Besserer Schutz vor Cyberkriminalität

Jonas Spieckermann
Senior Sales Engineer
Central Europe

Agenda

- Keinfaktor, Zweifaktor, Multi-Faktor-Authentifizierung
  - Schutz vor schwachen Passwörtern mit AuthPoint
- Falsch geklickt
  - Schutz vor Email-Phishing mit DNSWatch
- Daten weg
  - Allgemeiner Schutz vor dem Verlust sensibler Daten mit Total Security Suite

Keinfaktor, Zweifaktor, Multi-Faktor Authentifizierung

Massen-Doxxing: Beschuldigter soll Passwörter teilweise im Darknet gekauft haben

Ist der beschuldigte 20-Jährige gar kein großer Hacker? Nach neuen Erkenntnissen soll er einige Passwörter im Darknet gekauft und nicht selbst erhackt haben.

Von **Oliver Bünte**

174

https://www.heise.de/newsticker/meldung/Parteihack-Persoenliche-Dokumente-Hunderter-deutscher-Politiker-veroeffentlicht-4265180.html
https://www.heise.de/newsticker/meldung/Massen-Doxxing-Beschuldigter-soll-Passwoerter-teilweise-im-Darknet-gekauft-haben-4270379.html

17.01.2019 09:59 Uhr | Security

Passwort-Sammlung mit 773 Millionen Online-Konten im Netz aufgetaucht

Eine riesige Sammlung mit Zugangsdaten zu Online-Diensten zirkuliert in Untergrund-Foren. Die Passwörter von Millionen Nutzern sind betroffen.

Von **Fabian A. Scherschel**

829

(Bild: plantic\Shutterstock.com)

https://www.heise.de/security/meldung/Passwort-Sammlung-mit-773-Millionen-Online-Konten-im-Netz-aufgetaucht-4279375.html

Passwörter geraten schnell in falsche Hände!

Der Zettel!

BUSINESS INSIDER

TECH FINANCE POLITICS STRATEGY LIFE

A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note

Kif Leswing

3h 18,986

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

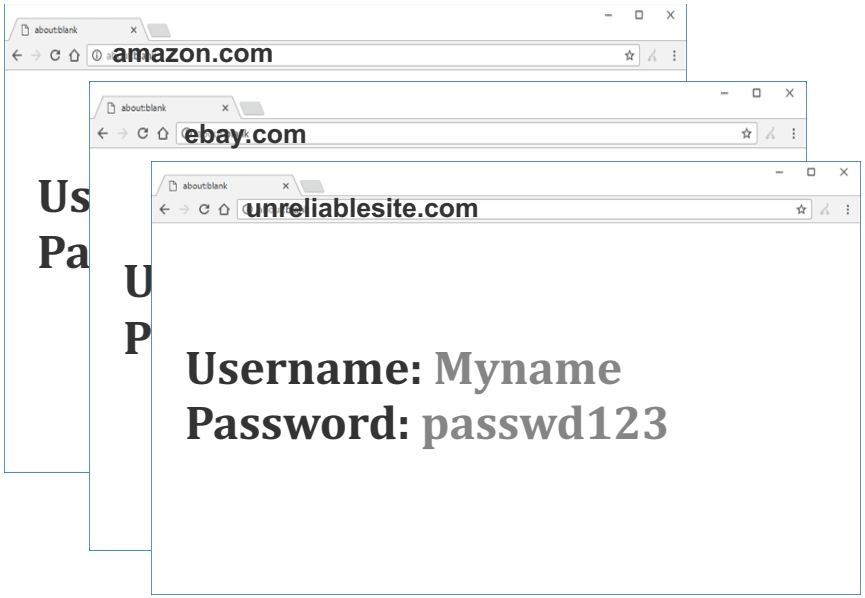
- **A false alert warning of an inbound missile was broadcast in Hawaii on Saturday.**
- **Since then, people have discovered that a photo taken in Hawaii's Emergency Management Agency for a news article in July includes a sticky note with a password.**

Zu einfach!

Eingabe im öffentlichen Wi-Fi oder Internet-Cafe!

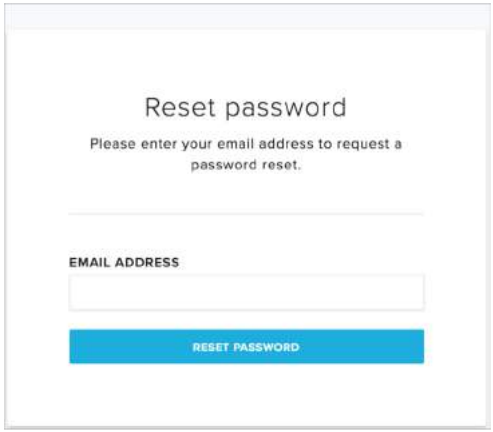
Passwörter geraten schnell in falsche Hände

Nur 1 Passwort!



Malware Infektion!

Passwort vergessen!



Phishing!

Der Verlust eines Kennworts ist schnell passiert!

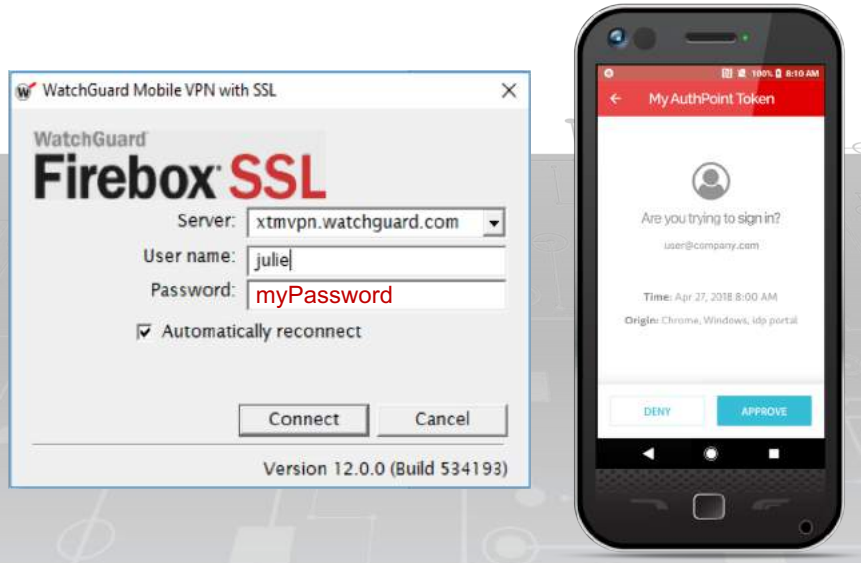
Selbst mit bestens aufgestellter Perimeter- und Endgerätesicherheit ist es schnell passiert:

