVANGATE by ELOVADE

Bitdefender Global Leader In Cybersecurity

GravityZone PHASR

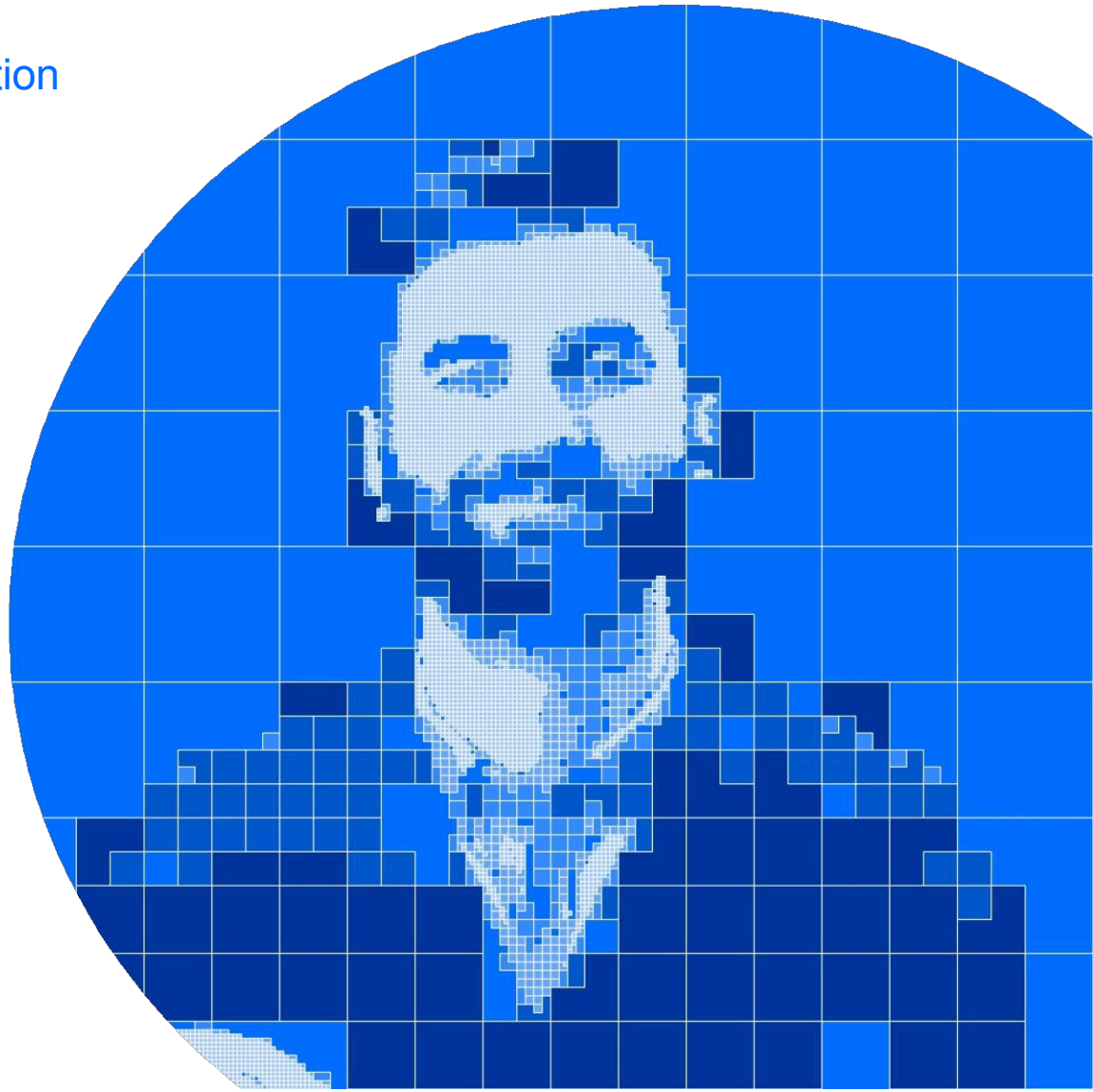
Proactive Hardening and Attack Surface Reduction



Bitdefender GravityZone **PHASR**

Proactive **H**ardening and **A**ttack **S**urface **R**eduction

- La prima soluzione di **hardening su misura** basata sul comportamento unico dell'utente e sui vettori di minaccia conosciuti.
- La prima soluzione dinamica di **riduzione della superficie di attacco**.
- Garantisce un **hardening ottimale per ogni singolo utente e dispositivo**.
- **Si adatta nel tempo al comportamento reale** dell'utente ed all'evolversi delle minacce.
- **Chiude i vettori di attacco non necessari** strumenti come PowerShell, WMI che possono essere sfruttati dagli attaccanti. (**LOLTools**)



