Komfortable Sicherheit statt Scheunentor

Abwehr – Die beste Verteidigung

HP WOLF SECURITY

Die Bedrohungen

HP WOLF SECURITY

Umfrage – Wo sehen Sie die größte Bedrohung?

Auswahlmöglichkeiten – Multiple – Choice:

- Hacker
- Fehlende klare Vorgaben
- Ransomware
- Fehlerhafte Konfiguration
- User
- Phishing
- Malware Übertragung per Konferenzlösung
- Zufälliger Befall mit Schadsoftware

BSI – Lage der IT-Sicherheit 2023

Ransomware ist weiterhin die größte Bedrohung:

- 66% aller Spam Mails waren Cyberangriffe
- 250.000 neue Schadprogramm Varianten pro Tag gefunden

Top 3 Bedrohungen je Zielgruppe

- Identitätsdiebstahl, Sextortion, Phishing
- Ransomware, IT-Supply Chain Risiken, Konfiguration von Online Servern
- Ransomoware, APTs, Konfiguration von Online Servern

Quelle: BSI Lage der IT-Sicherheit 2023

Risikofaktor Mensch

“Menschen stellen immer
die besten Sicherheitslücken dar.”

Elliot Alderson, Mr. Robot, Staffel 1, Episode 5

Ein falscher Klick

70%
der Sicherheitsverletzungen sind auf Social Engineering und menschliches Versagen zurückzuführen

92%
der Malware wird über email eingeschleust

67%
der Malware ist embedded in Word Dokumenten

100%
solcher Angriffe hängen davon ab, ob die Mitarbeiter den Köder schlucken

Die dunkle Seite – Live - Bericht

https://www.sicherheitstacho.eu/start/main

Der Endpunkt - Ganzheitlich

HP WOLF SECURITY

Security ist in unserer DNA

Mehr als 20 Jahre Innovationen in Security

- Setzen von Industriestandards für Endgerätesicherheit
- TPM, BIOS, Firmware Resilienz
- Wegweisende hardwaregestützte Sicherheit
- Enge Entwicklungspartnerschaften im Beriche Sicherheit Sicherheitspartnerschaften (Intel®, AMD® und Microsoft®)
- Verbesserte Endpunktsicherheit mit HP Wolf Security



Der Endpunkt – In Sicherheit

Modernes Endpunkt-Management

Cloud-basiertes Endpunkt-Management

Incident und Disaster Recovery

Wiederherstellung der Mitarbeiterproduktivität im Falle eines Ausfalls der Endpunktbeschädigung oder Katastrophenszenario

Lifecycle Management

Effizienter PC Support von Anschaffung bis Außerdienststellung

Nutzer Produktivität

Minimieren Sie Ausfallzeiten oder Serviceunterbrechungen für Upgrades, um die Produktivität zu maximieren

PC Plattform Integrität

Malware Kompromittierung unterhalb des Betriebsssystems

Physikalische Kompromittierung

Verlust von Daten oder Systemintegrität

Supply Chain Risiken

Die Kompromittierung des Geräts vor der Auslieferung des Geräts macht die Sicherheit auf Betriebssystemebene unwirksam

Compliance- und Audit-Kontrollen

Inadequate controls on in-scape infrastructure leads to findings

Hardwarebasierte Sicherheit

HP Wolf Pro & Enterprise
Threat protection

HP Sure Run
Defense protection

IR Camera
Fingerprint Sensor, Smart Card

TPM 2.0
Security chip

HP End Point
Security Controller

HP Sure Start
Pre-OS BIOS Protection

HP Sure Sense
Zero-day attack protection

HP Privacy Camera
for user privacy

HP Sure View Reflect
for screen privacy

HP Tamper Lock
Chassis intrusion detection

HP Sure Recovery
for device recovery

HP Wolf Pro & Enterprise
Threat protection

HP Sure Start
BIOS Prüfung und Schutz

HP Security Manager
Security-Flottenmanagment

HP Whitelisting
Firmware Schutz

TPM
Security chip

HP Connection Inspector
Schutz bei verdächtiger Kommunikation

HP Run-time Intrusion Detection
Schutz im laufenden Betrieb

Ganzheitliche Endpunkt Sicherheit von HP

- Sichere Plattform für Verfügbarkeit, Risikomanagement und Reporting
- HP engagiert sich seit langem für die Entwicklung sicherer Plattformstandards
- Über 20 Jahre Endpunktsicherheit, Innovationen und setzen von Standards