1 Benutzerkennwort wird gehackt • 1 Computer ist mit einem Keylogger infiziert • 1 Nutzer teilt seinen Pin mit

… und der Angreifer hat vollen Zugriff, fast als würde er vor Ort im Unternehmen sein

Dadurch ist Multifaktor Authentifizierung so wichtig!

- Es schützt die Anmeldedaten
- Es stellt sicher, dass der echte Anwender das Kennwort verwendet
- Es schützt den Anwender, wenn dass Kennwort gestohlen ist.

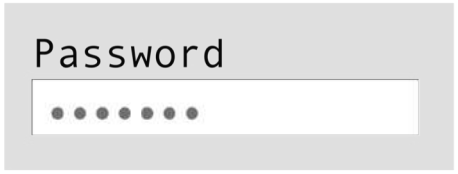


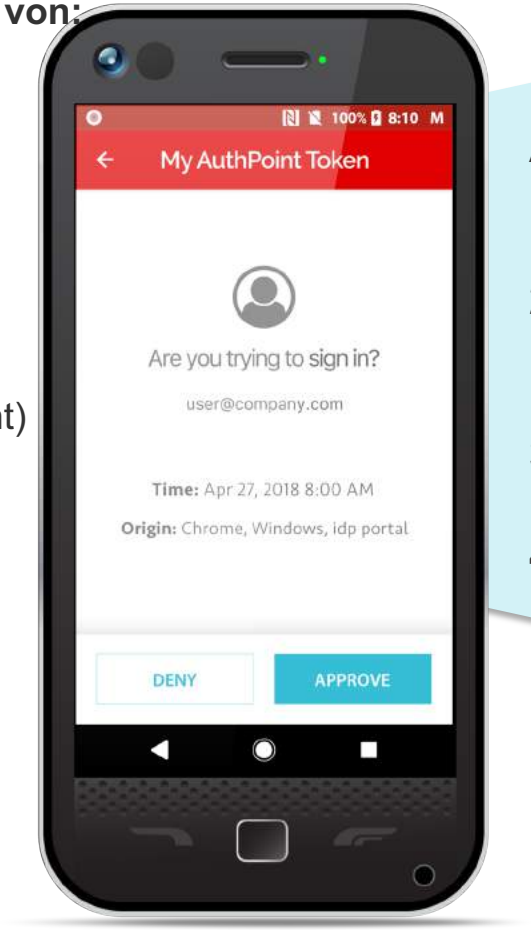
Username & password credentials can be confirmed by push-based authentication

Was ist Multi-Faktor-Authentifizierung?

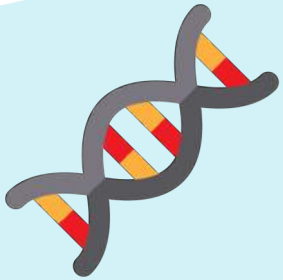
Verwendung von 2 oder mehr Authentifizierungsfaktoren von:

- **Etwas, das du kennst** (Passwort, PIN)
- **Etwas, das du hast** (Token, Handy)
- **Etwas, was du bist** (Fingerabdruck, Gesicht)