AVANGATE by ELOVADE

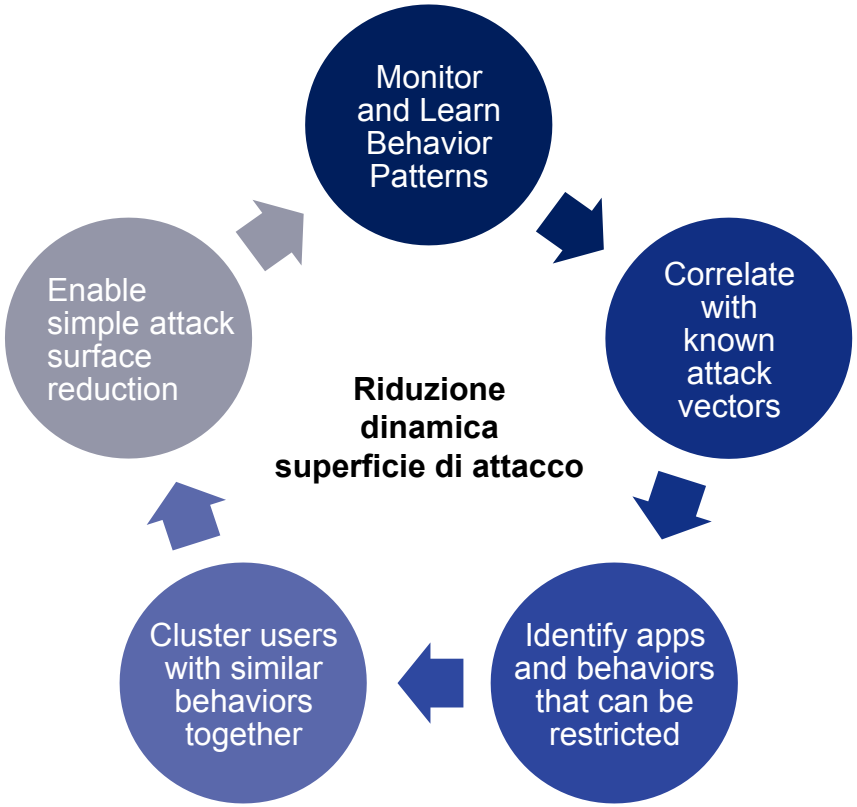
Bitdefender

PHASR - come lavora

Utilizza algoritmi di machine learning personalizzati per identificare comportamenti tipici per utenti.

Propone limitazioni su **strumenti** e **azioni** che **riducono la superficie di attacco senza penalizzare gli utenti**

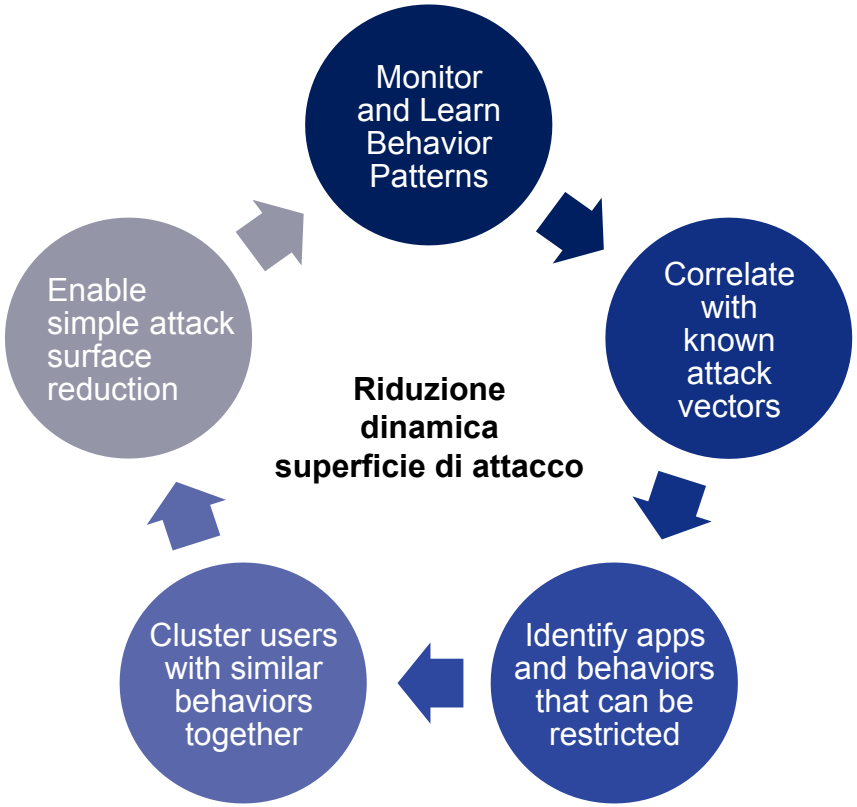
Aggiorna continuamente le raccomandazioni sulla base dei comportamenti dell'utente e della evoluzione delle minacce.



