Moderner IT-Schutz

Live-Webinar in Kooperation mit MATRIX42

Thomas Egli & Tony Förster

03. November 2020

Agenda

- Vorstellung von Armacom AG und Matrix42 AG
- Moderner IT-Schutz – gegen was genau?
  - Schutz des Endpoint gegen Einbruch von aussen
  - Schutz des Endpoint gegen Ausbreitung von innen
- Fragerunde

Haben Sie im Verlauf der Präsentation Fragen? Schreiben Sie diese in den Chat von GoToMeeting und wir versuchen alle offenen Fragen am Ende der Präsentation zu beantworten.

Dienstleitungen mit dem Blick für‘s Ganze

- IT-Infrastruktur Dienstleister seit 1997
- Sitz in Pratteln BL mit 30 Mitarbeitenden
- Projekte in der gesamten Schweiz

MATRIX42

- Weltweit tätiger Softwarehersteller aus Deutschland seit 1992
- Endpoint Security
- Unified Endpoint Management
- Enterprise Service Management

Moderner IT-Schutz – gegen was genau?

Wir konzentrieren uns heute auf den Endpoint und die zentralen Gefahren

- Datenklau
- Viren / Malware

Der Endpoint ist ein System mit einem Betriebssystem

Warum ist der moderne IT-Schutz heute besonders relevant?

Angriffe nehmen jährlich zu …

Zahlen, bitte! Täglich 390.000 neue Schadprogramme

Momentan hat man das Gefühl, in jedem Mail-Anhang und hinter jedem Link versteckt sich irgendeine Malware. Antiviren-Hersteller und Test-Labore verstärken diesen Eindruck noch durch irrwitzig hohe Zahlen neuer Schadprogramme.

