Global Leader
In Cybersecurity

Bitdefender®

Alle PHASR geladen und feuerbereit

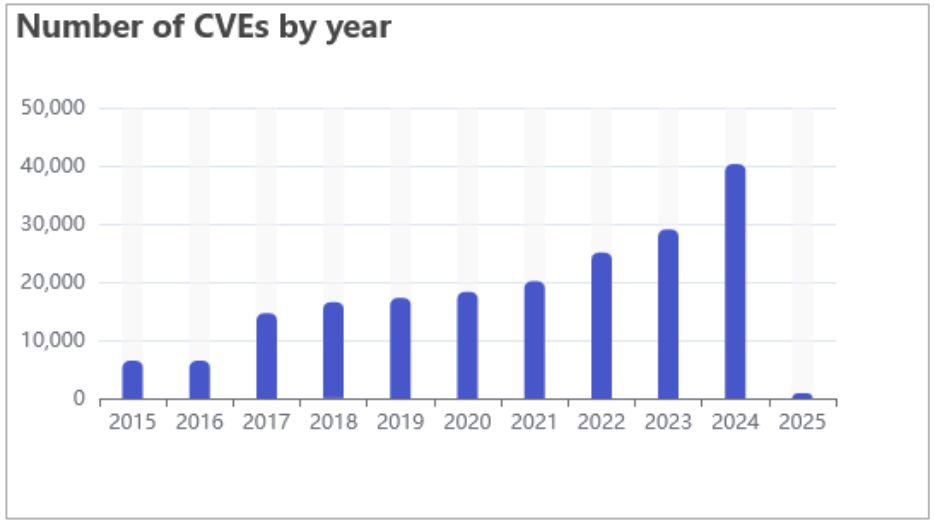
Cristian AVRAM | Manager, Solutions Architect

Bitdefender

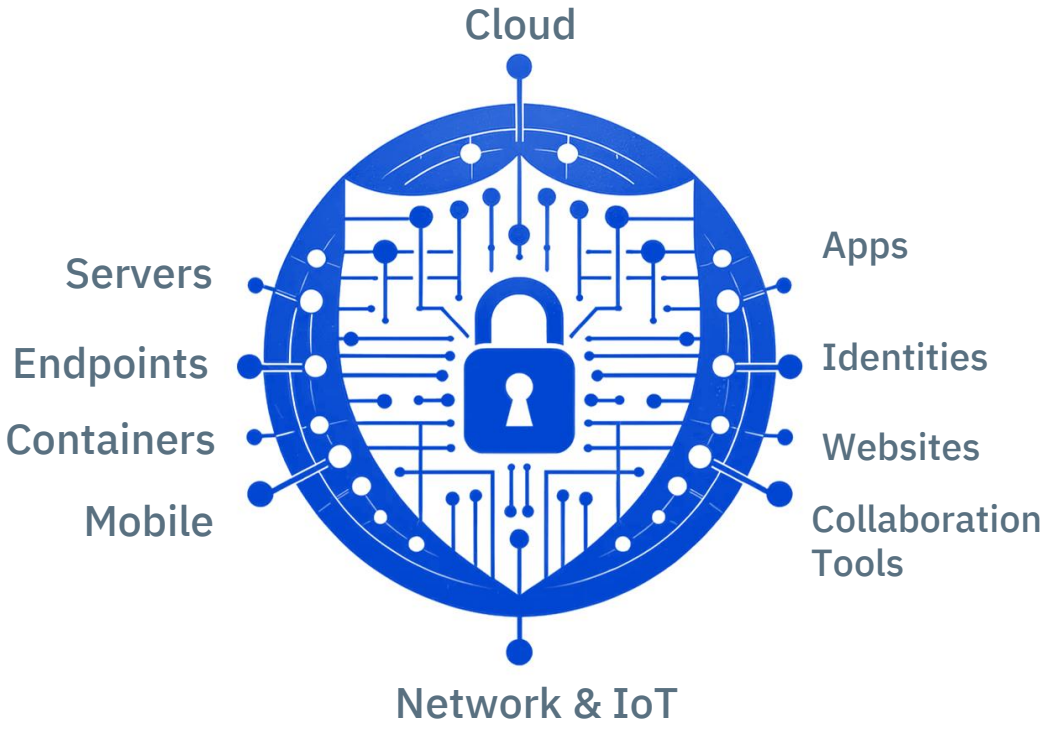
Schwachstellen und Angriffsflächen nehmen rapide zu

PROAKTIVES, RISIKOBASIERTES SCHWACHSTELLEN- UND EXPOSURE-MANAGEMENT REDUZIERT DATENLECKS, SICHERHEITSKOSTEN UND AUFWAND

Mehr Schwachstellen, schnellere Ausnutzung



Ausweitung der Angriffsfläche

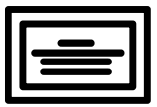


Bitdefender

Herausforderung im Cybersecurity-Risikomanagement

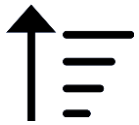
Organisationen wünschen sich

Härtung



Kleine Angriffsfläche, geringes Risiko

Benutzerfreundlichkeit



Kein oder nur geringer Einfluss auf den Geschäftsbetrieb

Verwaltbarkeit

Praktisch umsetzbar

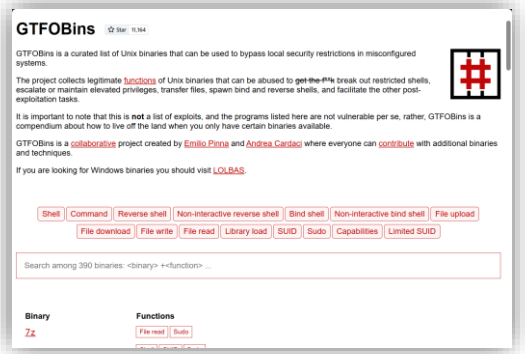
Bitdefender

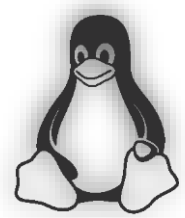
Living off the Land

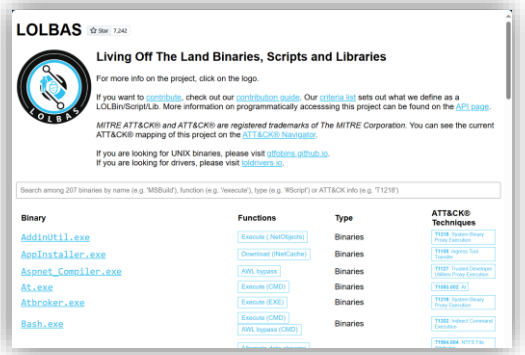
Living off the Land (LotL or LOL) – eine Technik, bei der Angreifer legitime, bereits auf dem Zielsystem vorhandene Tools ausnutzen.

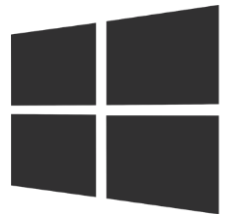
200+

Windows-Binärdateien, die von Bedrohungsakteuren missbraucht werden









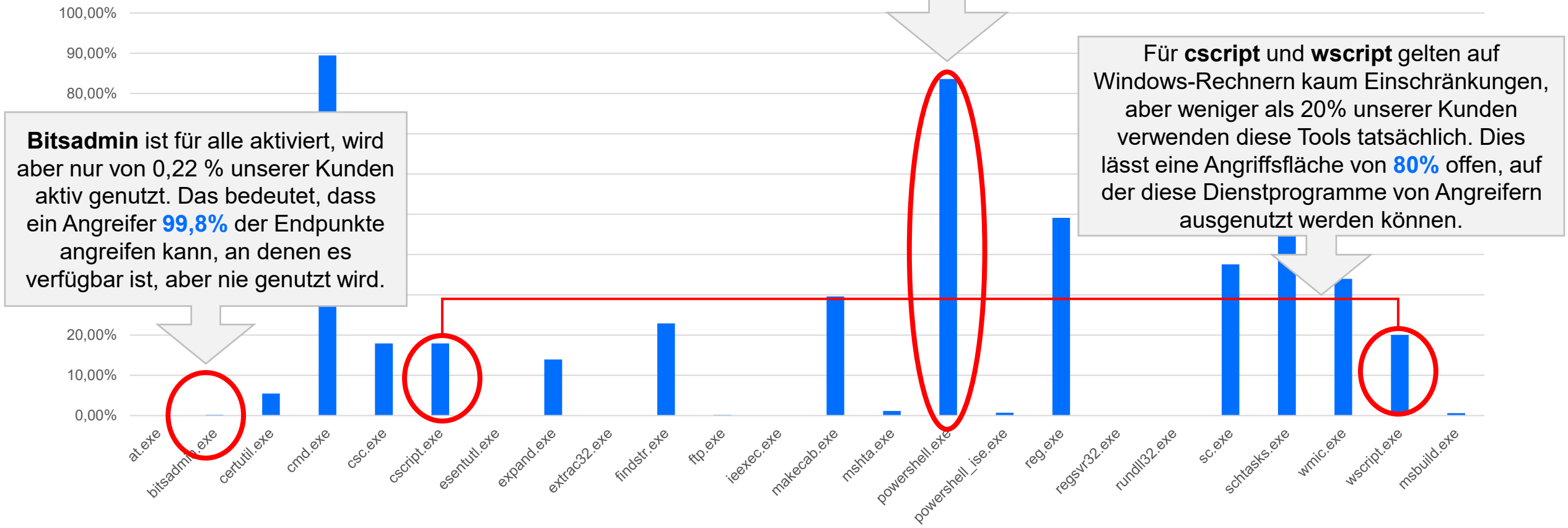
Bitdefender

Die Realität

PowerShell wird zwar von 83,6% unserer Kunden genutzt, aber dennoch kann in ca. **17% der Fälle** ein Angreifer potenziell schädliche Payloads auf Geräten ausführen, auf denen der Benutzer PowerShell nie verwendet hat.