AVANGATE by ELOVADE

Bitdefender

ci ricorda qualcosa ?...



AVANGATE by ELOVADE

FNCDP

Framework Nazionale per la Cybersecurity e la Data Protection

Il **F**ramework **N**azionale per la **C**ybersecurity e la **D**ata **P**rotection (**FNCDP**)
è uno strumento di supporto alle organizzazioni.

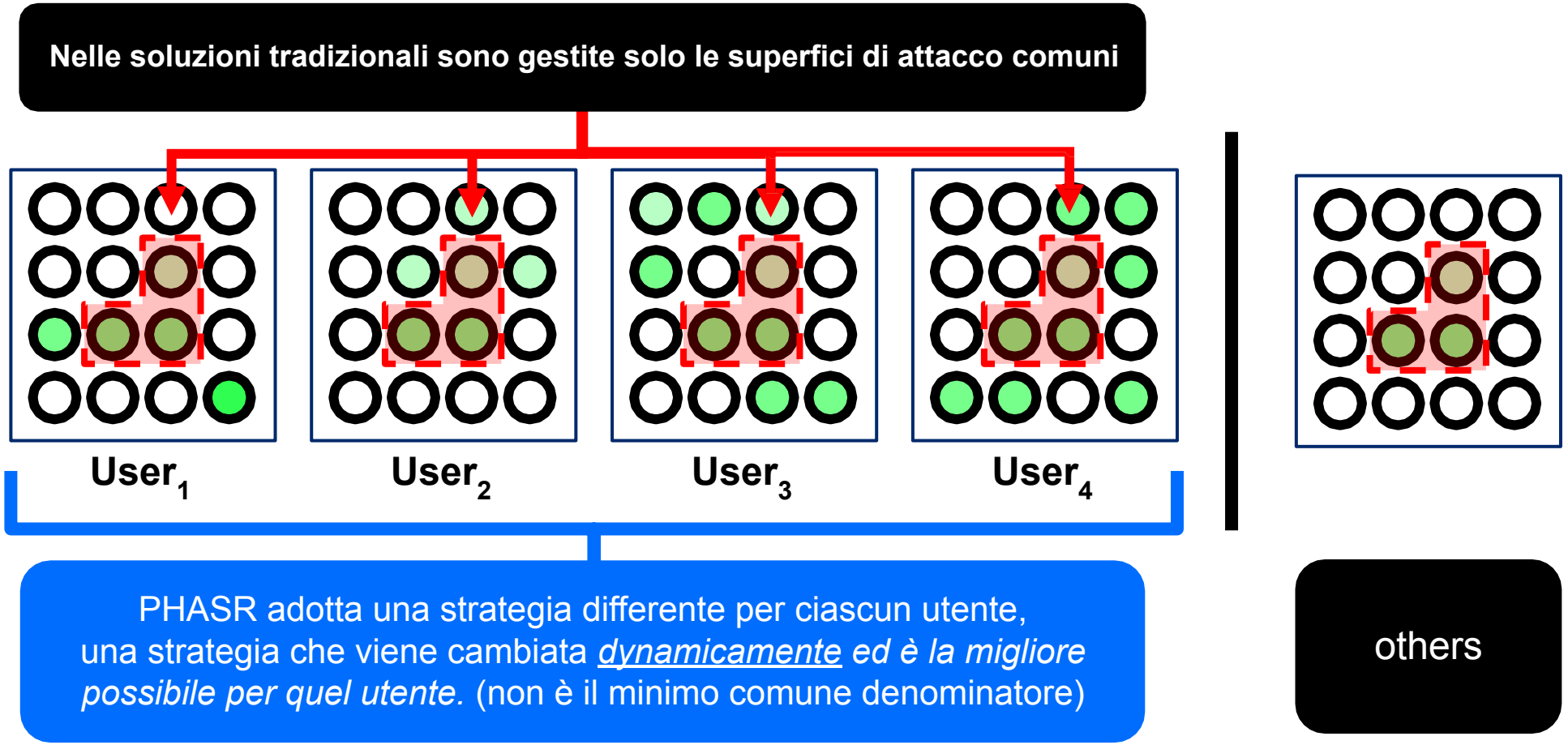
La sua adozione non può essere considerata esaustiva nella conformità alla direttiva **NIS 2**,
ma **può aiutare le organizzazioni nel definire un percorso** orientato alla cybersecurity e alla protezione dei dati, **coerente con i regolamenti**.