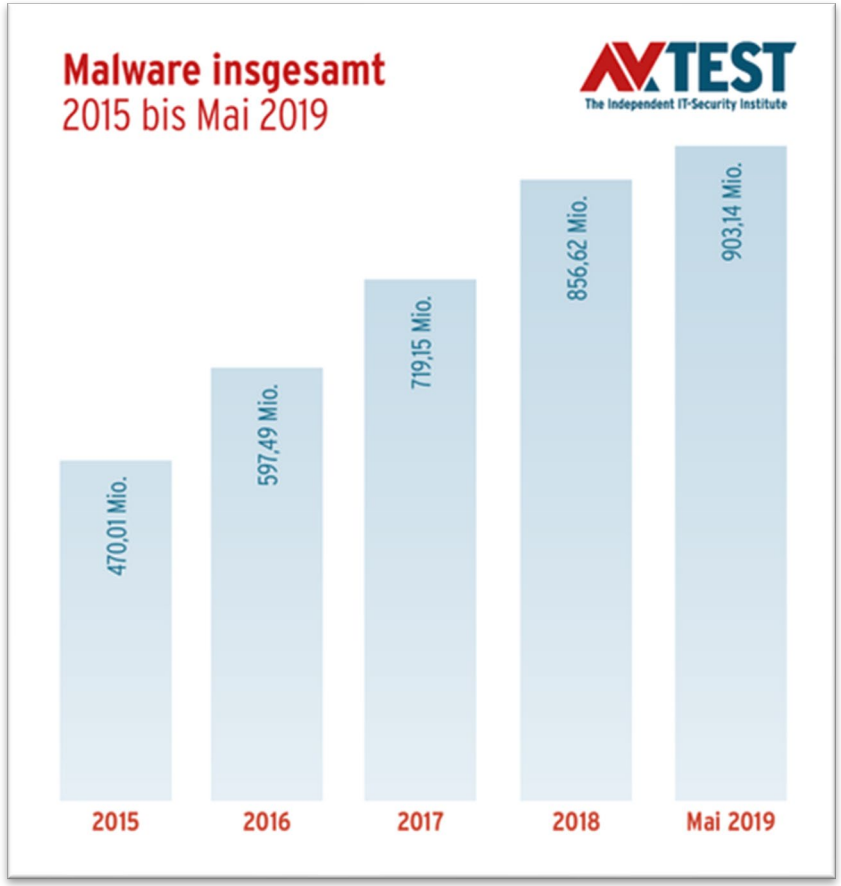
Quelle: Heise 2016

Malware-Top-10 2019: Angriffe im Sekundentakt

Neun neue Malware-Samples pro Minute bedrohen PCs und Netzwerke

Mehr als 4,9 Millionen Malware-Samples haben die Cyber-Defense-Spezialisten von G DATA 2019 identifiziert. Das Ziel der Cyberkriminellen: Passwörter und vertrauliche Daten auslesen oder Daten und Systeme verschlüsseln. Die zehn aktivsten Malware-Familien hat G DATA in der aktuellen Jahres-Top-Ten zusammengestellt.

Quelle: G Data 2020



Quelle: AV-Test Institut 2019

… und verursachen grossen Schaden

CSIS-Studie *22.02.2018, 14:44 Uhr*

600 Milliarden Dollar Schaden durch Cybercrime

Cyberkriminalität verursacht immer grössere Schäden. Nach neusten Studienergebnissen von McAfee sind dies weltweit jährlich 600 Milliarden Dollar.

Quelle: Computerworld 2018

Cybercrime

Die Raubzüge der Online-Betrüger

Homeoffice hat eine unerwünschte Nebenwirkung: Cyber-Angriffe nehmen zu. Die Justiz hat kaum eine Chance.

Quelle: SRF 2020

Verschlüsselungserpresser legen nun große Konzerne lahm

Die Uhrenmacher Swatch Group, eine französische Großreederei, der mithin größte private Spitalsbetreiber mit 400 Kliniken sowie ein großer Versicherungsbroker in den USA wurden binnen einer Woche erfolgreich angegriffen.

Quelle: Fm4.orf.at 2020

Trojaner Emotet wieder aktiv

Nach mehrmonatigem Unterbruch beobachtetet MELANI erneut verschiedene Malspam-Wellen mit infiziertem Word-Dokumenten im Anhang. Dabei handelt es sich um einen bereits länger bekannten Trojaner namens Emotet (auch bekannt als Heodo). Ursprünglich als E-Banking-

Quelle: NCSC 2020

Datensicherheit ist also ein heisses Thema!

Die Kehrseite der neuen Arbeitswelt

- Ständige Zunahme der Gateways

Erhöhte Risiken

- 700 Laptops gehen wöchentlich am Flughafen Charles de Gaulle verloren[1]
- 17‘000 UBS-Sticks jährlich in britischen Wäschereien gefunden[2]
- $ 3.62 Millionen durchschnittliche Kosten in Folge von Datenverlust[1]