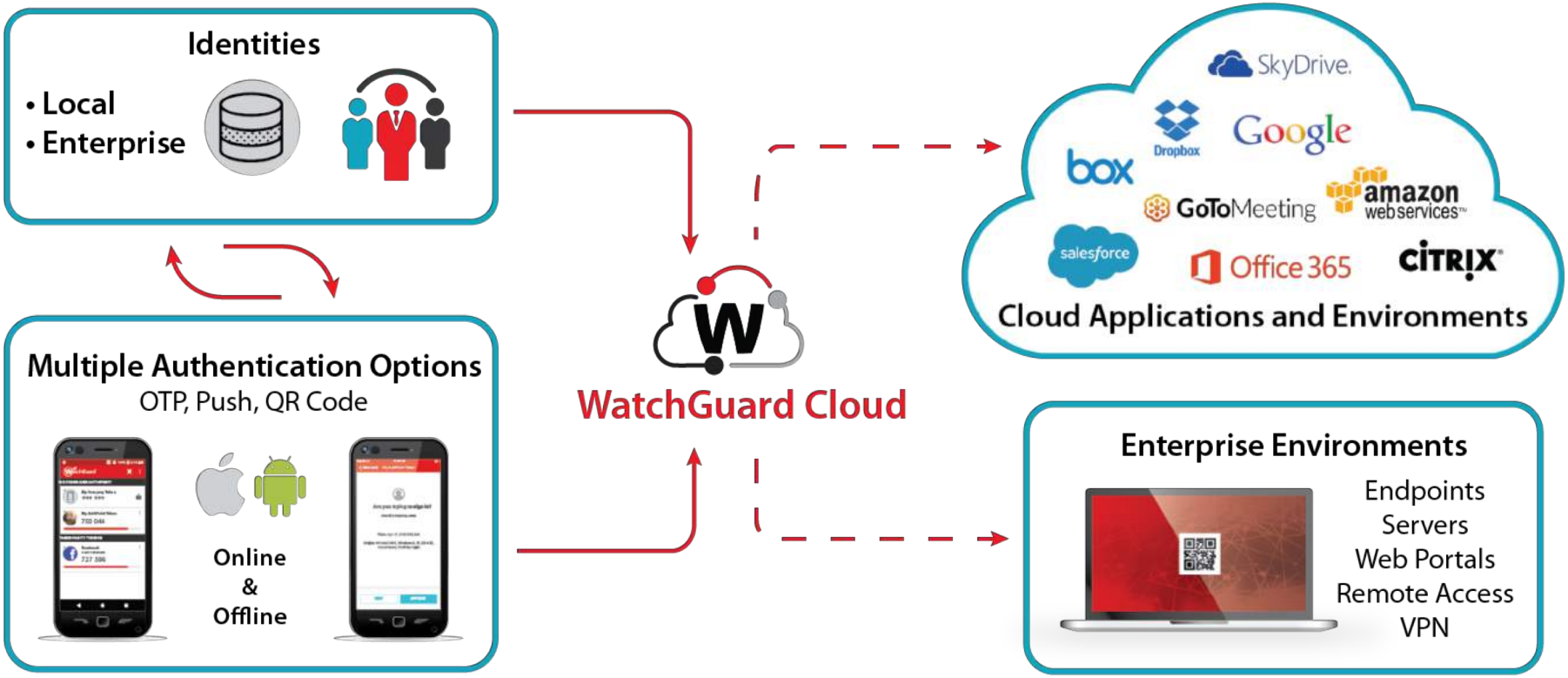


AuthPoint-Faktoren:

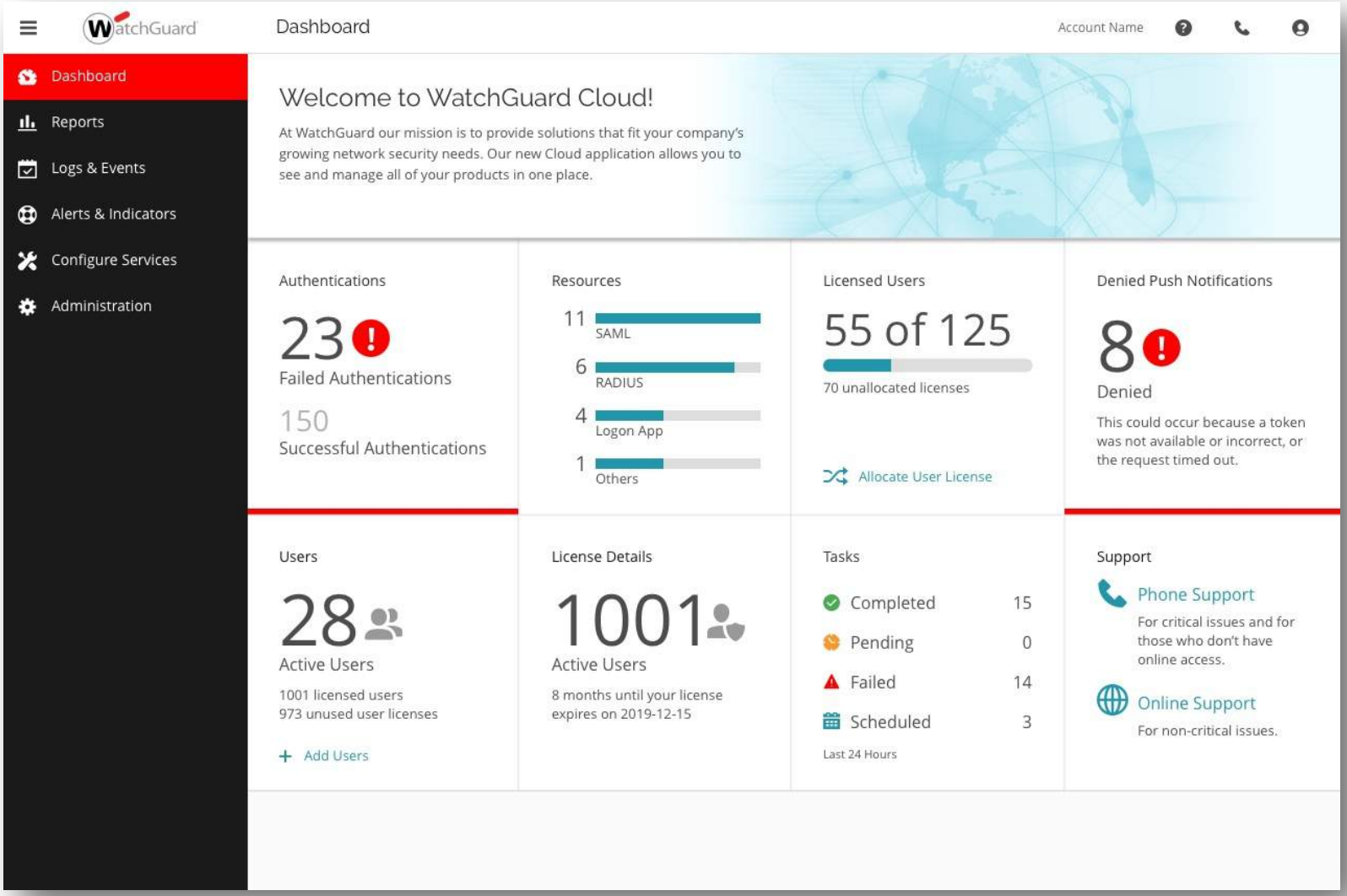


1. **Ihr Passwort**
2. **Genehmigung für Ihren mobilen Authentifikator**
3. **Korrekte Handy-DNA**
4. **Ein Fingerabdruck für den Zugriff** (mit bestimmten Telefonmodellen)

Schützt VPNs, Web Apps, PC-Anmeldung und mehr!