FNCDP è stato ispirato sin dalla prima edizione al framework **NIST**, ed anche nel suo ultimo aggiornamento del 2025, riprende tutti i tratti essenziali dell'ultima versione del framework NIST.

Rif. https://www.cybersecurityframework.it/

Bitdefender

Ogni utente è unico. Dovrebbe esserlo anche la sua sicurezza.

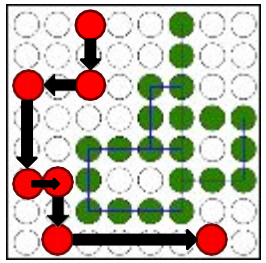


AVANGATE by ELOVADE

Bitdefender

Profilo statico delle soluzioni tradizionali

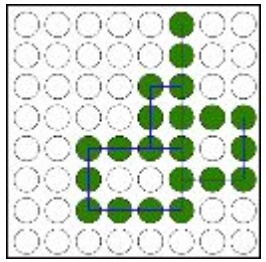
Attacker



New Attack Pattern Identified by the attacker

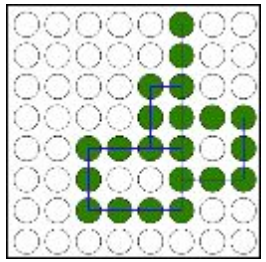
Company X protected by Product A

User1



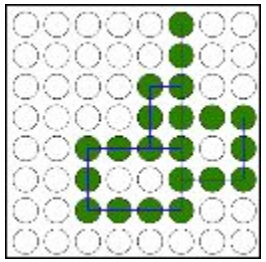
Attack Surface Protection

User2



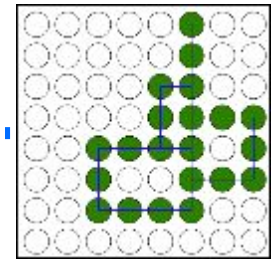
Attack Surface Protection

User3



Attack Surface Protection

UserN



Attack Surface Protection

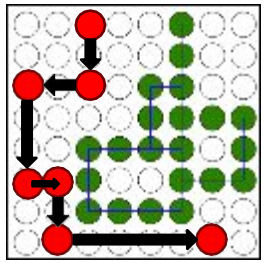
Elaborata una strategia evasiva per un utente/endpoint, l'attaccante può utilizzarla su qualunque altro.