[1] Ponemon-Institut | [2] Credant Technologies

Moderner IT-Schutz zur Bekämpfung von…

…externen Gefahren

„Einbruch verhindern“

…internen Gefahren

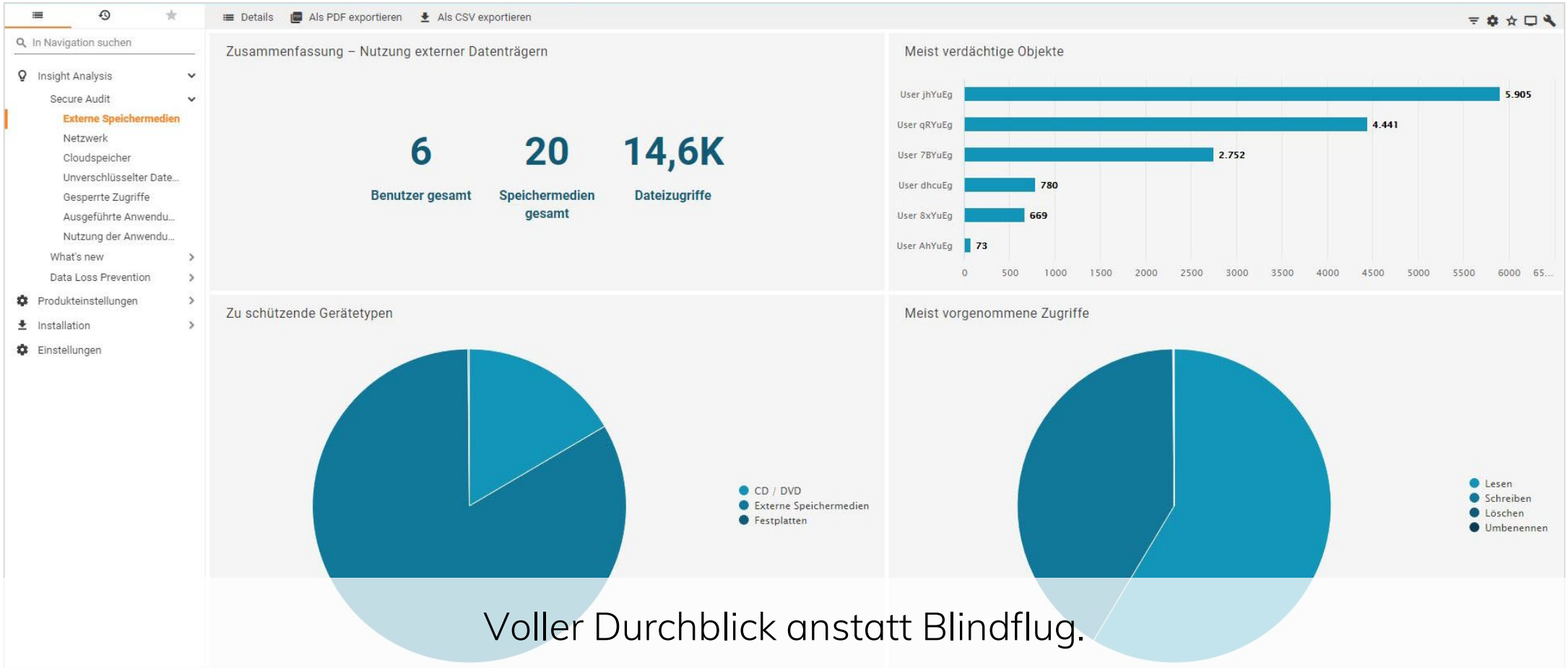
„Ausbruch verhindern“

Externe Gefahren

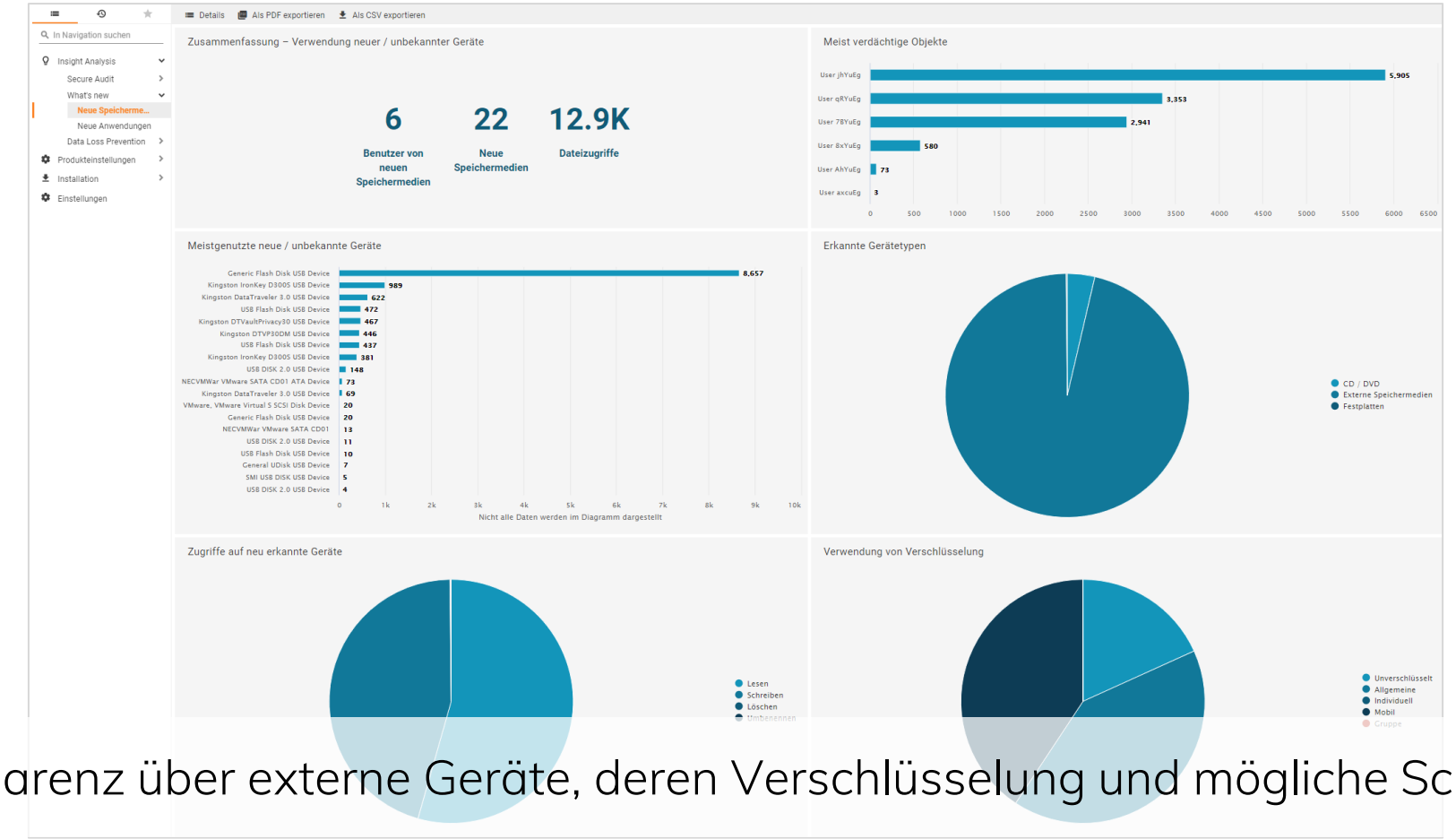
Die Herausforderungen

- Die Übersicht erlangen – das brauchen alle, haben aber die wenigsten
- Ihre Mitarbeiter erhalten Datenträger mit wichtigen Daten, Wartungstools und ähnlichem
  - Sie wollen lesende Zugriffe gestatten – aber ohne Risiko!
  - Datenträger automatisiert prüfen
- Zentrale Verwaltung der erlaubten Cloudspeicher im Unternehmen
  - Messen der verwendeten Speicher