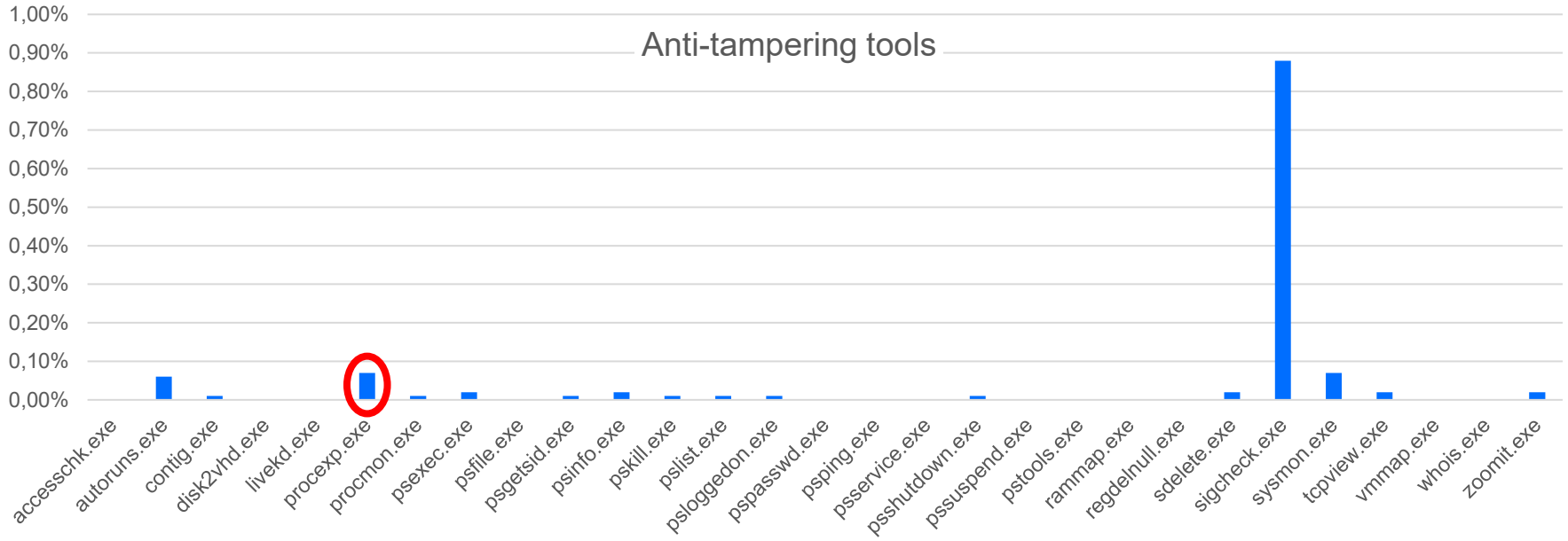
Bitsadmin ist für alle aktiviert, wird aber nur von 0,22 % unserer Kunden aktiv genutzt. Das bedeutet, dass ein Angreifer **99,8%** der Endpunkte angreifen kann, an denen es verfügbar ist, aber nie genutzt wird.

Für **cscript** und **wscript** gelten auf Windows-Rechnern kaum Einschränkungen, aber weniger als 20% unserer Kunden verwenden diese Tools tatsächlich. Dies lässt eine Angriffsfläche von **80%** offen, auf der diese Dienstprogramme von Angreifern ausgenutzt werden können.

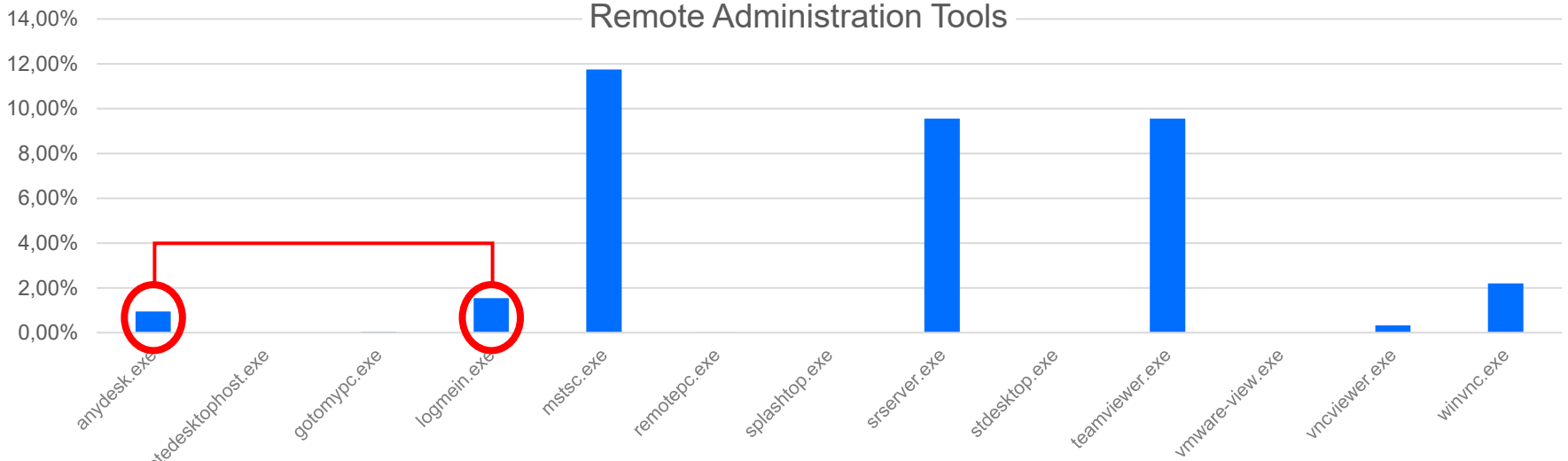


Bitdefender

Die Realität



Process Explorer ist eines der am häufigsten von Angreifern verwendeten Tools, um ein Sicherheitsprodukt zu deaktivieren. Allerdings nutzen nur **0,07%** unserer Kunden dieses Tool. Das bedeutet, dass wir es in **99,3%** der Fälle blockieren können und so verschiedene Angriffe einschränken, ohne den Geschäftsbetrieb zu beeinträchtigen.

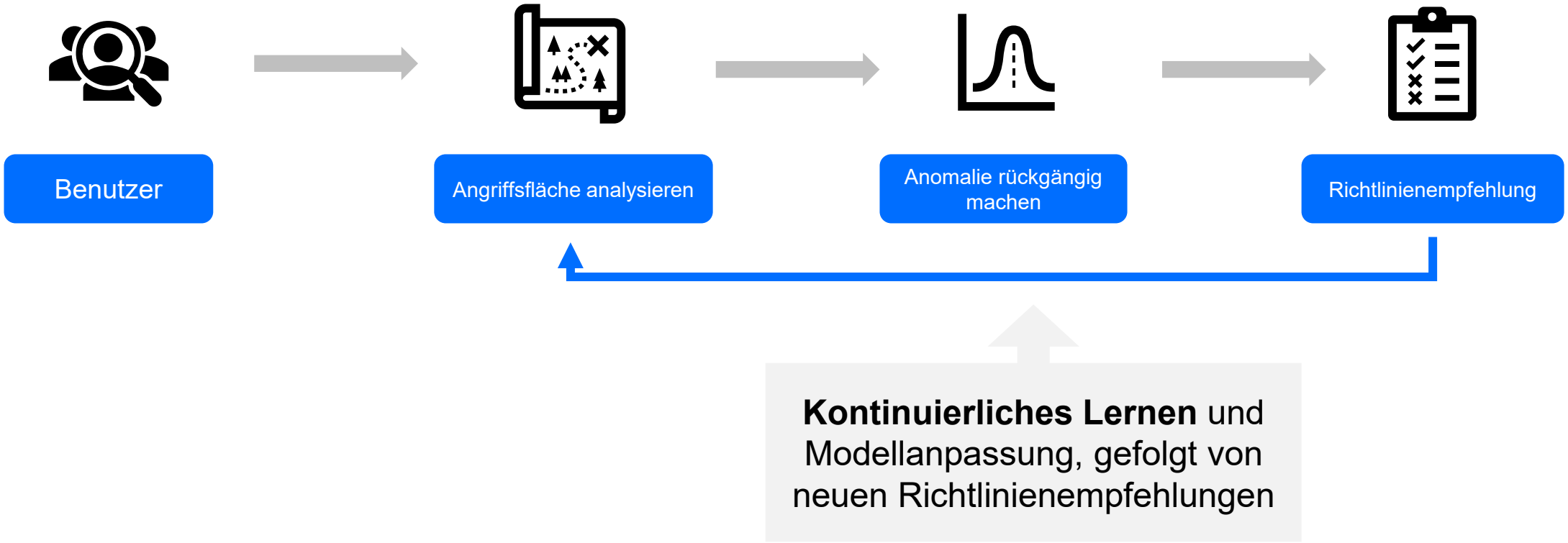


Sowohl **AnyDesk** als auch **LogMeIn** werden in Phishing-basierten Angriffen eingesetzt (als Tools, die das Opfer installieren muss und die dem Angreifer weiteren Fernzugriff auf den Computer ermöglichen). Beachten Sie, dass **weniger als 2%** unserer Kunden diese Tools tatsächlich nutzen.

Bitdefender

Was ist PHASR?