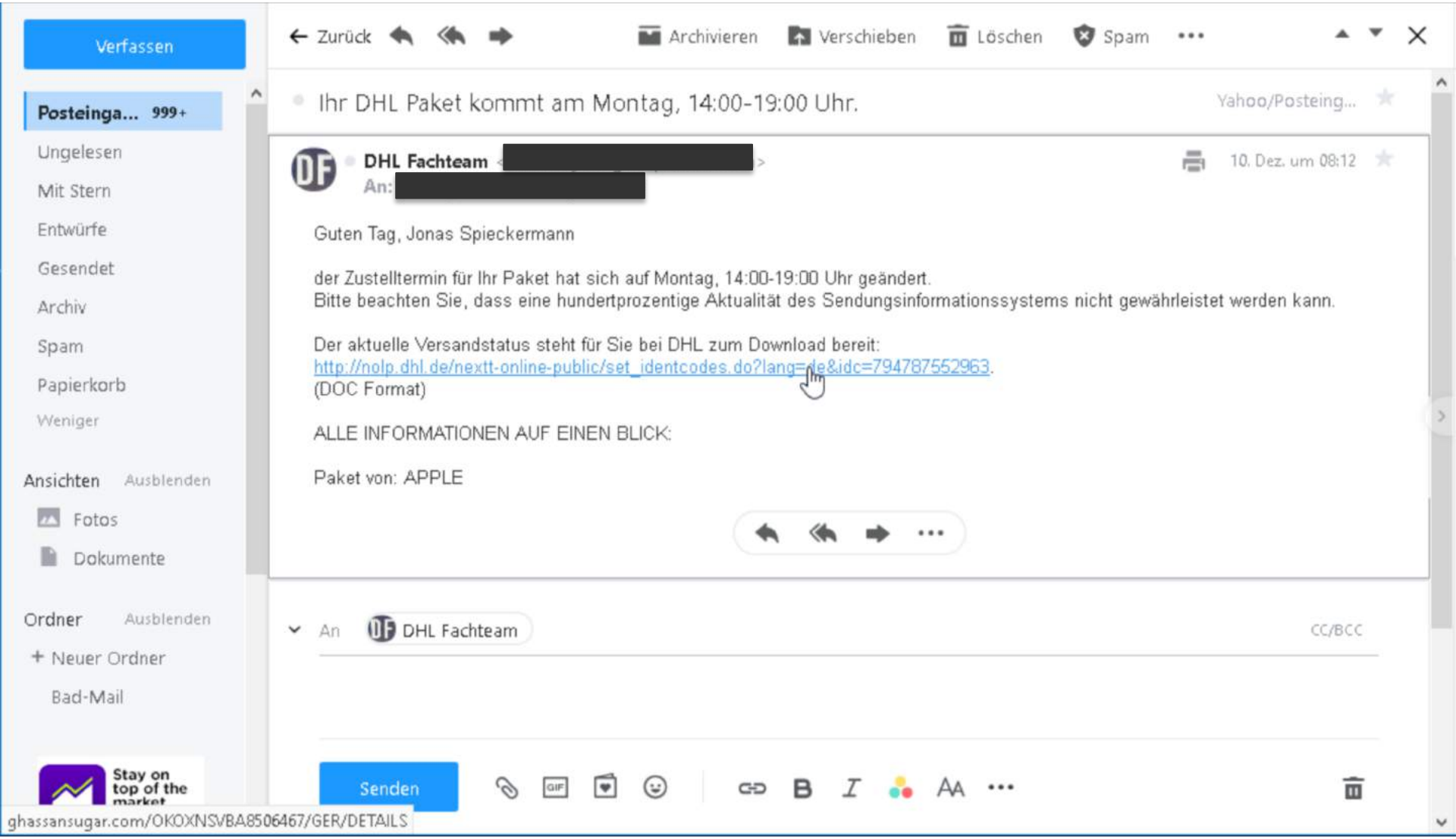


WatchGuard Cloud – Verwalten von überall



Falsch geklickt
Wirkungsvoller Schutz vor Phishing

Jeden Tag gibt es Opfer von Phishing Angriffen!