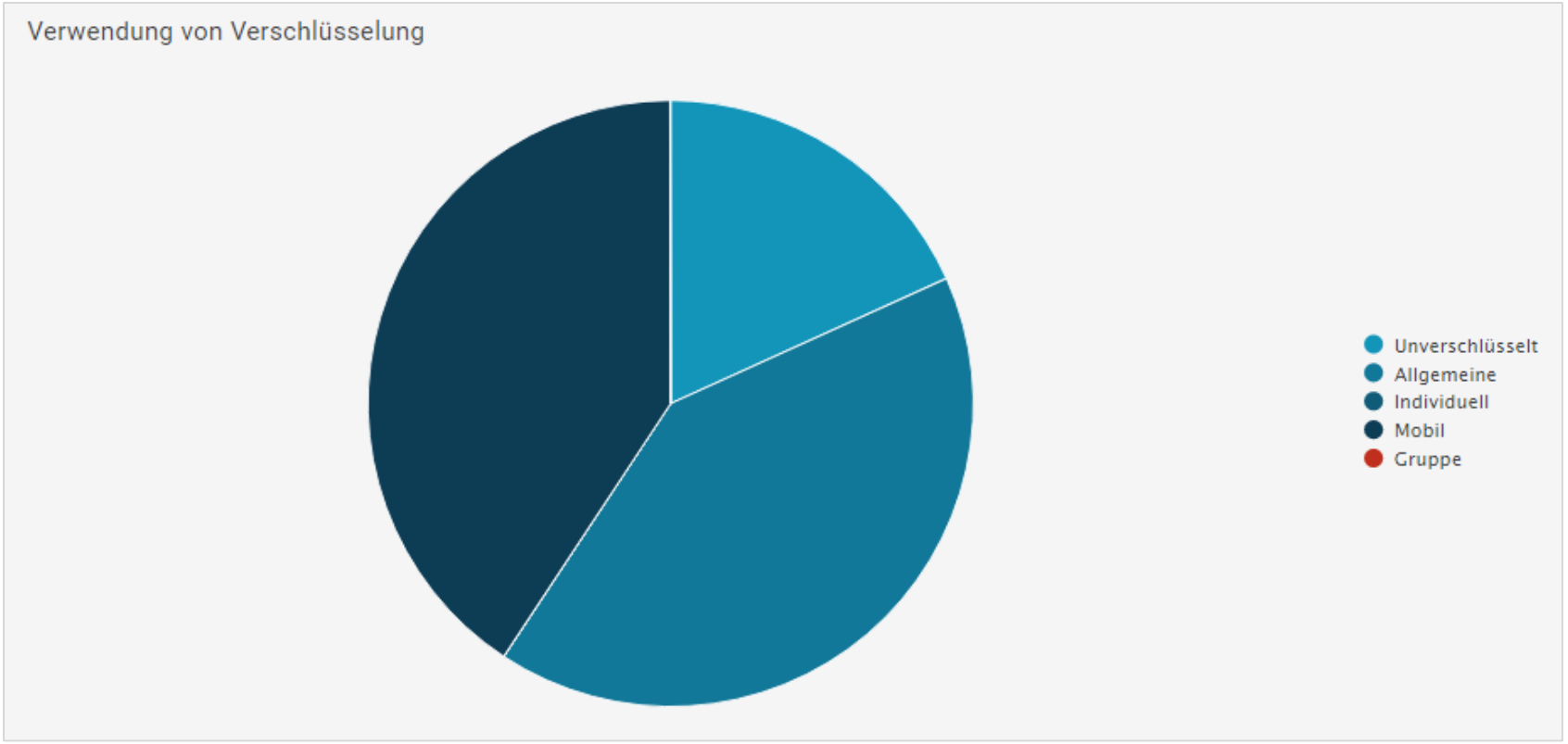
Was passiert gerade mit Ihren Daten?



Voller Durchblick anstatt Blindflug.