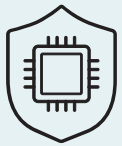

Sure Admin


Sure Recover


Sure Start


Seamleass Firmware Update


Tamper Lock


Endpoint Security Controller


eMMC Module


Factory Services

Plattformsicherheit für betriebliche Effizienz, Risikomanagement und hohe Verfügbarkeit

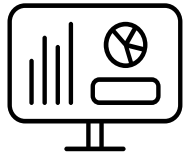
Sure Click Enterprise

Threat Containment – Mikro Virtualisierung

HP WOLF SECURITY

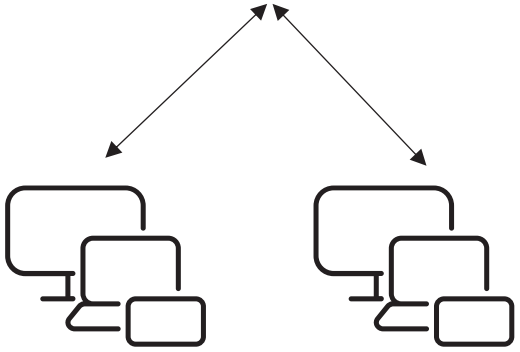
Architektur – Cloud oder 100 % on Premise

Richtlinien



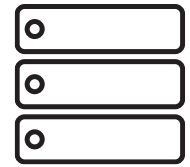
Reporting und Analyse

Cloud Controller – Frankfurt am Main

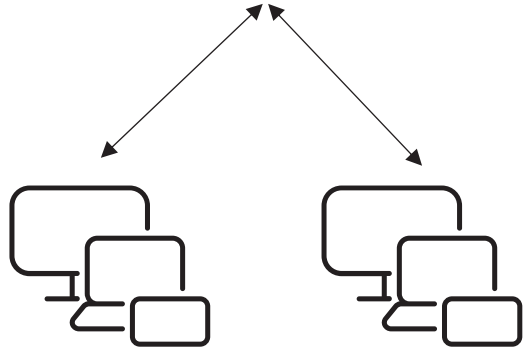


End User PC

End User PC



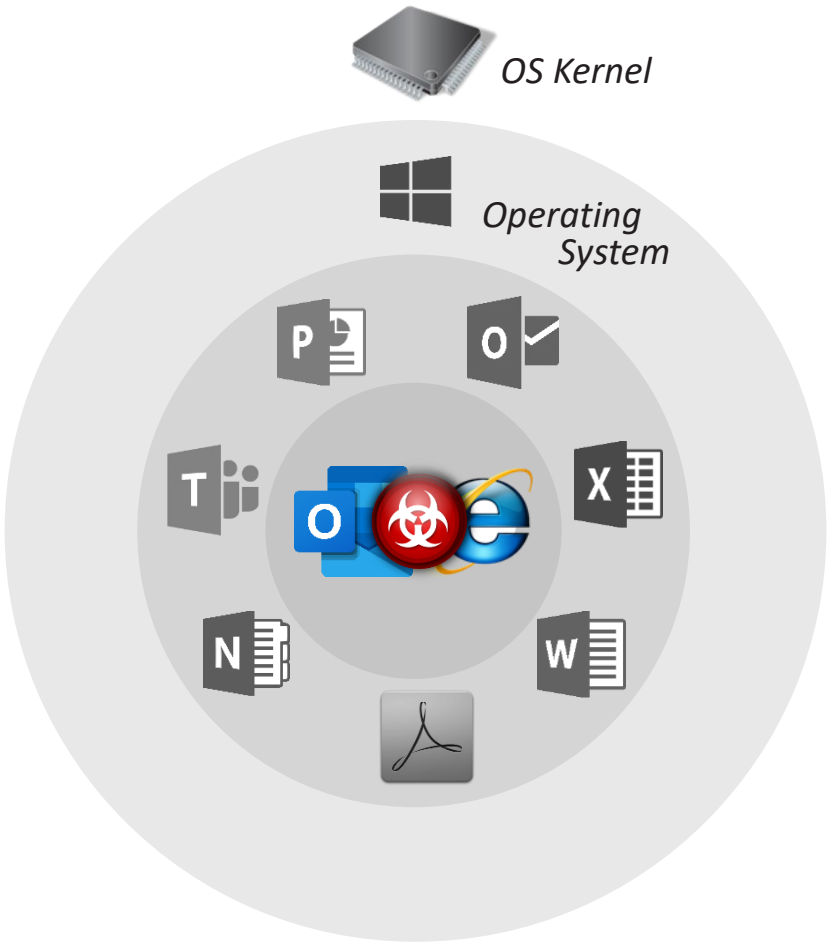
On Premise Controller



End User PC

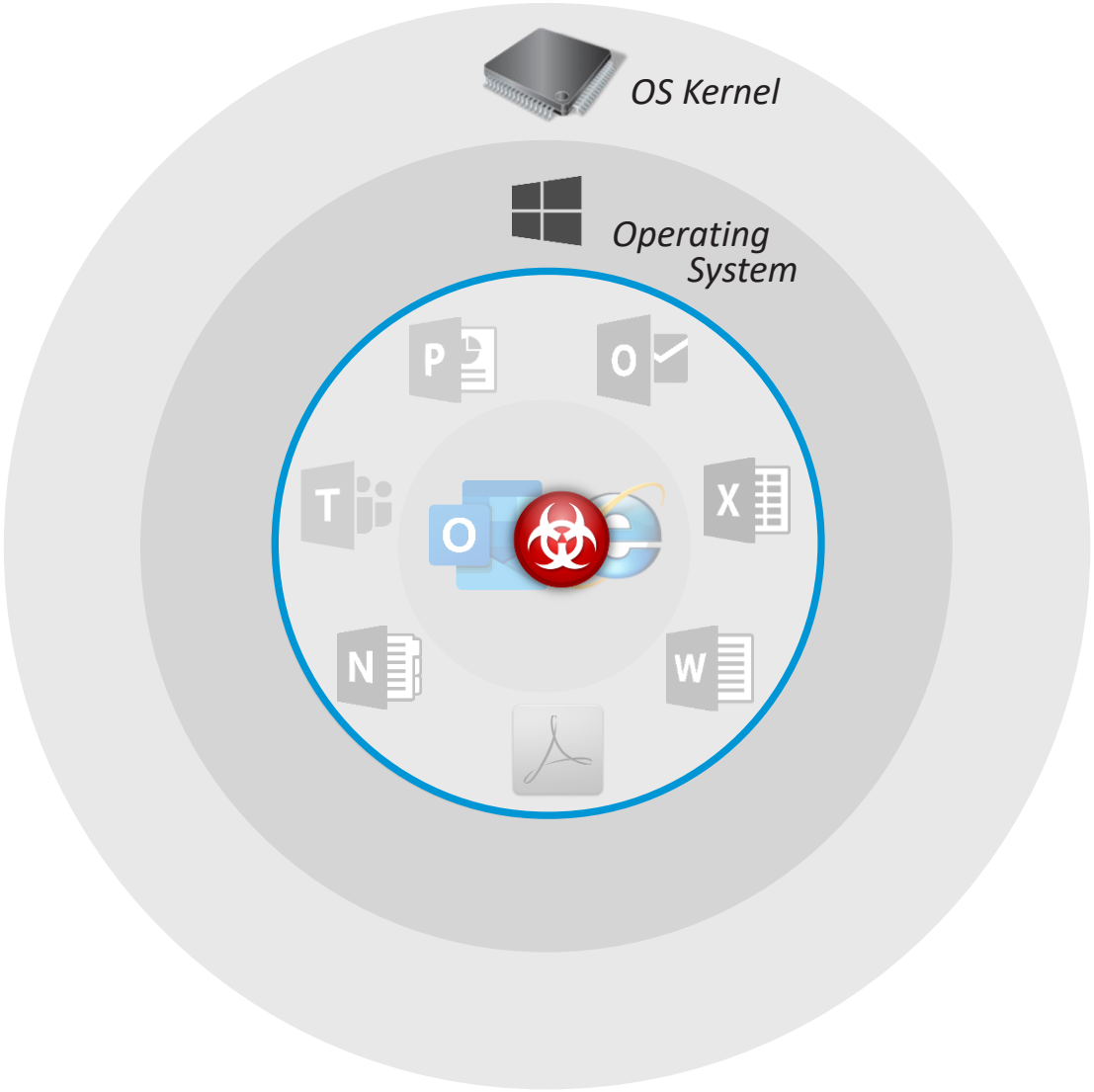
End User PC

Üblicherweise...