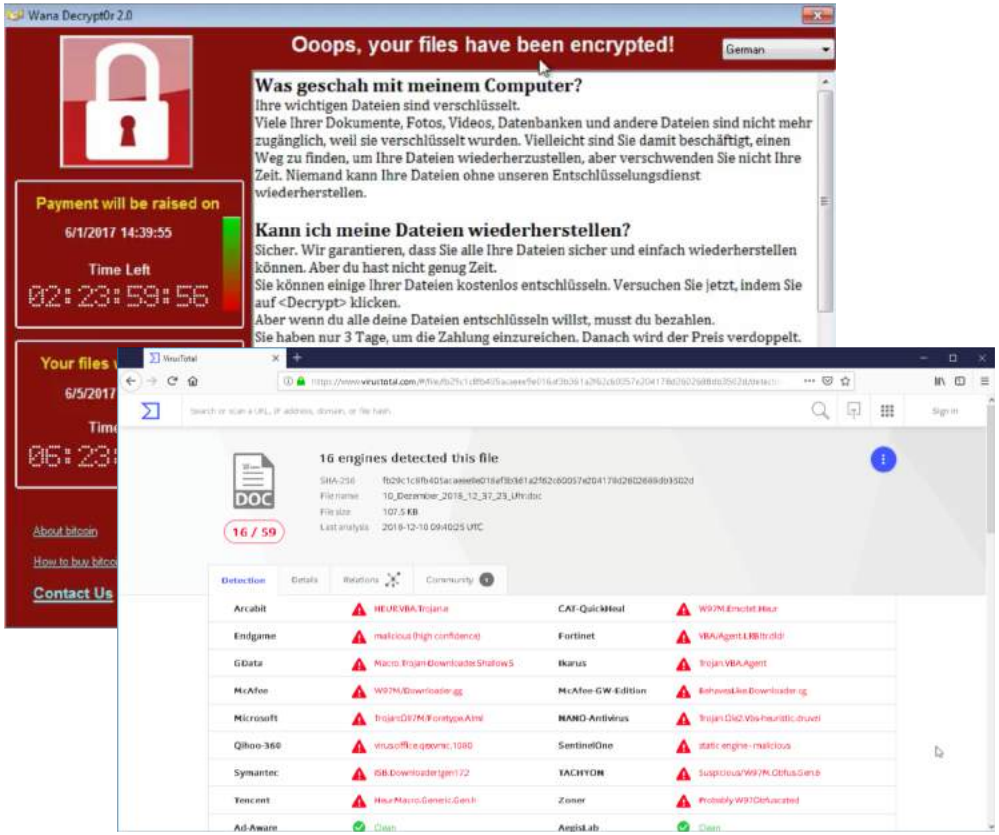


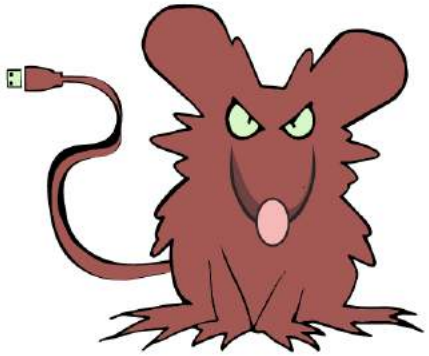
Unterschiedliche Zielpersonen

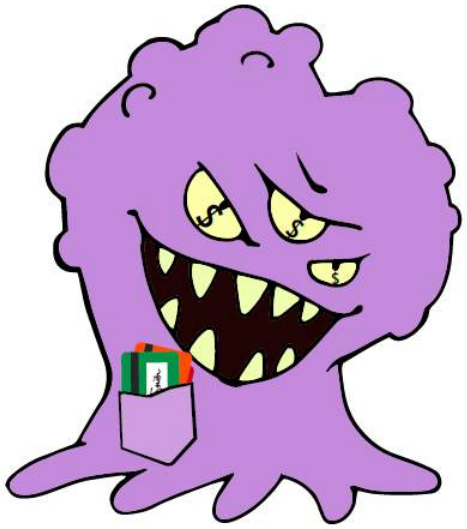
Phishing Angriffe beziehen sich gezielt auf „Menschen“