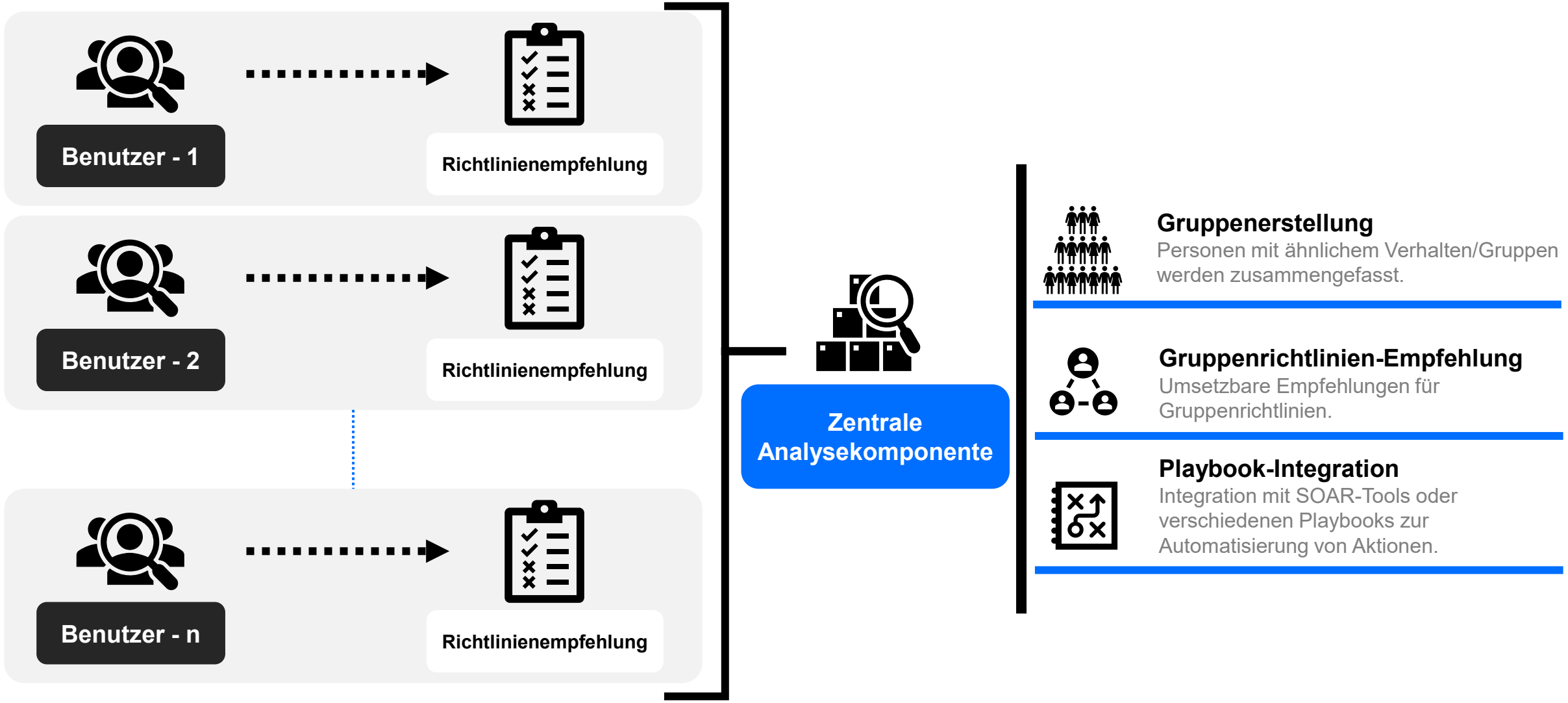
PROACTIVE HARDENING AND ATTACK SURFACE REDUCTION



Bitdefender

Was ist PHASR?

DYNAMISCHE REDUZIERUNG DER ANGRIFFSFLÄCHE UND MINIMIERUNG VON SICHERHEITSVERLETZUNGEN



Bitdefender

Bitdefender GravityZone PHASR

ADAPTIVE ATTACK SURFACE REDUCTION - MASSGESCHNEIDERTE SICHERHEIT FÜR JEDEN NUTZER

- **Die erste Lösung zur maßgeschneiderten Härtung**, basierend auf dem individuellen Verhalten von Nutzern und Endpunkten sowie bekannten Bedrohungsvektoren
- **Die erste dynamische Lösung zur Reduzierung der Angriffsfläche**, die sich kontinuierlich an verändertes Nutzerverhalten anpasst
- Von „One-size-fits-all“ zu **optimaler Härtung** für jeden einzelnen Nutzer
- **Schließt unnötige Angriffsflächen** – z. B. Tools wie PowerShell oder WMI, die von Angreifern ausgenutzt werden können

Bitdefender

Überwachte Tool-Kategorien

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

Bitdefender

Beispiel für einen typischen Angriffsablauf

VON DER ERSTEN E-MAIL BIS ZUR VERSCHLÜSSELUNG DER DATEN

A E-Mail wird geöffnet

B Angehängtes Dokument wird mit Microsoft Word geöffnet

C Microsoft Word führt ein VBA-Makro aus

D Das Word-Makro startet ein PowerShell-Skript

E Das PowerShell-Skript lädt eine Binärdatei herunter

F Das PowerShell-Skript führt die Binärdatei aus

G Die Binärdatei listet alle Dokumente vom lokalen Laufwerk auf

H Die Binärdatei verschlüsselt die aufgelisteten Dokumente

Bitdefender

Beispiel für einen typischen Angriffsablauf

VON DER ERSTEN E-MAIL BIS ZUR VERSCHLÜSSELUNG DER DATEN

- **A** E-Mail wird geöffnet
- **B** Angehängtes Dokument wird mit Microsoft Word geöffnet
- **C** Microsoft Word führt ein VBA-Makro aus
- **D** Das Word-Makro startet ein PowerShell-Skript
- **E** Das PowerShell-Skript lädt eine Binärdatei herunter
- **F** Das PowerShell-Skript führt die Binärdatei aus
- **G** Die Binärdatei listet alle Dokumente vom lokalen Laufwerk auf
- **H** Die Binärdatei verschlüsselt die aufgelisteten Dokumente

Jede der 255 prädiktiven Sicherheitsmeldungen entspricht einer Kette von A…H Wahrscheinlichkeiten

Prädiktive Sicherheitsmeldung:

1 = A
2 = A → B
3 = A → C
…
9 = B
10 = B → C
…
20 = A → B → C
…
120 = A → B → C → D → E → F → G → H
121 = B → C → D → E → F → G → H
…
254 = G → H
255 = H

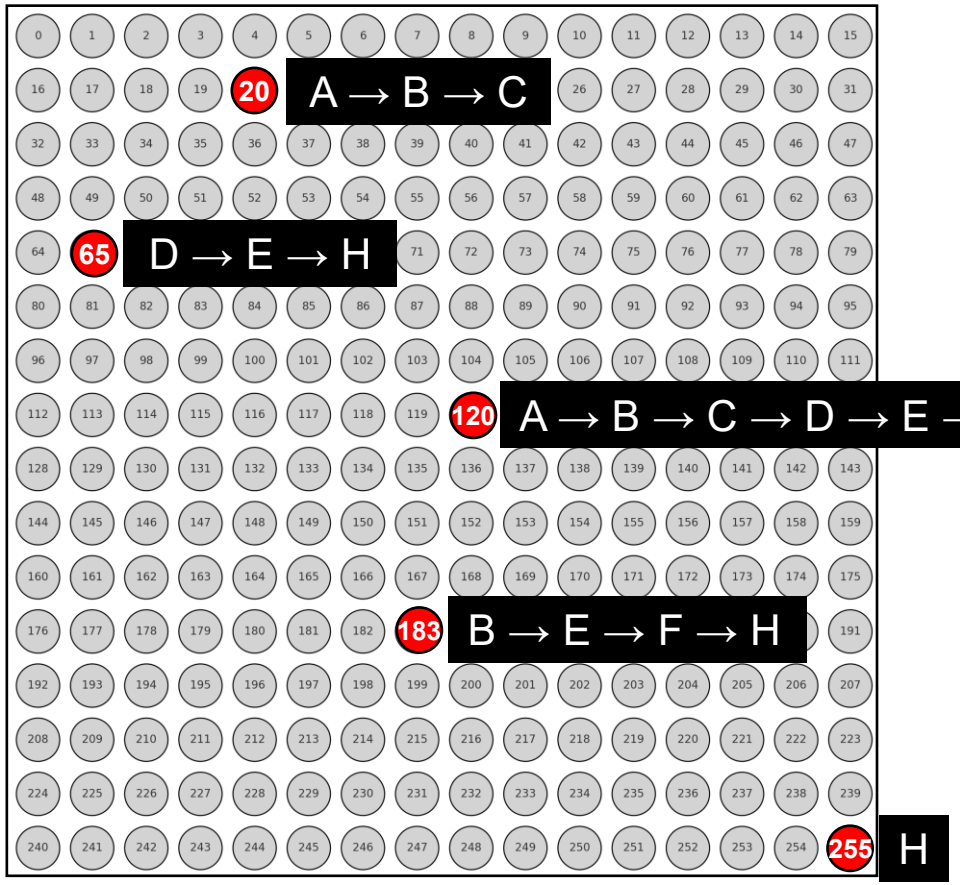
Bitdefender

Beispiel für einen typischen Angriffsablauf

VON DER ERSTEN E-MAIL BIS ZUR VERSCHLÜSSELUNG DER DATEN

- **A** E-Mail wird geöffnet
- **B** Angehängtes Dokument wird mit Microsoft Word geöffnet
- **C** Microsoft Word führt ein VBA-Makro aus
- **D** Das Word-Makro startet ein PowerShell-Skript
- **E** Das PowerShell-Skript lädt eine Binärdatei herunter
- **F** Das PowerShell-Skript führt die Binärdatei aus
- **G** Die Binärdatei listet alle Dokumente vom lokalen Laufwerk auf
- **H** Die Binärdatei verschlüsselt die aufgelisteten Dokumente

Abbildung aller Meldungen auf einer 16×16-Karte



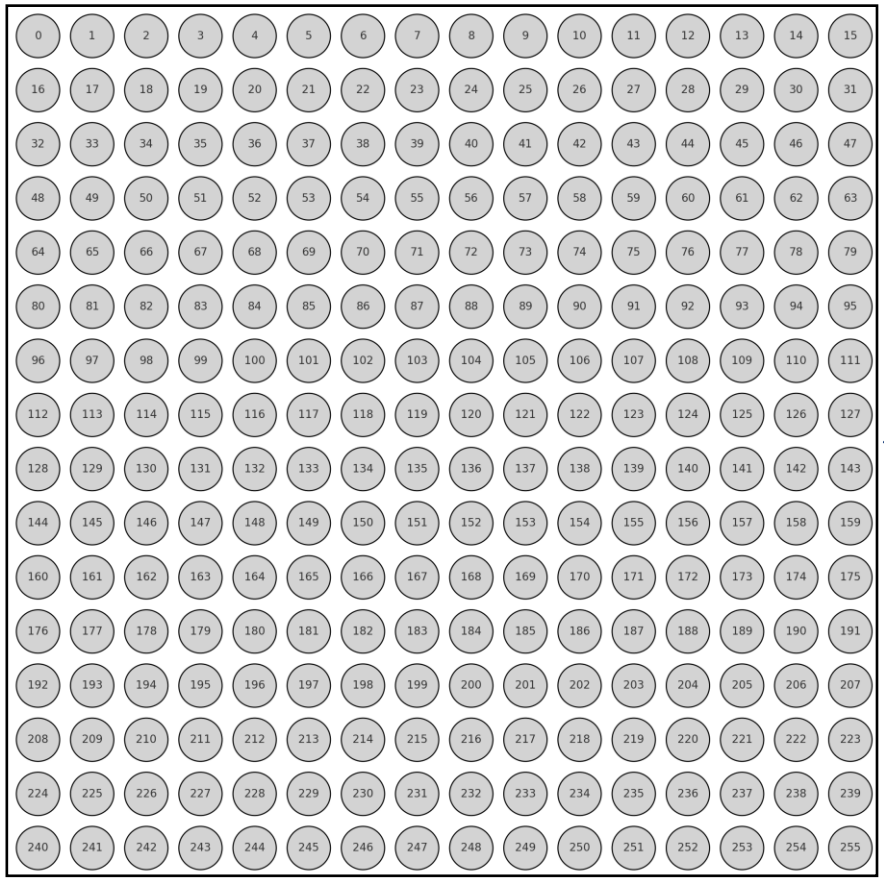
Bitdefender

Beispiel für einen typischen Angriffsablauf

VON DER ERSTEN E-MAIL BIS ZUR VERSCHLÜSSELUNG DER DATEN

- **A** E-Mail wird geöffnet
- **B** Angehängtes Dokument wird mit Microsoft Word geöffnet
- **C** Microsoft Word führt ein VBA-Makro aus
- **D** Das Word-Makro startet ein PowerShell-Skript
- **E** Das PowerShell-Skript lädt eine Binärdatei herunter
- **F** Das PowerShell-Skript führt die Binärdatei aus
- **G** Die Binärdatei listet alle Dokumente vom lokalen Laufwerk auf
- **H** Die Binärdatei verschlüsselt die aufgelisteten Dokumente