Ein Klick genügt um einen maximalen Schaden für Ihr Unternehmen zu verursachen

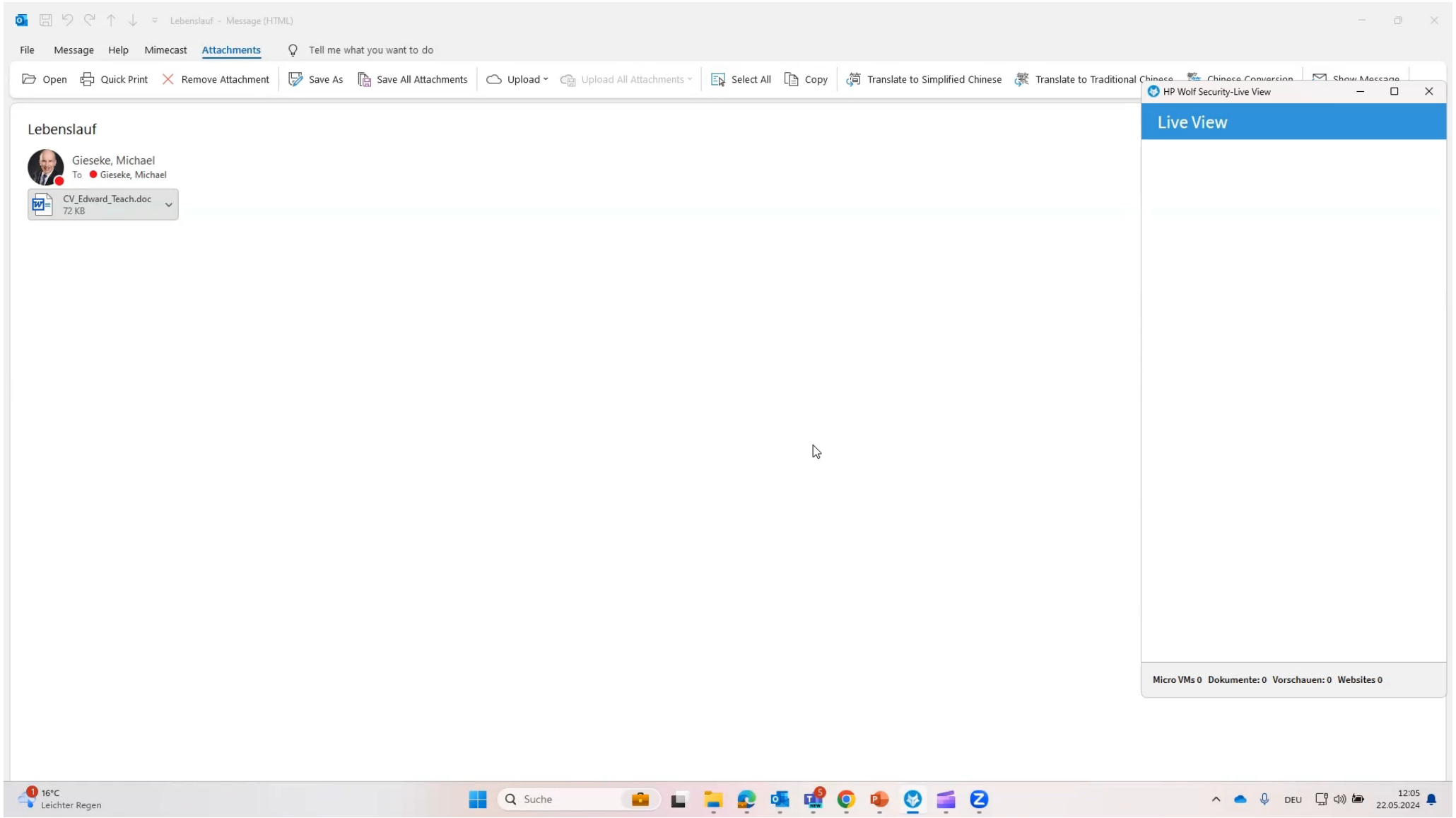