Die Folgen sind vielfältig

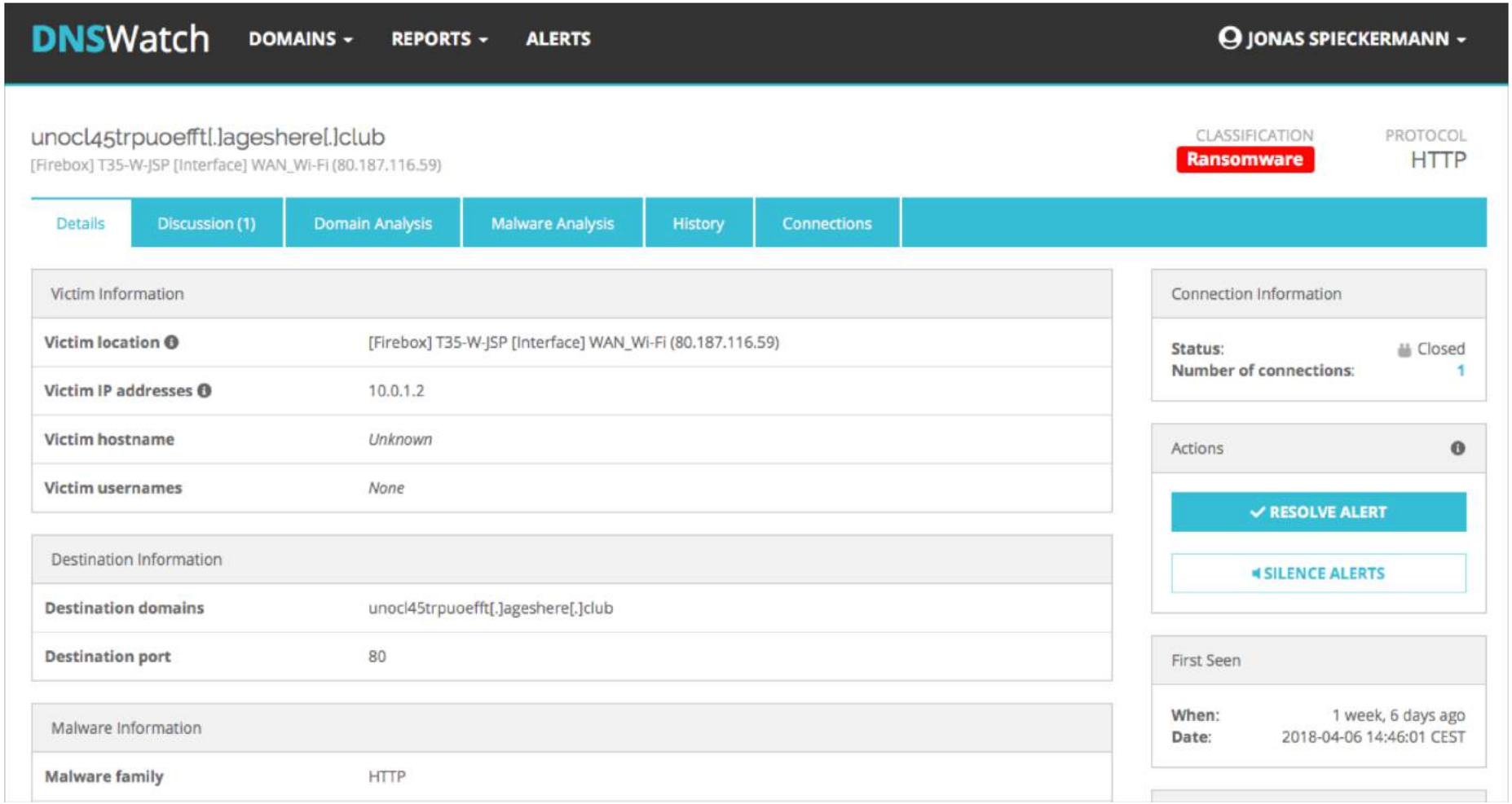
.....nicht nur Ransomware







Früher Konter gegen Phishing Attacken



Schutz mit Awareness Training

WatchGuard DNSWatch

WEBSITE BLOCKIERT

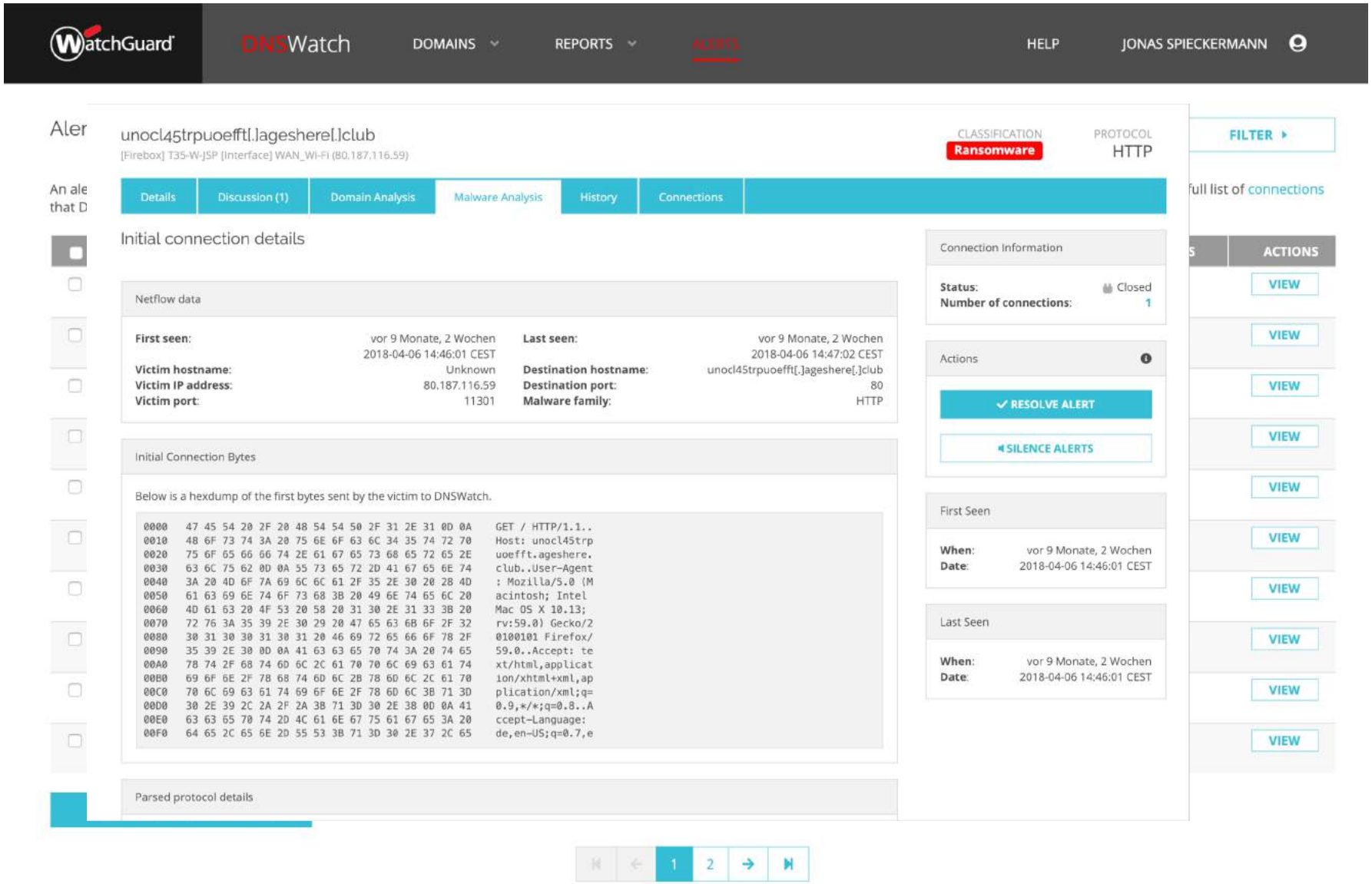
Oh je! Wir glauben, Sie haben auf einen Phishing-Versuch geklickt!