AVANGATE by ELOVADE

Bitdefender

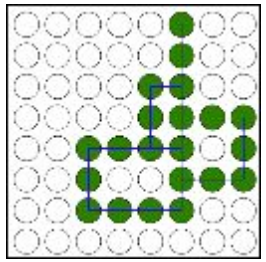
Profili diversificati di PHASR

Attacker

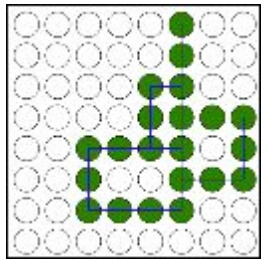


Attack Pattern Identified by the attacker

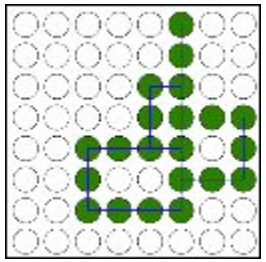
Company X protected by Product A day 0



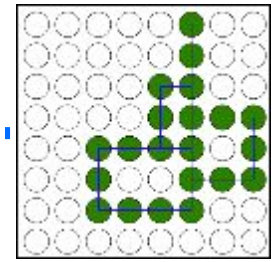
User$_1$ Attack Surface Protection



User$_2$ Attack Surface Protection

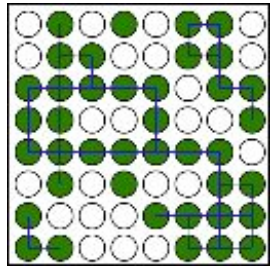


User$_3$ Attack Surface Protection

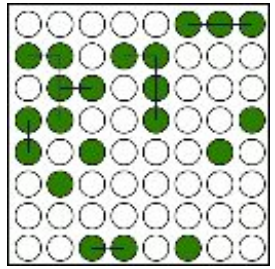


User$_n$ Attack Surface Protection

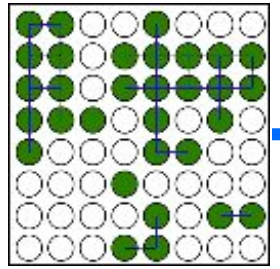
Company X protected by PHASR day 0



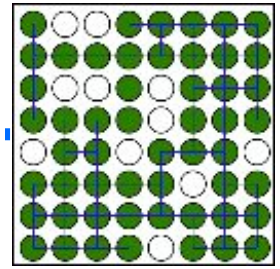
User$_1$ Attack Surface Protection



User$_2$ Attack Surface Protection



User$_3$ Attack Surface Protection



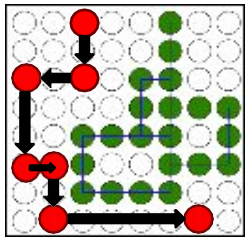
User$_n$ Attack Surface Protection

AVANGATE by ELOVADE

Bitdefender

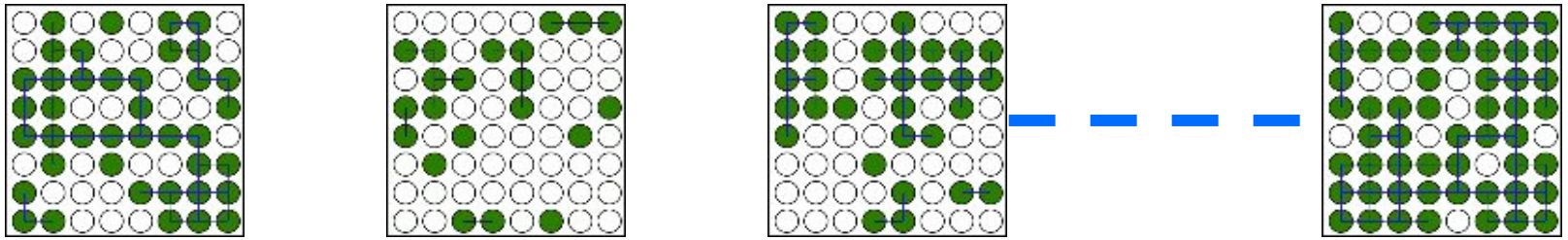
Profili dinamici di PHASR

Attacker

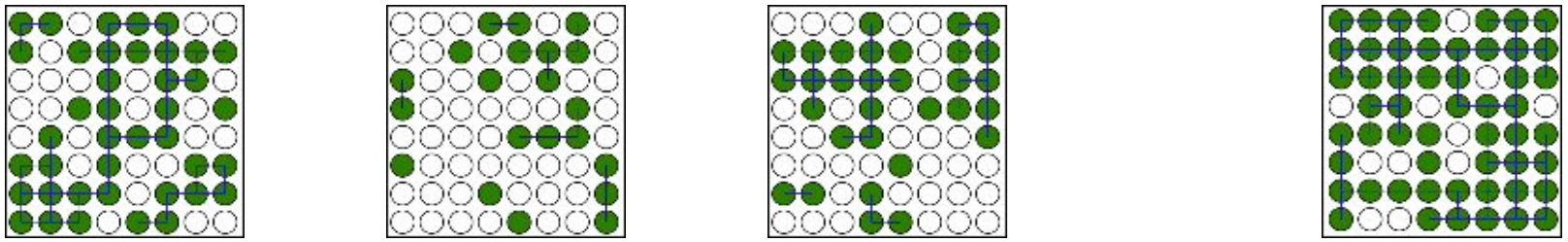


Attack Pattern Identified by the attacker

Company X protected by PHASR day 0



Company X protected by PHASR day N



User$_1$ Attack Surface Protection

User$_2$ Attack Surface Protection

User$_3$ Attack Surface Protection

User$_n$ Attack Surface Protection

AVANGATE by ELOVADE

Bitdefender

Cosa rende PHASR **unico**

Dinamico

Gli algoritmi di autoapprendimento si adattano continuamente a nuovi comportamenti e vettori di attacco.