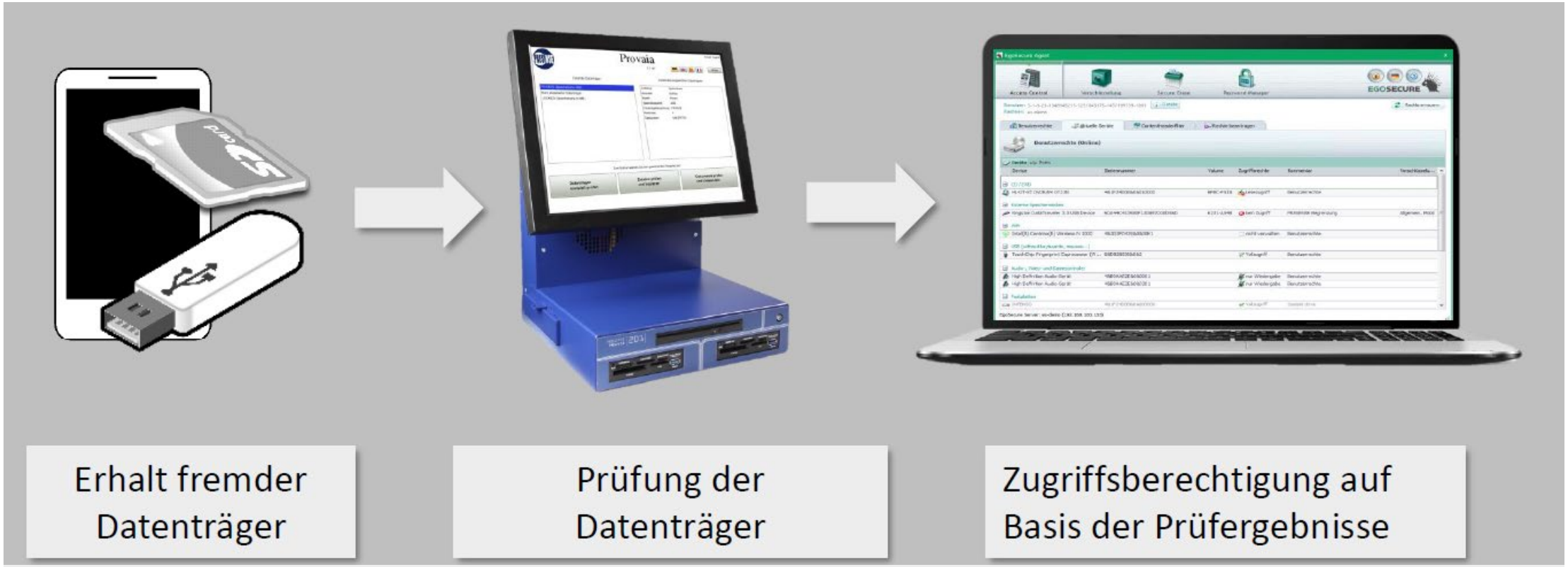
Volle Transparenz über externe Geräte, deren Verschlüsselung und mögliche Schwachstellen



Volle Transparenz über externe Geräte, deren Verschlüsselung und mögliche Schwachstellen

Audit-Vorgaben werden erfüllt

- (EU) - DSGVO
- ISO 27001/2
- TISAX
- BSI



Die Datenschleuse als intelligente Datenwaschanlage zum Schutz mobiler Datenträger

Egosecure

- Privilegierte Benutzerzugriffskontrolle
  ↳ EgoSecure CONTROL
- Verhinderung von Angriffen durch Datenverschlüsselung
  ↳ EgoSecure ENCRYPTION
- Auditdaten und Kontrolle
  ↳ EgoSecure AUDIT
- Überwachung der Datenverletzung ohne Verschlüsselung
  ↳ EgoSecure AUDIT