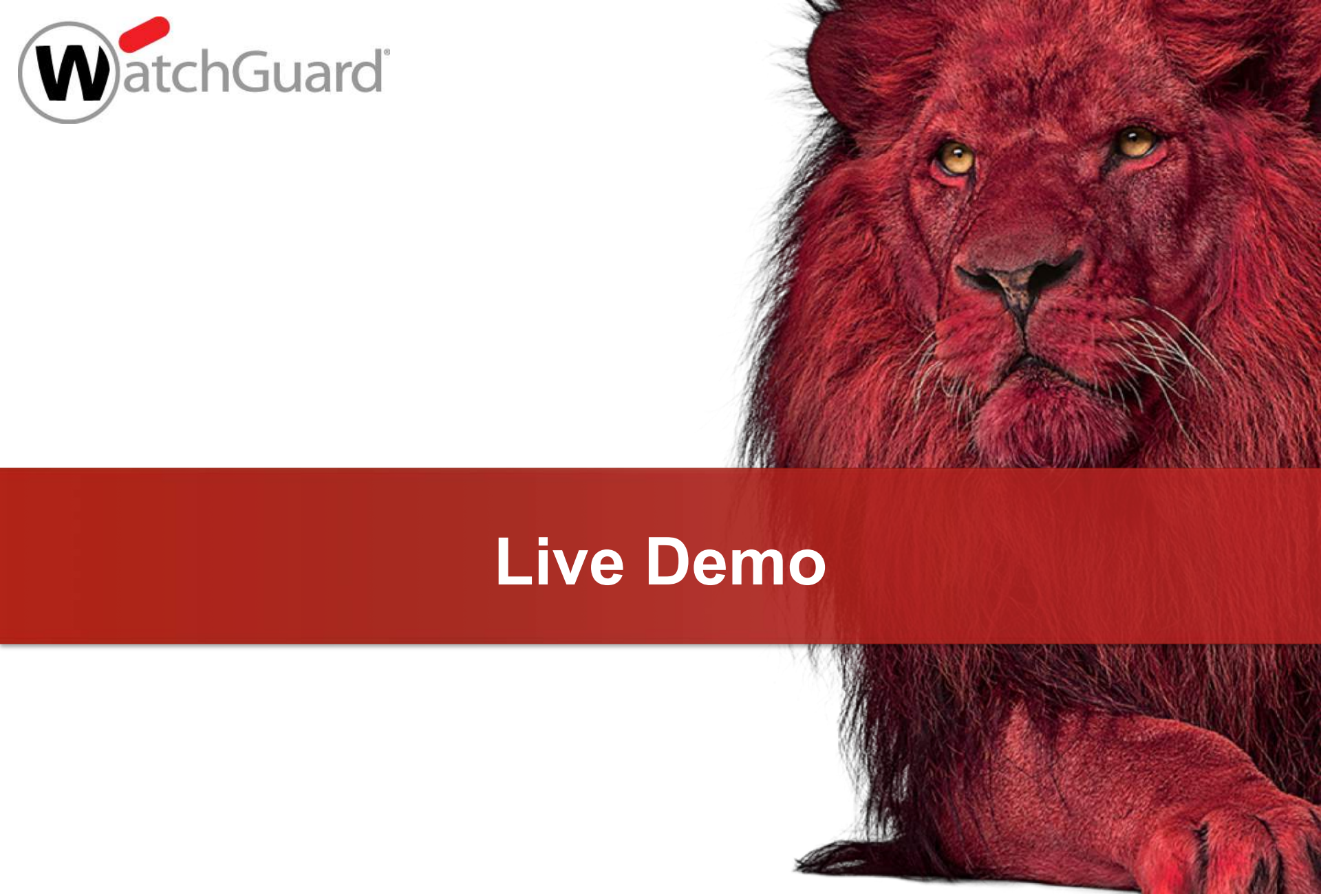
Es sieht so aus, als hätten Sie auf etwas Gefährliches geklickt.

Schützen Sie sich vor Phishing-Gefahren.

- Wenn Sie eine unerwartete E-Mail erhalten, sollten Sie auf einen verdächtigen Betreff achten und das Feld VON der E-Mail sorgfältig prüfen, um sicherzugehen, dass diese von einer legitimen Quelle gesendet wurde.
- Achten Sie genau auf Grammatik-, Schreib- und Kommafehler in Betreff, Text der E-Mail und den URLs.
- Falls Sie eine unerwartete E-Mail mit Hyperlinks erhalten, sollten Sie mit Ihrer Maus auf den Hyperlink zeigen, bevor Sie darauf klicken, um zu sehen, ob er zum Thema der E-Mail passt.
- Seien Sie bei allen E-Mails, die Sie erhalten und die sich als vom Management gesendet ausgeben oder Konsequenzen androhen, falls Sie nicht handeln, misstrauisch.
- Falls Sie Zweifel haben, forschen Sie nach, bevor Sie handeln.
- Klicken Sie nicht auf Links in Benachrichtigungsemails von sozialen Medien.
- Gehen Sie stattdessen direkt zu der App, um Beiträge und Bilder zu sehen.

Intensive Analysemöglichkeiten





Live Demo

Und wenn das nicht reicht?

Allgemeiner Schutz vor Datendiebstahl und Verlust mit Total Security

Verhinderte Angriffe in Deutschland

https://www.secplicity.org/threat-landscape/?s=2019-01-01&e=2019-01-21&type=all&region=DE

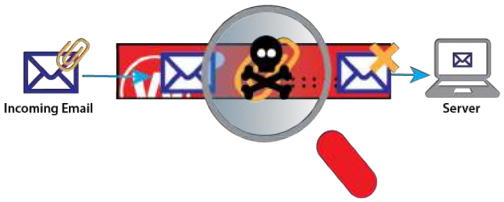
Ein mehrschichtiger Sicherheitsansatz

WatchGuard sprengt die Fesseln der Cyber Kill Chain® in jeder Bedrohungsphase – durch einen mehrschichtigen Sicherheitsansatz, intelligente **Abwehr**, die **Erkennung** von und **Reaktion** auf Bedrohungen, die gezielte Angriffe im Keim ersticken