Preciso

Abilitare restrizioni a livello di azione all'interno degli strumenti attivi, non solo lo strumento tout cour.

Fluido

Si integra perfettamente con l'infrastruttura esistente, senza interruzioni e con uno sforzo minimo.

AVANGATE by ELOVADE

Bitdefender

Perchè adottare PHASR

- **Profonda riduzione della superficie di attacco**
  (identifica il **20% di azioni** che generano l'**80% dei rischi**)
- **Prevenzione** proattiva di **attacchi LotL e mirati**
- **Salvaguardia** della **produttività** e dell'efficienza operativa
- **Riduzione dell'affaticamento da allerta**

AVANGATE by ELOVADE

Bitdefender

dicono di noi

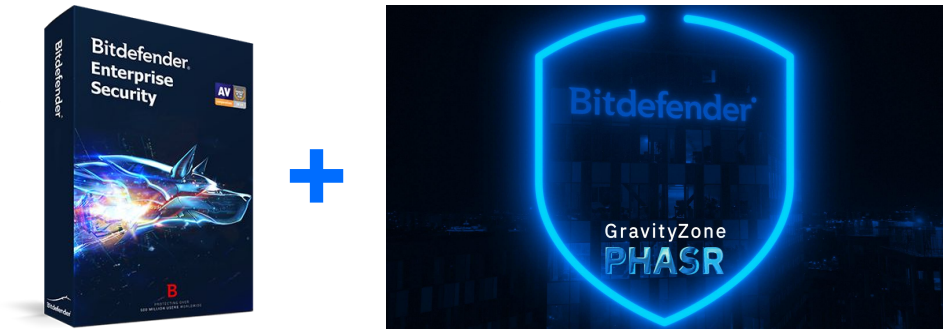
"*Bitdefender has consistently performed well in independent tests including MITRE Engenuity and has introduced innovative features such as Deep Process Inspector and Advanced Reasoning.* ***Most recently, in 2024 Bitdefender Proactive Hardening and Attack Surface Reduction (PHASR), a groundbreaking technology*** *that transforms how defense-in-depth-security is applied and managed across businesses.*"

IDC, IDC ProductScape: Worldwide Small and Medium-Sized Business Endpoint Protection Market, 2024–2025: Technology Supplier Solution Functionality, doc #US52830124, January 2025

AVANGATE by ELOVADE

Bitdefender

PHASR - Licensing



PHASR si avvale del sensore EDR,

pertanto richiede una licenza in add-on,

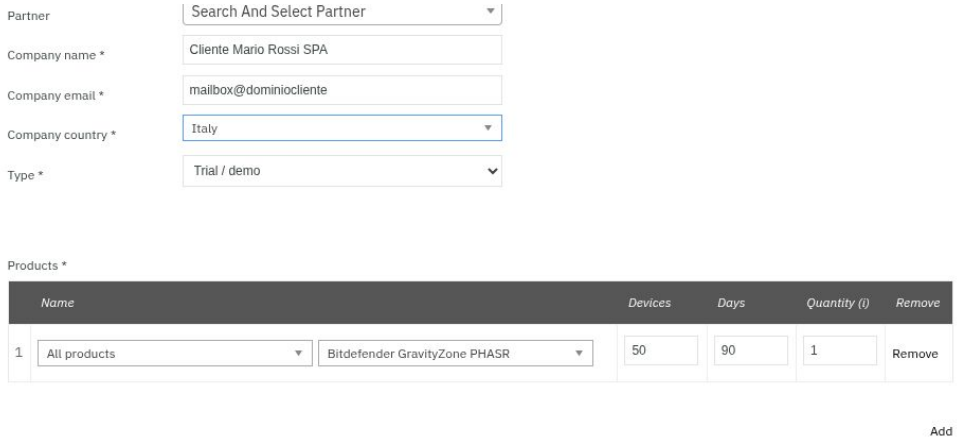
da aggiungere alla suite GravityZone Business Security Enterprise.