ISOLATION – HP SureClick Enterprise



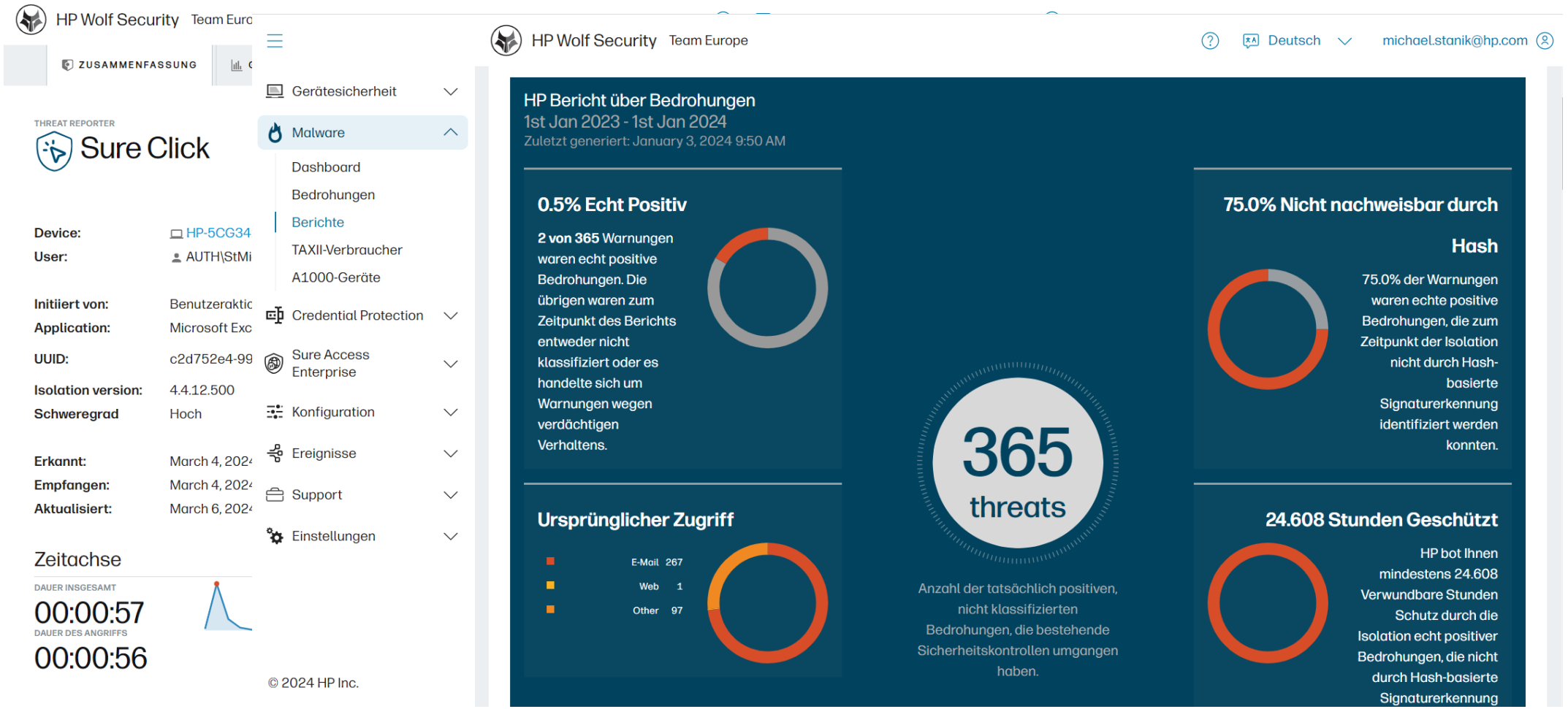
ISOLATION auf dem Endpunkt:

- Arbeitet in einer virtuellen Maschine, isoliert vom gesamten System
- Keine Performance Einbußen
- Bedrohungen verschwinden sobald der Browser/die Email/die Datei geschlossen wird
- Sicheres Öffnen von Anhängen und Browsing
- Schutz in Conferencing Lösungen

ISOLATION – HP SureClick Enterprise



Management und Reporting - Dashboard



BSI-Empfehlung

1. Isolation gehört zu den Mindestanforderungen für Web-Browser welche vom BSI (Bundesamt für Sicherheit in der Informationstechnik) definiert wurden
2. Micro VMs sind lt. BSI essenziell um sich vor Ransomware zu schützen Seite 14: “Ausführung potenziell gefährlicher Inhalte in gekapselten Umgebungen”

4 Ausführbarkeit von Schadprogrammen einschränken (Client Einstellungen)

4.6 Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen

Eine weitere Schutzschicht kann die Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen, insbesondere (Mirco-) VMs, sein. Dabei wird eine temporäre Arbeitsumgebung gestartet, welche regelmäßig wieder gelöscht oder zurückgesetzt wird. Wenn Dokumente und Dateien aus unsicheren Quellen in einer virtuellen Umgebung (VM) geöffnet werden, müsste entsprechende Schadsoftware aus dieser VM ausbrechen, um das eigentliche System zu infizieren. Entsprechende (Micro-) VMs können beispielsweise auch das Öffnen Links aus E-Mails abdecken. Selbstverständlich müssen auch entsprechende Lösungen, welche (Micro-) Virtualisierung anbieten aktuell gehalten werden. Zum einen können Betriebssystem-Updates zu Problemen führen, zum anderen kann nur so verhindert werden, dass Schadprogramme aus der VM ausbrechen können.

Quelle: BSI Maßnahmenkatalog Ransomware - Arbeitspapier

EDR vs HP SureClick Enterprise

Identifikation und Reaktion auf eine vorhanden Anomalie

Prävention und Isolation von und gegen verdächtige Eindringlinge

HP SureClick Enterprise und EDR in Kombination

Prävention und Isolation von und gegen verdächtige Eindringlinge

Identifikation und Reaktion auf eine vorhanden Anomalie

Wie nutzen Kunden HP SureClick Enterprise?

- eMails mit Anhängen, Downloads aus dem Internet und aus Konferenzlösungen (z.B. MS Teams)
  - **Bewerbungen, Agenturen, Bürgerkommunikation, Dienstleister, Labore, Krankenkassen, Pflegedienste, Befunde, jegliche Art von externer Kommunikation**
  - **Downloads aller Art werden geschützt**
- Phishing Schutz:
  - **Externe Links werden isoliert geöffnet, definierte Seiten können freigegeben werden**
  - **Bekannte Phishing Sites werden geblockt**
  - **Downloads von Ransomware isoliert**
- Daten von USB-Sticks werden isoliert geöffnet
  - **Bürger bringen Unterlagen mit**
  - **Rechner sind im privaten Umfeld genutzt**
  - **Sicherstellung von Beweisen (Polizei) von Handy oder USB Stick**
  - **Schulen**
- Umfangreiche Auswertung bei Angriffen
- Unterstützt Compliance
- Produktivität und Sicherheit gleichzeitig

Zusammenfassung

Den Endpunkt gesamtheitlich betrachten:

- **Sichere Hardware-Plattform**
- **Software**
- **HP Services**

HP SureClick Enterprise – Prävention durch Isolation – BSI empfohlene Technologie

- Die Anforderungen an Sie steigen, auch in Komplexität und Menge
- Ransomware ist die größte Bedrohung
- Prävention statt Reaktion dank HP SureClick Enterprise
- HP SureClicK Enterprise entlastet und schützt Sie

- Kontakt:
  - **Michael.Gieseke@hp.com**

Kommen Sie auf uns zu und lassen Sie uns die Welt etwas sicherer machen!

HP WOLF SECURITY