Abbildung aller Meldungen auf einer 16×16-Karte



In der Praxis bezeichnen wir diese Karte als **Angriffsfläche**. Jeder dieser Kreise stellt dabei einen potenziellen **Angriffsvektor** bzw. **Angriffsschritt** dar.

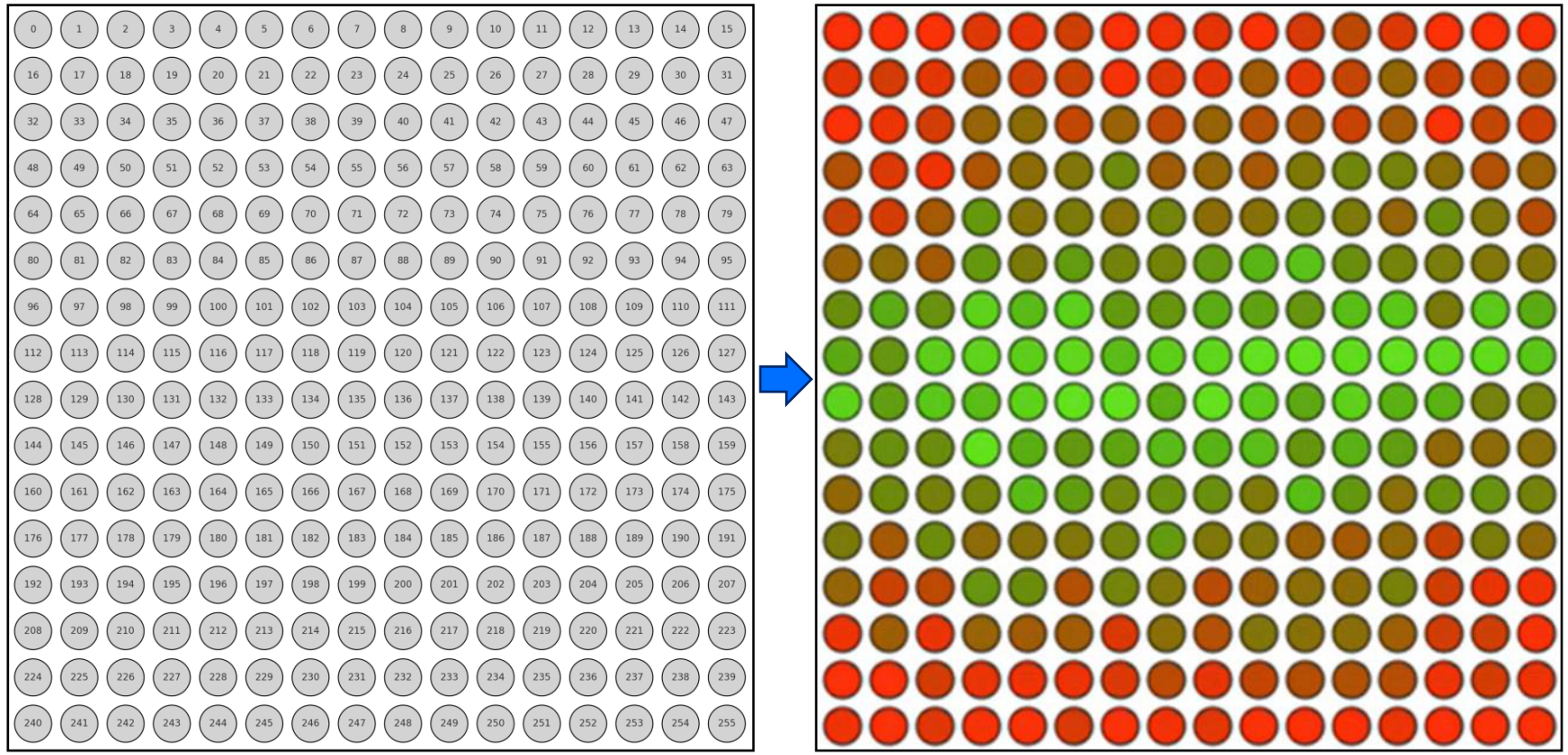
Bitdefender

Beispiel für einen typischen Angriffsablauf

VON DER ERSTEN E-MAIL BIS ZUR VERSCHLÜSSELUNG DER DATEN

- **A** E-Mail wird geöffnet
- **B** Angehängtes Dokument wird mit Microsoft Word geöffnet
- **C** Microsoft Word führt ein VBA-Makro aus
- **D** Das Word-Makro startet ein PowerShell-Skript
- **E** Das PowerShell-Skript lädt eine Binärdatei herunter
- **F** Das PowerShell-Skript führt die Binärdatei aus
- **G** Die Binärdatei listet alle Dokumente vom lokalen Laufwerk auf
- **H** Die Binärdatei verschlüsselt die aufgelisteten Dokumente

Für diese Matrix lässt sich eine Heatmap erstellen



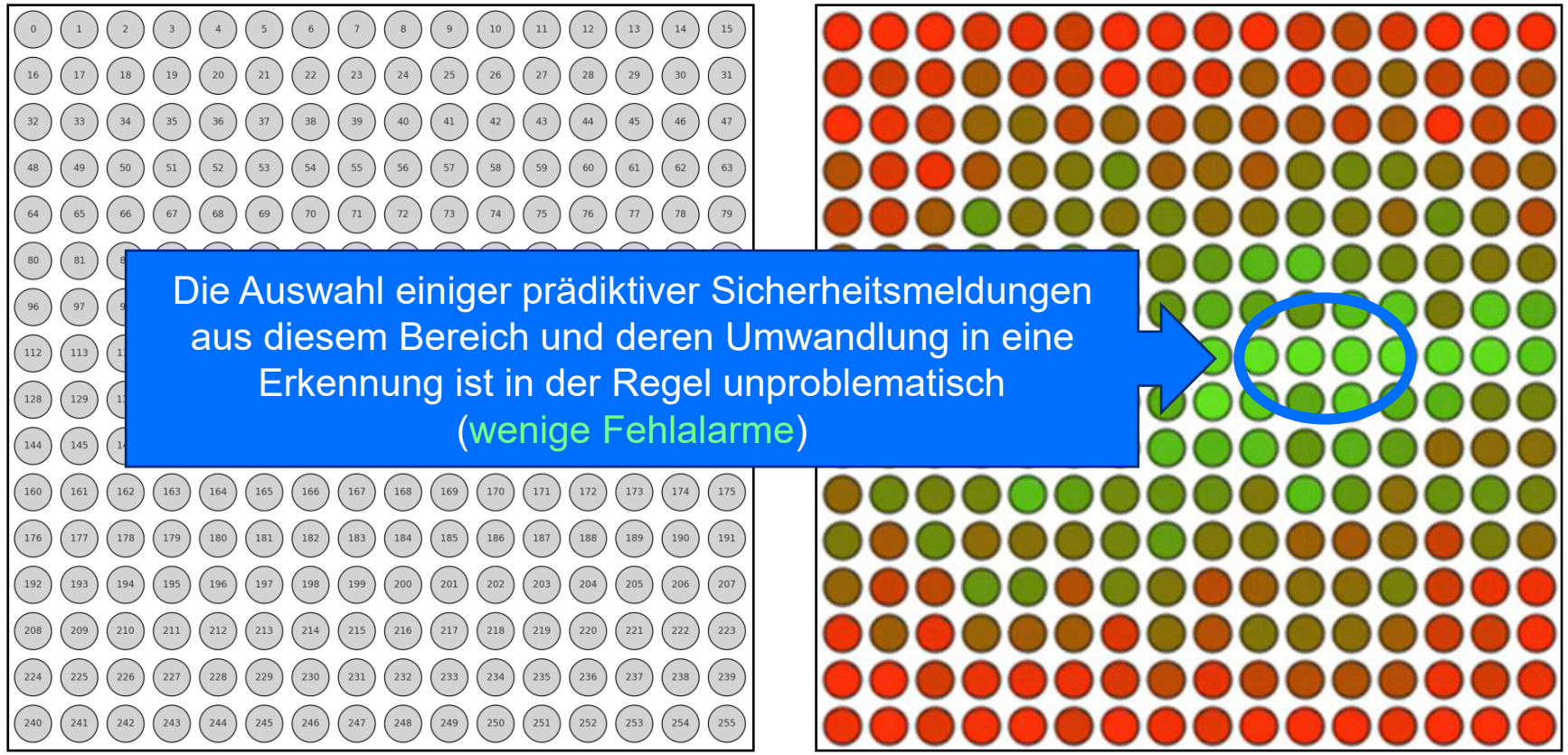
Bitdefender

Beispiel für einen typischen Angriffsablauf

VON DER ERSTEN E-MAIL BIS ZUR VERSCHLÜSSELUNG DER DATEN

- **A** E-Mail wird geöffnet
- **B** Angehängtes Dokument wird mit Microsoft Word geöffnet
- **C** Microsoft Word führt ein VBA-Makro aus
- **D** Das Word-Makro startet ein PowerShell-Skript
- **E** Das PowerShell-Skript lädt eine Binärdatei herunter
- **F** Das PowerShell-Skript führt die Binärdatei aus
- **G** Die Binärdatei listet alle Dokumente vom lokalen Laufwerk auf
- **H** Die Binärdatei verschlüsselt die aufgelisteten Dokumente