** PHASR è già disponibile anche per il licensing mensile per MSP,*
come add-on per i protection model SECURE, SECURE PLUS, SECURE EXTRA

AVANGATE
by ELOVADE

Bitdefender

PHASR - TRIAL ed NFR



Presso il portale Partner Advantage Network (PAN)

- **https://pan.bitdefender.com/**
- **Toolbox → NFR Requests**

i partner possono ottenere licenze TRIAL (max 45gg) ed NFR (max 365gg) per PHASR.

Le licenze TRIAL,
possono essere utilizzate sulle company di nuovi clienti o sulle company di clienti esistenti,
ATTIVATI con licenze PREPAID o TRIAL.

Le licenze NFR,
possono essere utilizzate sulle company create dal partner per uso interno/dimostrativo.

AVANGATE by ELOVADE

Allegati

Bitdefender

vedi sezione Documenti di GoToWebinar

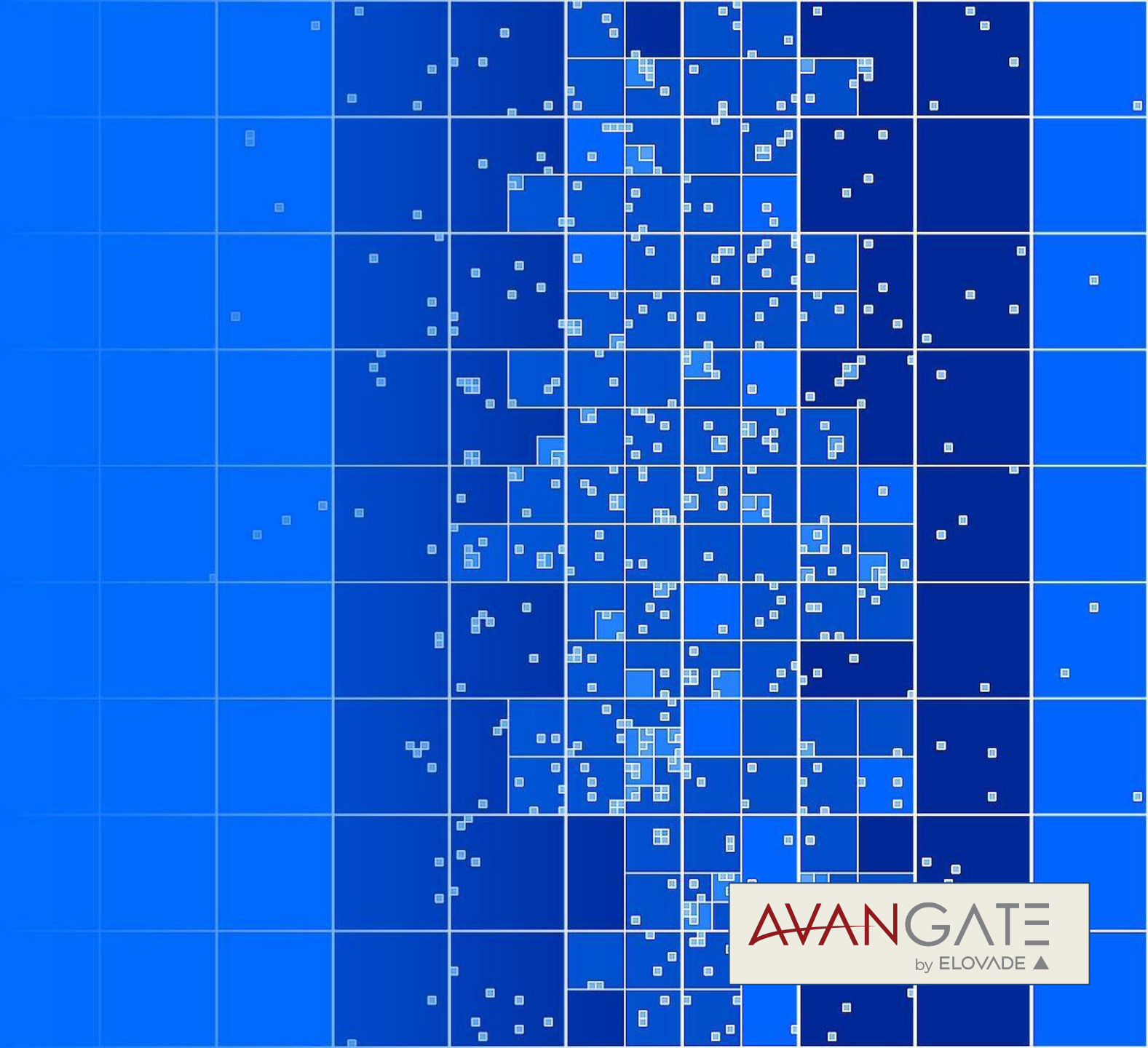
Slide di questa presentazione (pdf)