Interne Gefahren

Die Herausforderungen

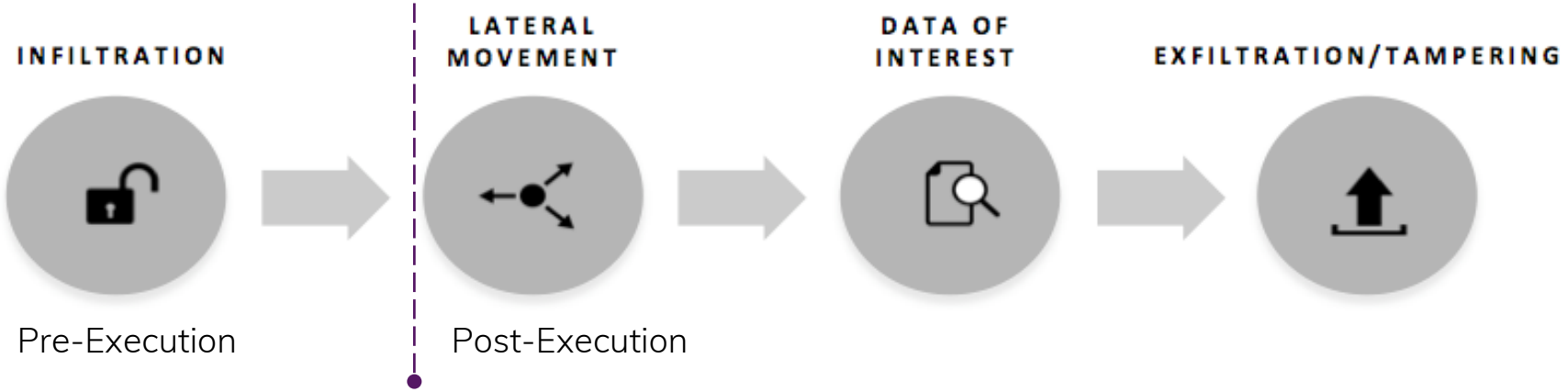
- Täglich gibt es mehrere 100‘000 neue Viren und Malware
  - Es ist unmöglich alle zu kennen
  - Herkömmliche Virenscanner nützen daher wenig
- Was passiert wenn der Virus bereits auf dem System ist?
  - Wann wird er erkannt?
  - Wird er überhaupt erkannt?
- Was passiert mit dem Virus und dem Endpoint, wenn der Virus erkannt wird?
  - Kann ich nachvollziehen, woher er kommt?
  - Kann ich nachvollziehen, welchen Weg er im Unternehmen nehmen will (Ausbreitung)?

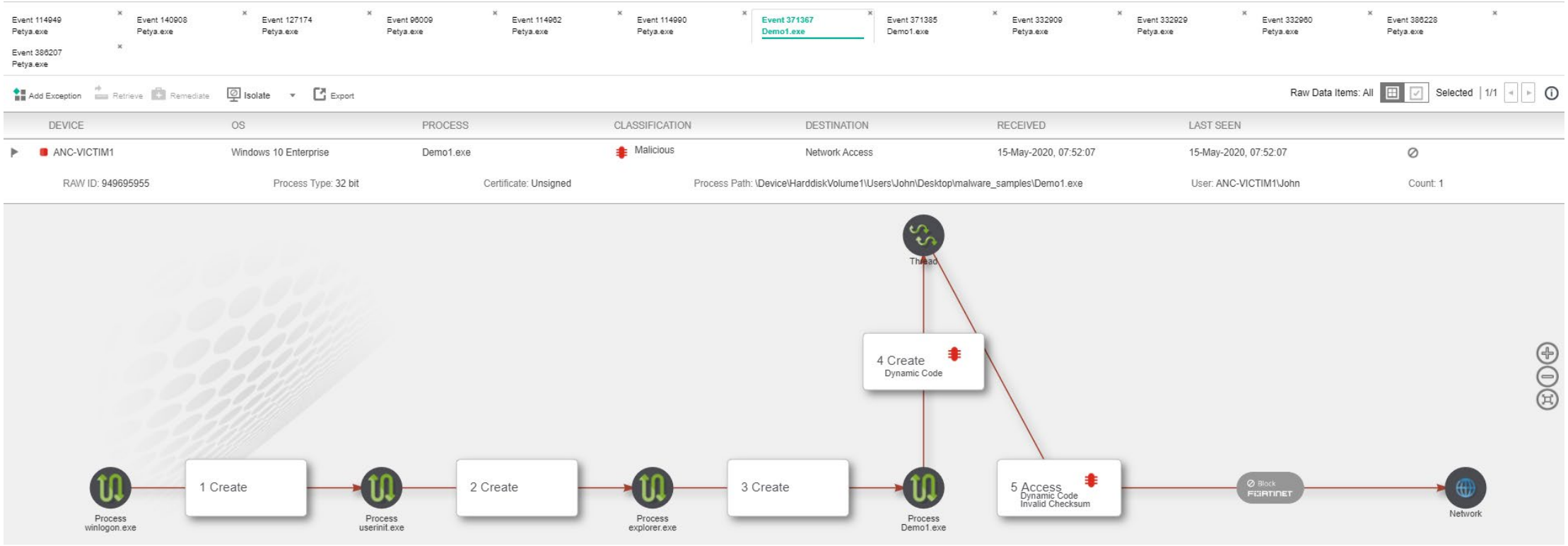
Bewertung einer Anti-Malware Standardlösung