Für diese Matrix lässt sich eine Heatmap erstellen



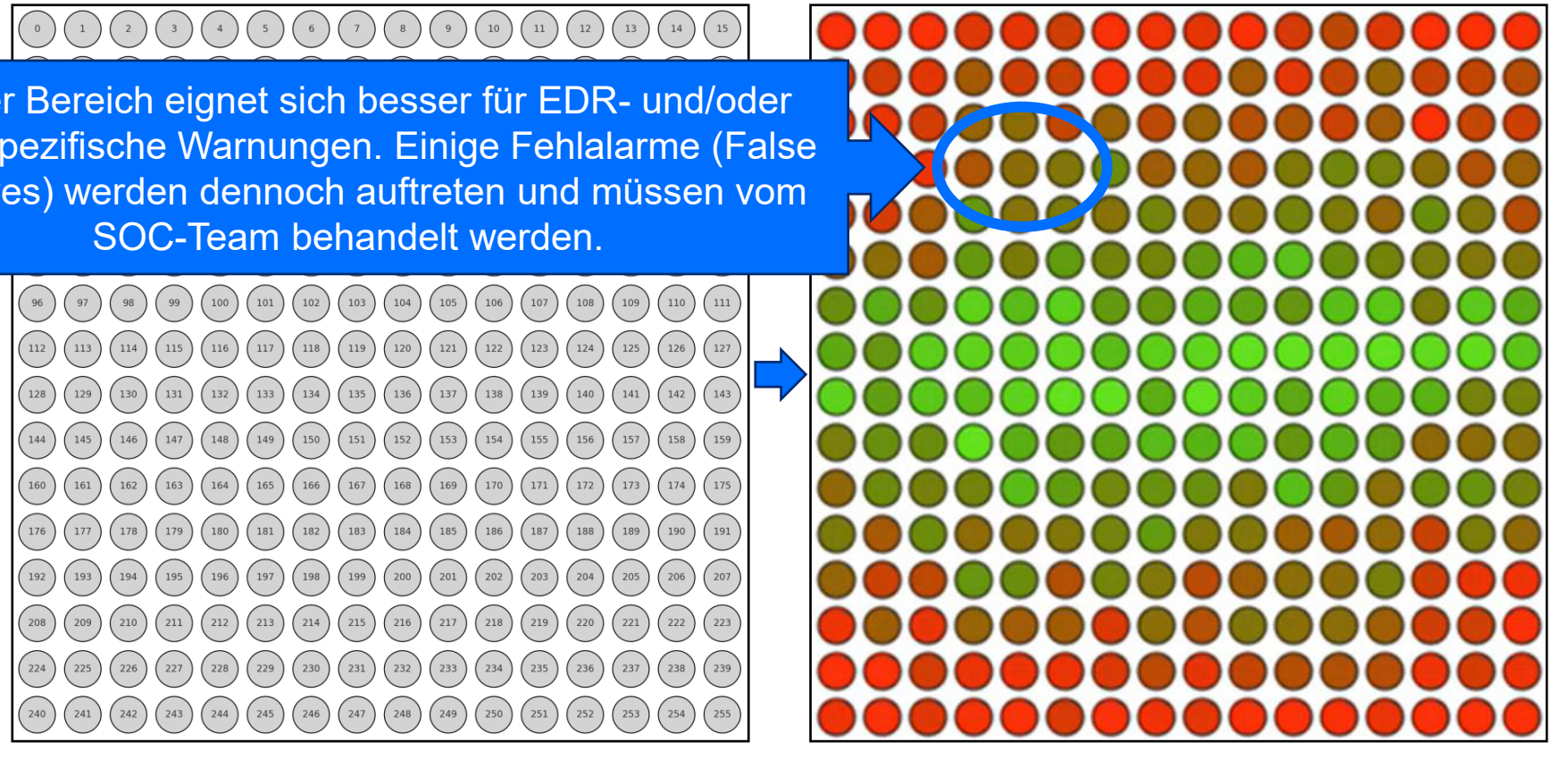
Bitdefender

Beispiel für einen typischen Angriffsablauf

VON DER ERSTEN E-MAIL BIS ZUR VERSCHLÜSSELUNG DER DATEN

- **A** E-Mail wird geöffnet
- **B** Angehängtes Dokument wird mit Microsoft Word geöffnet
- **C** Microsoft Word führt ein VBA-Makro aus
- **D** Das Word-Makro startet ein PowerShell-Skript
- **E** Das PowerShell-Skript lädt eine Binärdatei herunter
- **F** Das PowerShell-Skript führt die Binärdatei aus
- **G** Die Binärdatei listet alle Dokumente vom lokalen Laufwerk auf
- **H** Die Binärdatei verschlüsselt die aufgelisteten Dokumente

Für diese Matrix lässt sich eine Heatmap erstellen



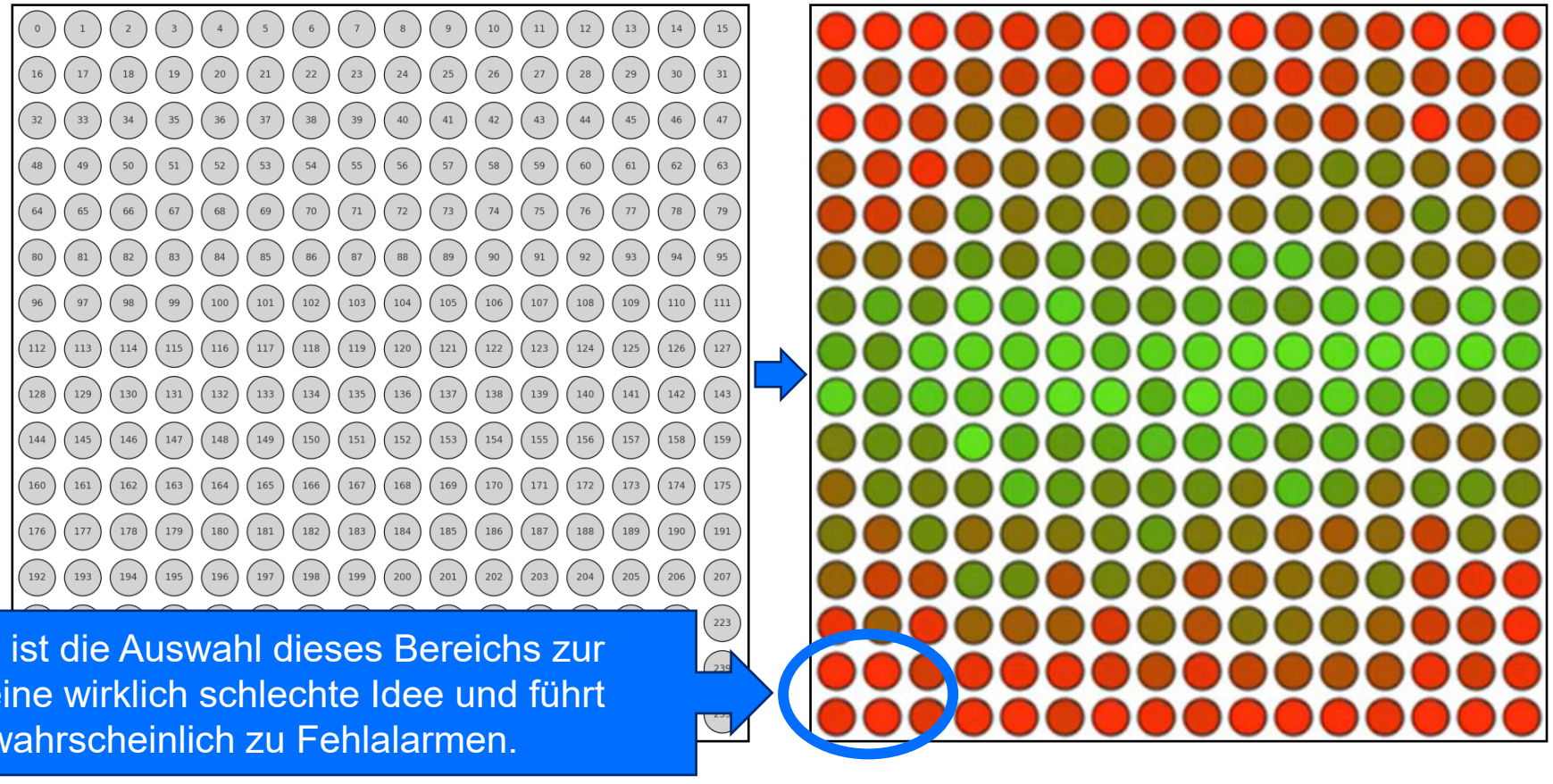
Bitdefender

Beispiel für einen typischen Angriffsablauf

VON DER ERSTEN E-MAIL BIS ZUR VERSCHLÜSSELUNG DER DATEN

- **A** E-Mail wird geöffnet
- **B** Angehängtes Dokument wird mit Microsoft Word geöffnet
- **C** Microsoft Word führt ein VBA-Makro aus
- **D** Das Word-Makro startet ein PowerShell-Skript
- **E** Das PowerShell-Skript lädt eine Binärdatei herunter
- **F** Das PowerShell-Skript führt die Binärdatei aus
- **G** Die Binärdatei listet alle Dokumente vom lokalen Laufwerk auf
- **H** Die Binärdatei v… die aufgelisteten…

Für diese Matrix lässt sich eine Heatmap erstellen

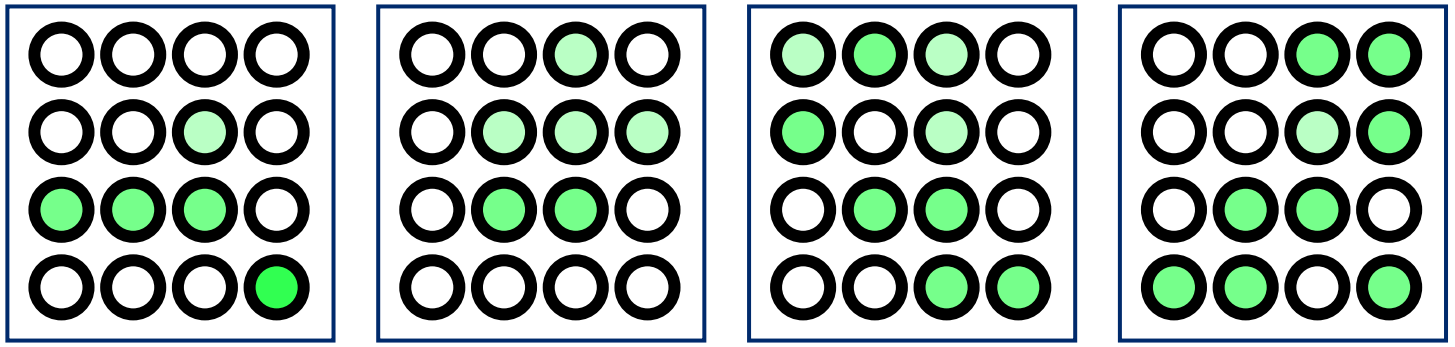


Andererseits ist die Auswahl dieses Bereichs zur Erkennung eine wirklich schlechte Idee und führt höchstwahrscheinlich zu Fehlalarmen.