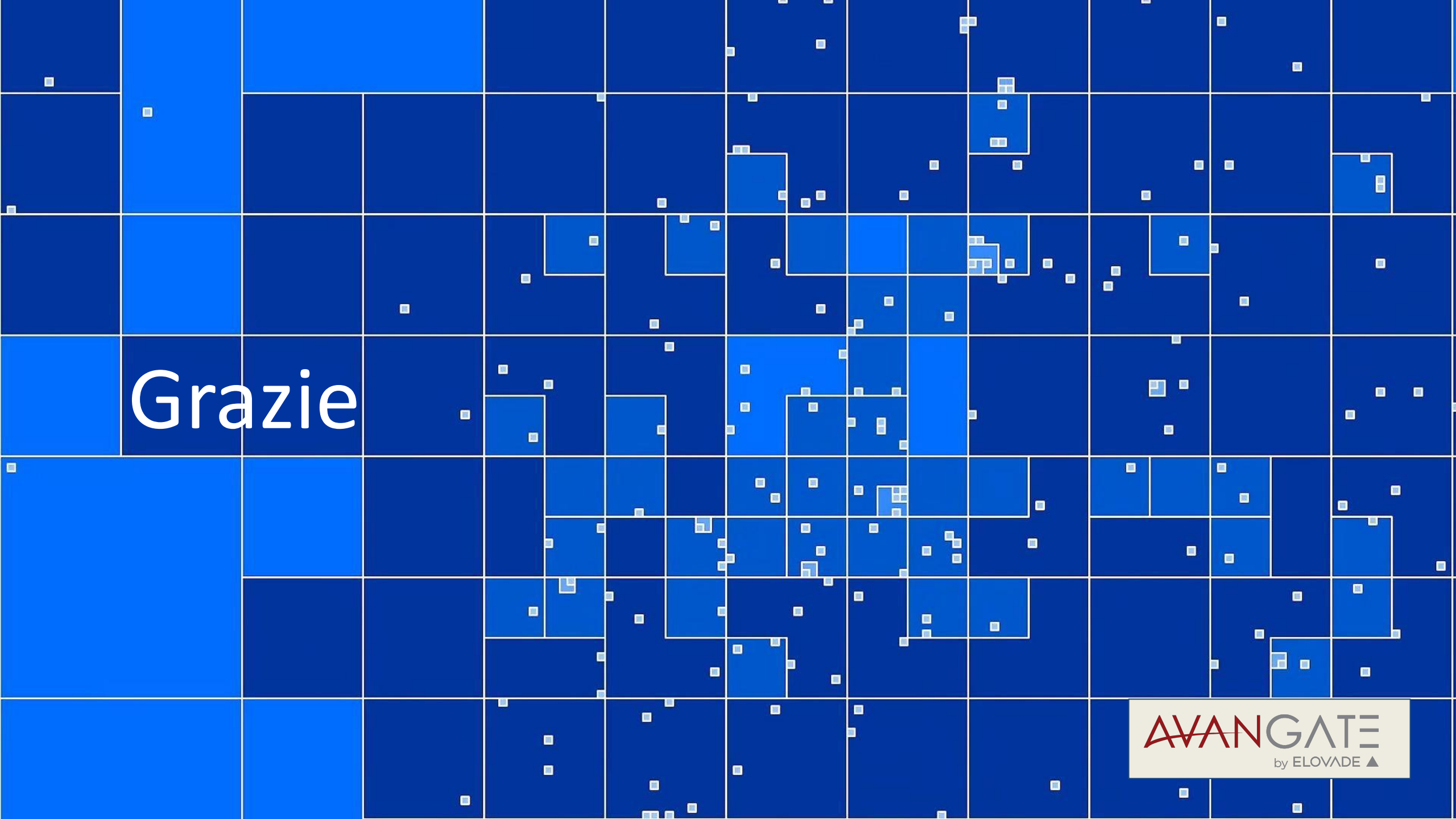
Bitdefender GravityZone PHASR - Datasheet (ENG)

Bitdefender Understanding IOL Attacks - eBook (ENG)

AVANGATE by ELOVADE

Domande




Grazie
AVANGATE
by ELOVADE