Erkennung bekannter Malware	Ja, sehr hoch
Erkennung unbekannter Malware	Nicht zu 100% und nur mit Next-Gen Antivirus-Programmen
Blockieren von schädlichen Auswirkungen	Ziel ist die Vernichtung des Virus, nicht der Schutz vor bösartigem Verhalten
Entschärfung	Dauert zwischen 4 Stunden und 2 Wochen bis ein Weg gefunden wird, den Virus zu entfernen
Forensik	Hochentwickelte Tools, aber kein Bestandteil einer Standardsoftware
Automation, Service und Prozess Integration	Nein, muss vom Kunden gemacht werden

Was macht den Unterschied?

Anti-Malware Standardlösung	Ständige Updates erforderlich = Starke Performance-Einbussen = Kein Schutz vor Zero Day Attacks	Enpoint Detection and Response = Nur Entdeckung, kein umfassender Schutz
FortiEDR Next-Gen Antivirus	Ohne Updates und Signaturen = Zero Day Defense	Post Execution Prevention = Echtzeit Blockierung von Zero Day, In-Memory, Fileless Malware





Dank der forensischen Analyse können Angriffe zurück verfolgt werden

Bewertung von FortiEDR

Erkennung bekannter Malware	Sehr hoch
Erkennung unbekannter Malware	Post infection protection
Blockieren von schädlichen Auswirkungen	Post infection protection
Entschärfung	Automatisch (Unified Endpoint Management und IntelAct)
Forensik	Grafische Prozesskette in Echtzeit (Endpoint Detection and Response)
Automation, Service und Prozess Integration	Nach definiertem Prozess automatisch (ITSM)

Moderner IT-Schutz zur Bekämpfung von…

…externen Gefahren

„Einbruch verhindern“

…internen Gefahren

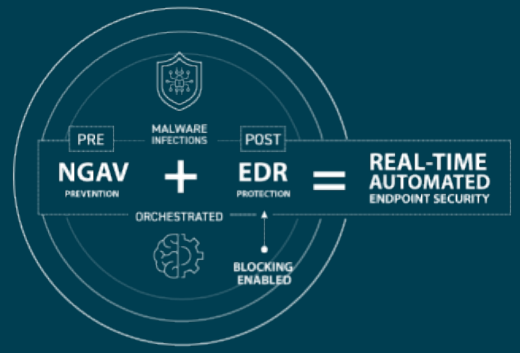
„Ausbruch verhindern“

...beispielsweise durch diese Technologien

EGOSECURE

Alles läuft wie bisher, nur sicher.

FortiEDR



Gezielte Isolation von bekannten und unbekannten Bedrohungsakteuren in Echtzeit.

Fragerunde

Schreiben Sie Ihre Frage in den Chat von GoToMeeting.

Vielen Dank für Ihr Interesse!

Kontaktpersonen:

Thomas Egli
Armacom AG
+41 61 599 79 44
thomas.egli@armacom.ch

Tony Förstner
Matrix42 AG