Bitdefender

Der Wettbewerbsvorteil von PHASR

ERFASSUNG VON ENDPOINT- UND VERHALTENSBASIERTEN DATEN ZUR ERSTELLUNG INDIVIDUELLER RISIKOPROFILE

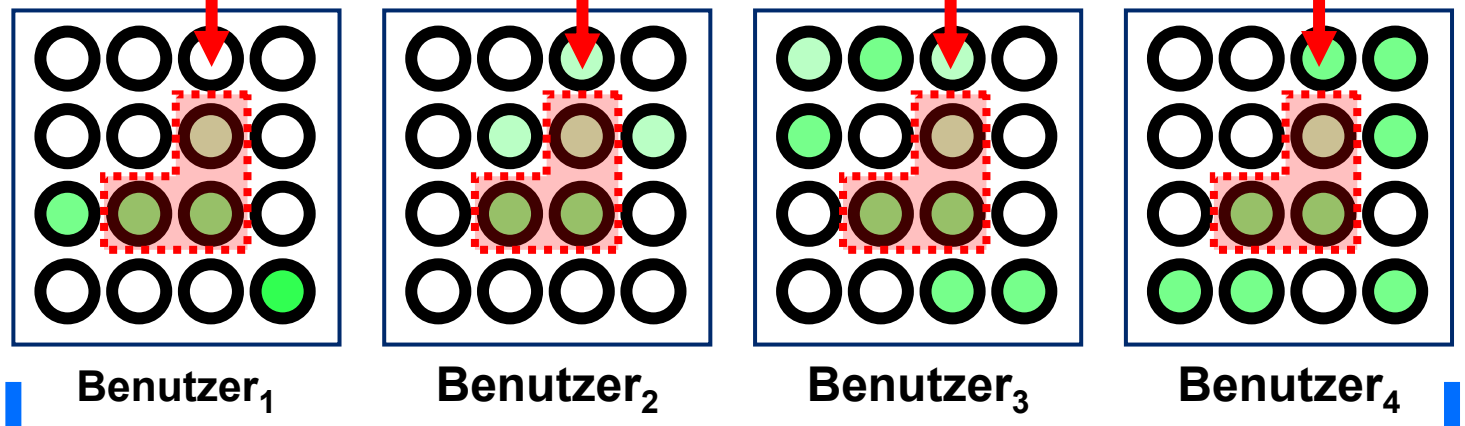


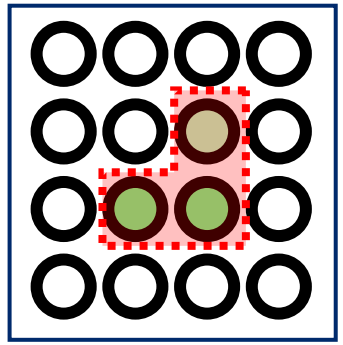
Bitdefender

Der Wettbewerbsvorteil von PHASR

ERFASSUNG VON ENDPOINT- UND VERHALTENSBASIERTEN DATEN ZUR ERSTELLUNG INDIVIDUELLER RISIKOPROFILE

Bei klassischen Sicherheitslösungen werden nur die üblichen Angriffsflächen verwaltet





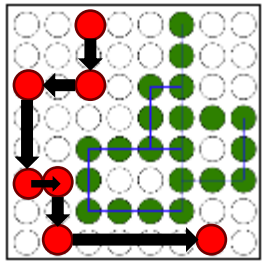
PHASR verwendet eine unterschiedliche Erkennung für jeden Benutzer, die sich **dynamisch** anpasst und **optimal für den jeweiligen Benutzer** ist (nicht für alle gleich).

Andere Lösungen (Eine gute Lösung für alle, aber NICHT DIE BESTE LÖSUNG.)

Bitdefender

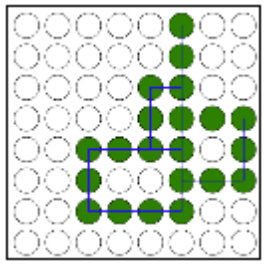
Der Wettbewerbsvorteil von PHASR

Angreifer

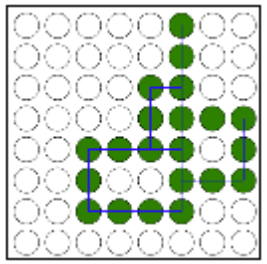


Angriffsmuster vom Angreifer identifiziert

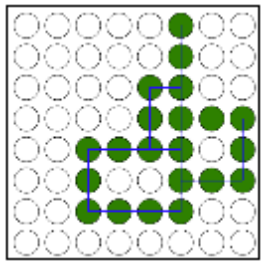
Unternehmen X, geschützt durch Produkt A



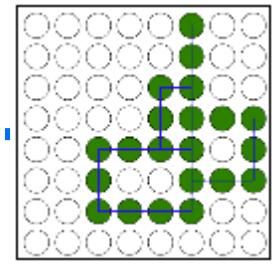
Benutzer$_1$ – Schutz der Angriffsfläche



Benutzer$_2$ – Schutz der Angriffsfläche



Benutzer$_3$ – Schutz der Angriffsfläche

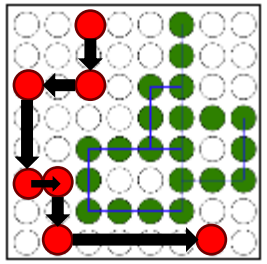


Benutzer$_n$ – Schutz der Angriffsfläche

Bitdefender

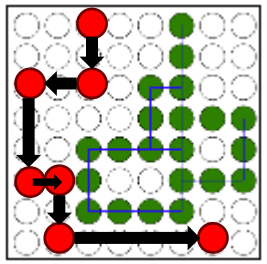
Der Wettbewerbsvorteil von PHASR

Angreifer

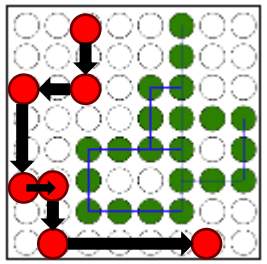


Angriffsmuster vom Angreifer identifiziert

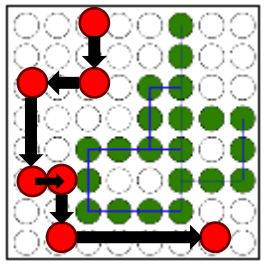
Unternehmen X, geschützt durch Produkt A



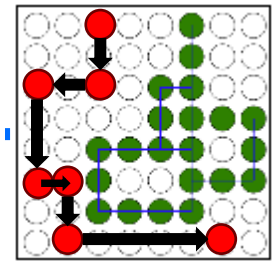
Benutzer$_1$ – Schutz der Angriffsfläche



Benutzer$_2$ – Schutz der Angriffsfläche



Benutzer$_3$ – Schutz der Angriffsfläche

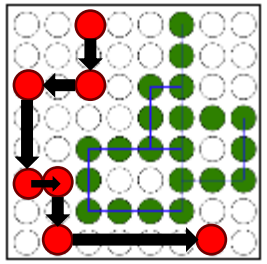


Benutzer$_n$ – Schutz der Angriffsfläche

Bitdefender

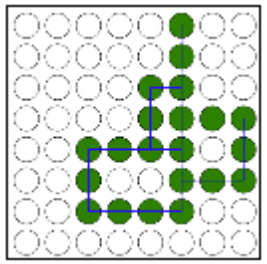
Der Wettbewerbsvorteil von PHASR

Angreifer

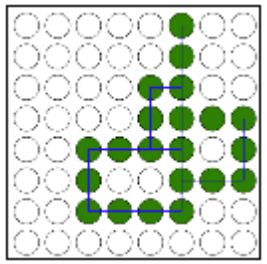


Angriffsmuster vom Angreifer identifiziert

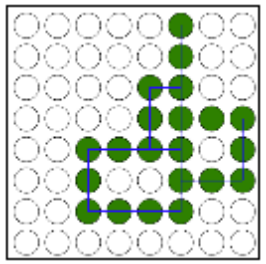
Unternehmen X, geschützt durch Produkt A



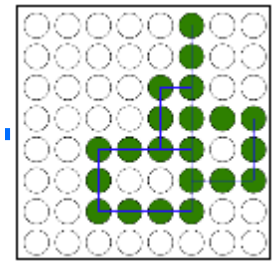
Benutzer$_1$ – Schutz der Angriffsfläche



Benutzer$_2$ – Schutz der Angriffsfläche

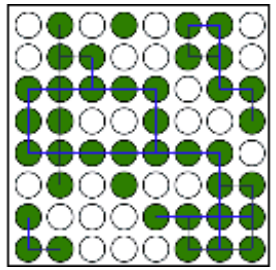


Benutzer$_3$ – Schutz der Angriffsfläche

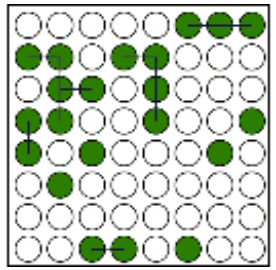


Benutzer$_n$ – Schutz der Angriffsfläche

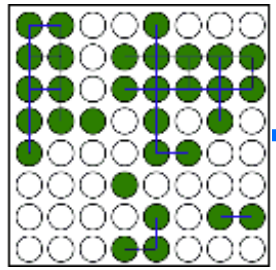
Unternehmen X, geschützt durch PHASR



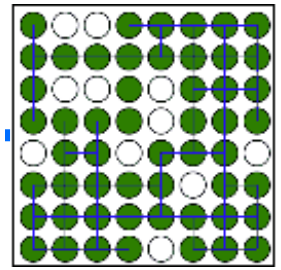
Benutzer$_1$ – Schutz der Angriffsfläche



Benutzer$_2$ – Schutz der Angriffsfläche



Benutzer$_3$ – Schutz der Angriffsfläche

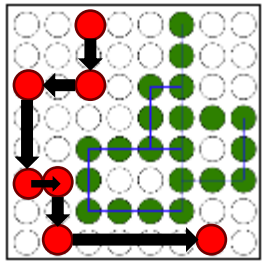


Benutzer$_n$ – Schutz der Angriffsfläche

Bitdefender

Der Wettbewerbsvorteil von PHASR

Angreifer



Angriffsmuster vom Angreifer identifiziert

Unternehmen X, geschützt durch Produkt A

Diese Muster werden dynamisch aktualisiert

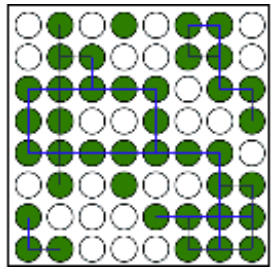
Benutzer$_1$ – Schutz der Angriffsfläche

Benutzer$_2$ – Schutz der Angriffsfläche

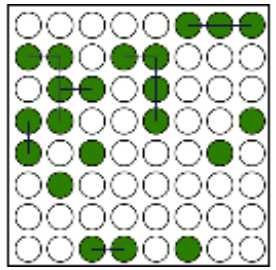
Benutzer$_3$ – Schutz der Angriffsfläche

Benutzer$_n$ – Schutz der Angriffsfläche

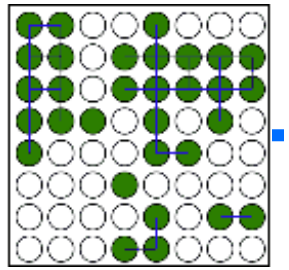
Unternehmen X, geschützt durch PHASR



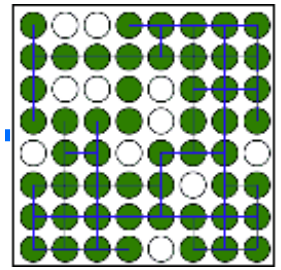
Benutzer$_1$ – Schutz der Angriffsfläche



Benutzer$_2$ – Schutz der Angriffsfläche



Benutzer$_3$ – Schutz der Angriffsfläche

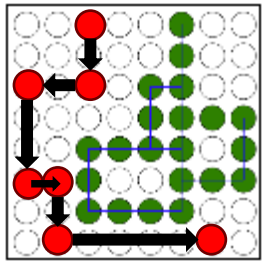


Benutzer$_n$ – Schutz der Angriffsfläche

Bitdefender

Der Wettbewerbsvorteil von PHASR

Angreifer



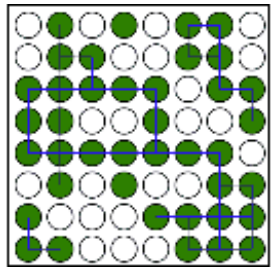
Angriffsmuster vom Angreifer identifiziert

Unternehmen X, geschützt durch Produkt A

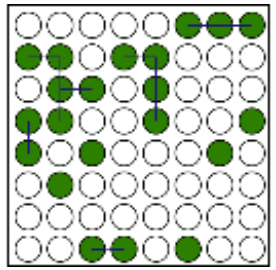
So sieht PHASR in der Realität aus (ständig in Veränderung & Weiterentwicklung)

2^{850}

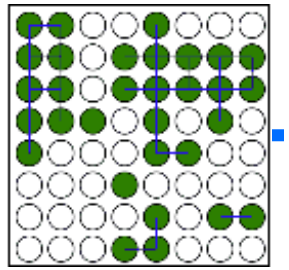
Unternehmen X, geschützt durch PHASR



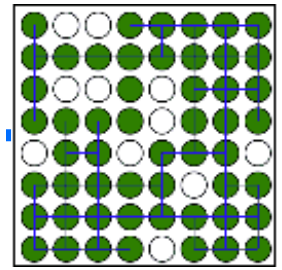
Benutzer$_1$ – Schutz der Angriffsfläche



Benutzer$_2$ – Schutz der Angriffsfläche



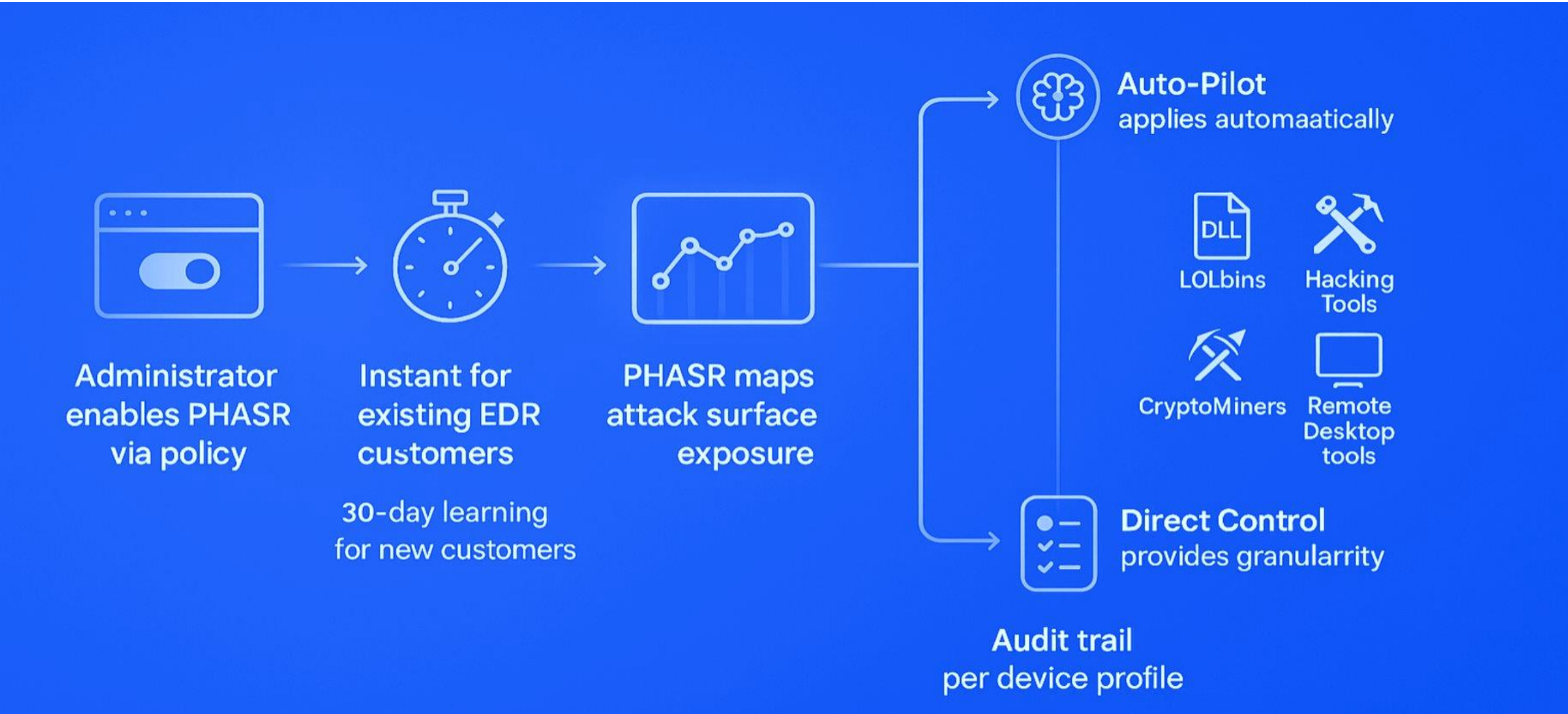
Benutzer$_3$ – Schutz der Angriffsfläche



Benutzer$_n$ – Schutz der Angriffsfläche

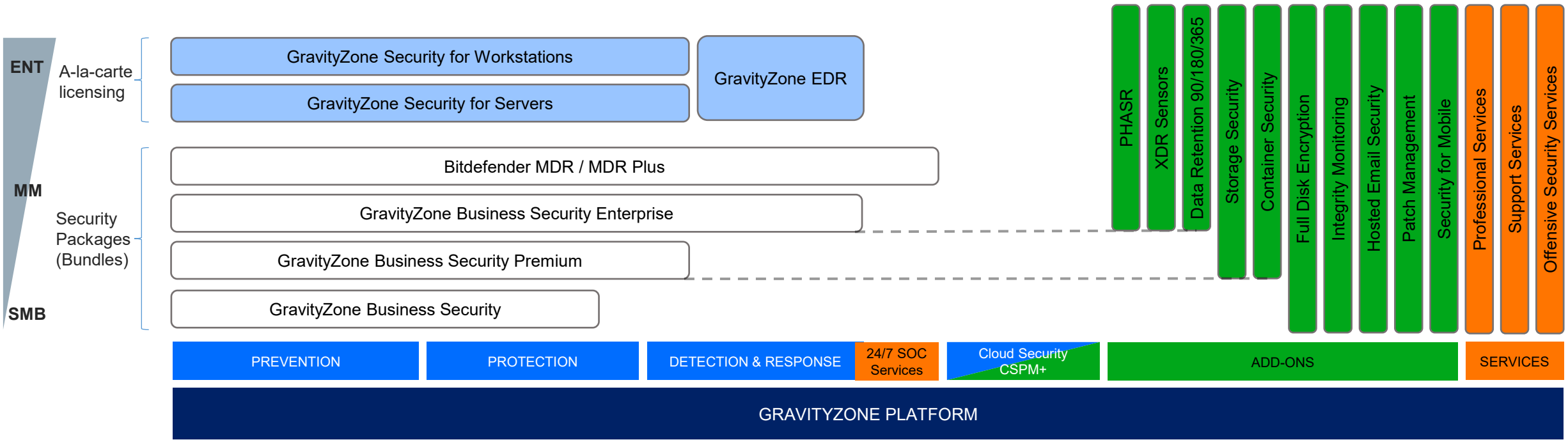
Bitdefender

PHASR - Sofortiges Lernen, Autopilot und Direkte Kontrolle



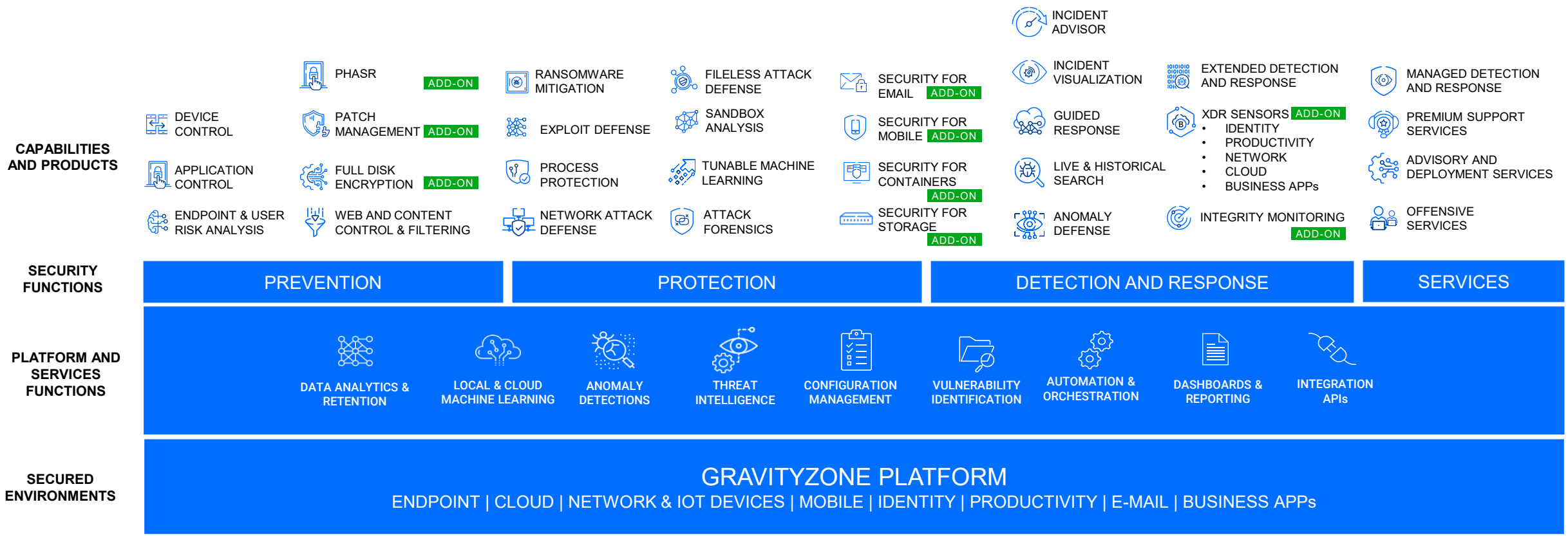
Bitdefender

GravityZone Bundles & Add-ons



Bitdefender

Blueprint for Cyber Resilience



Bitdefender

GravityZone

ON-PREMISE vs CLOUD

(only main Features and Differences shown)

FEATURE / SECURITY TECHNOLOGY	ON-PREMISE	CLOUD
MANAGEMENT & INTEGRATION		
▼ Multi Tenancy		✓
▼ Active Directory Integration	✓	✓
▼ vCenter Server Integration	✓	
▼ Xen Server Integration	✓	
▼ Nutanix Prism Integration	✓	
▼ AWS Integration	✓	✓
▼ Azure Integration	✓	
DETECTION AND RESPONSE MODULES		
▼ EDR	✓	✓
▼ XDR		✓
▼ Search Queries (Historical & Live)		✓
▼ Full Remote Shell		✓
▼ Yara Rules		✓
HARDENING		
▼ Endpoint Risk Analytics (ERA)		✓
▼ PHASR		✓
▼ Application Control (Blacklisting)	✓	✓
▼ Application Control (Whitelisting)	✓	
▼ Integrity Monitoring		✓
SECURITY SERVICES / ADD-ONs		
▼ Security for Mobile Devices	✓*	✓
▼ Email Security		✓
▼ CSPM+		✓
SERVICES		
▼ MDR		✓

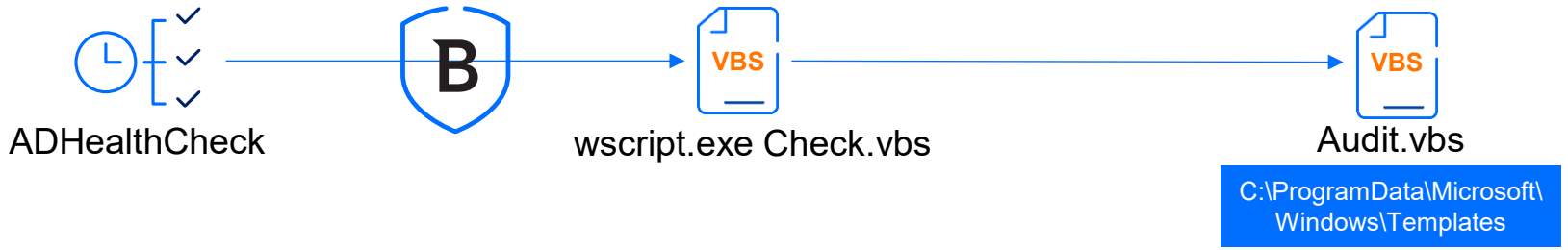
*legacy

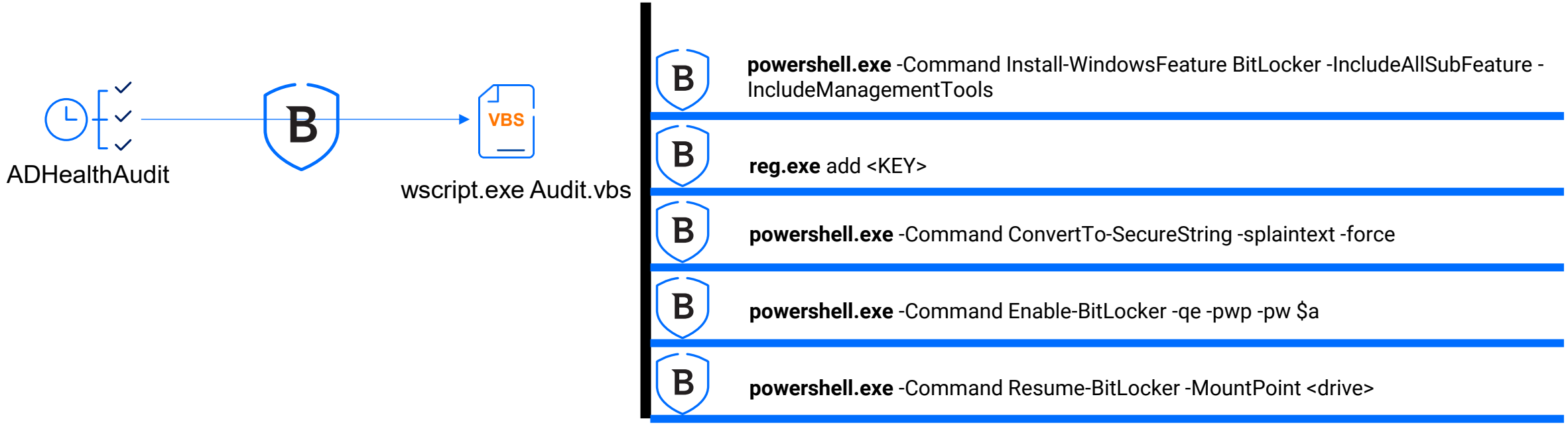
Bitdefender

PHASR in Aktion

BEISPIEL EINES SUPPLY-CHAIN-ANGRIFFS

Prozessausführung



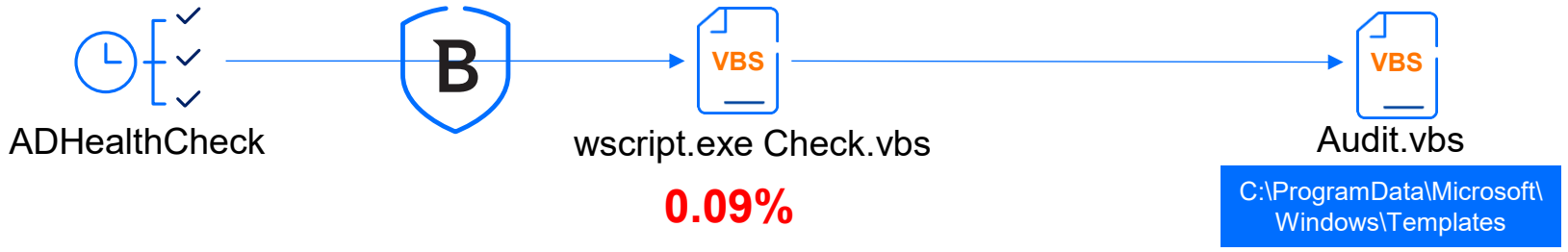


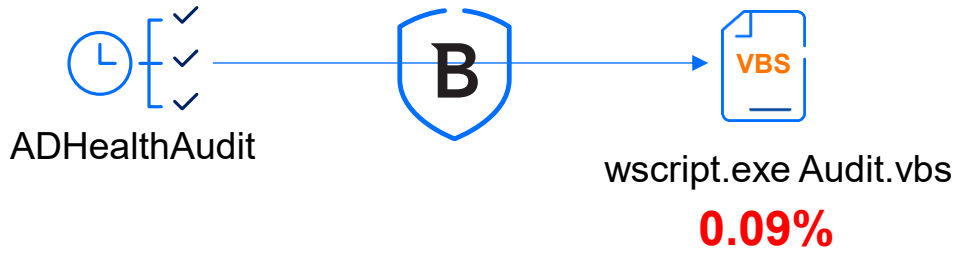
Bitdefender

PHASR in Aktion

BEISPIEL EINES SUPPLY-CHAIN-ANGRIFFS

Prozessausführung





BitLocker process: 0.13%

*Wahrscheinlichkeit, dass es sich um eine legitime Aktion / einen legitimen Befehl handelt

B	**powershell.exe** -Command Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools	0.0000172%
B	**reg.exe** add <KEY>	
B	**powershell.exe** -Command ConvertTo-SecureString -splaintext -force	0.0164%
B	**powershell.exe** -Command Enable-BitLocker -qe -pwp -pw $a	0.0112%
B	**powershell.exe** -Command Resume-BitLocker -MountPoint <drive>	0.00228%

Trusted.
Always.