Malware Erkennung am Gateway

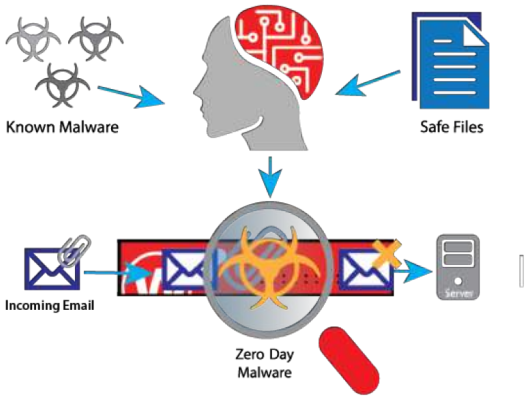
1. Gateway Antivirus

signaturbasierte AV Engine



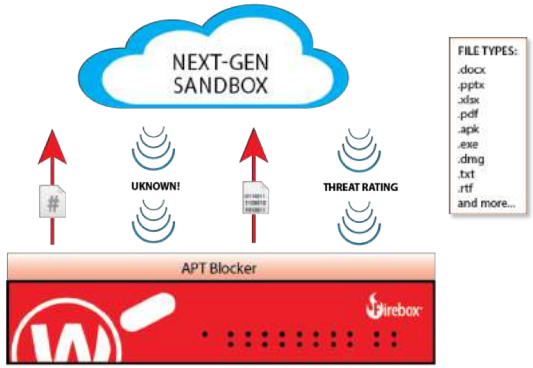
2. Intelligent AV

KI unterstützte Malware Erkennung

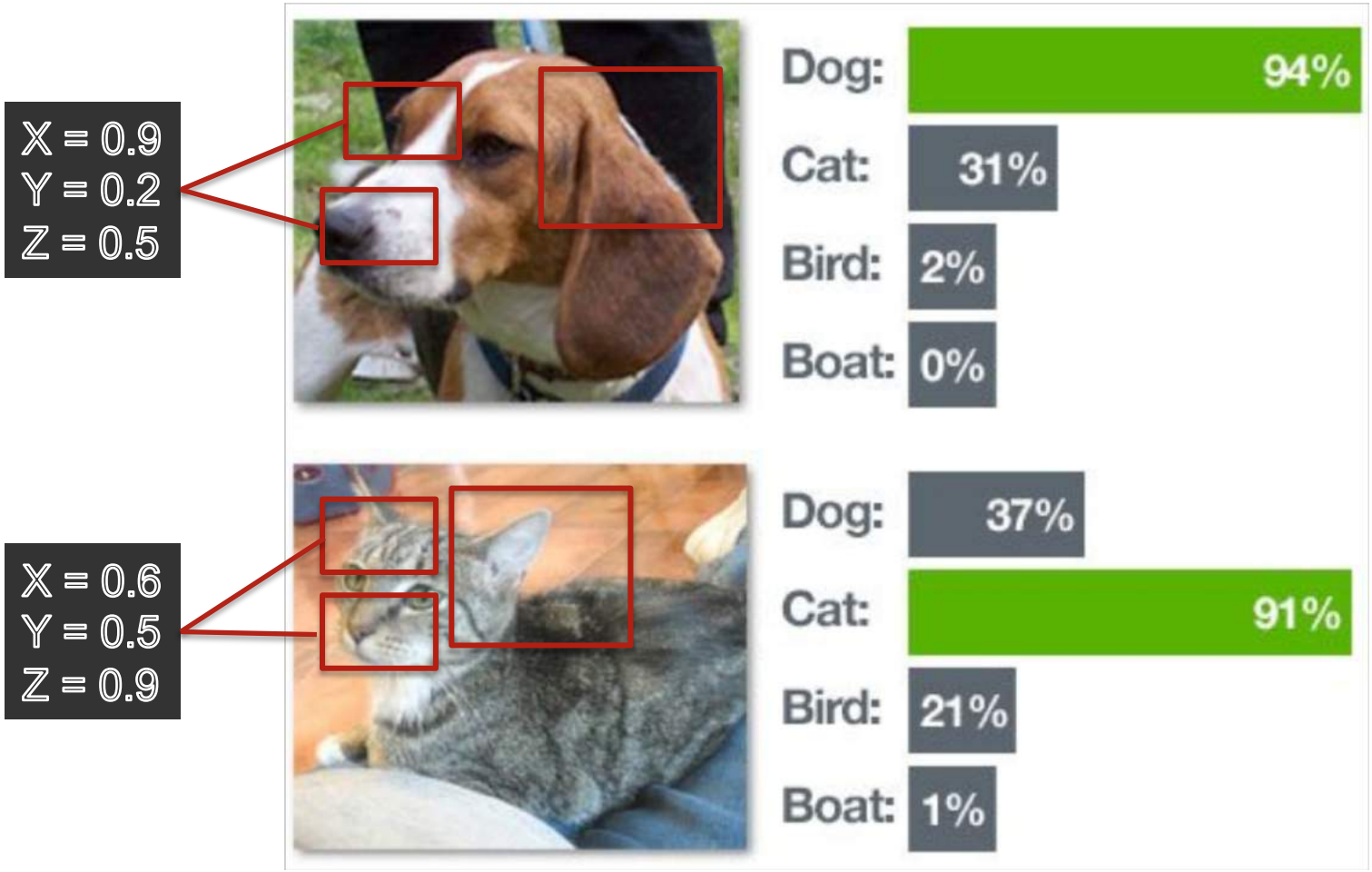


3. APT Blocker

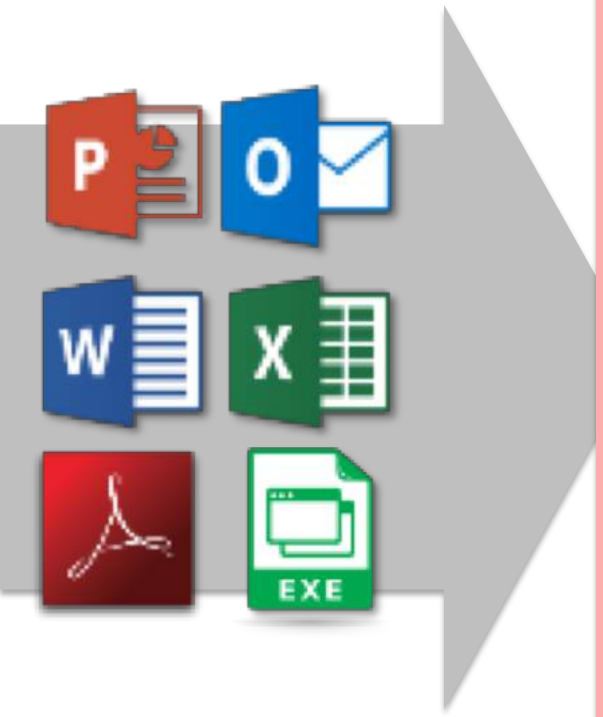
Sandbox Technologie



Künstliche Intelligenz?



Schutz mit KI für Firebox : IntelligentAV

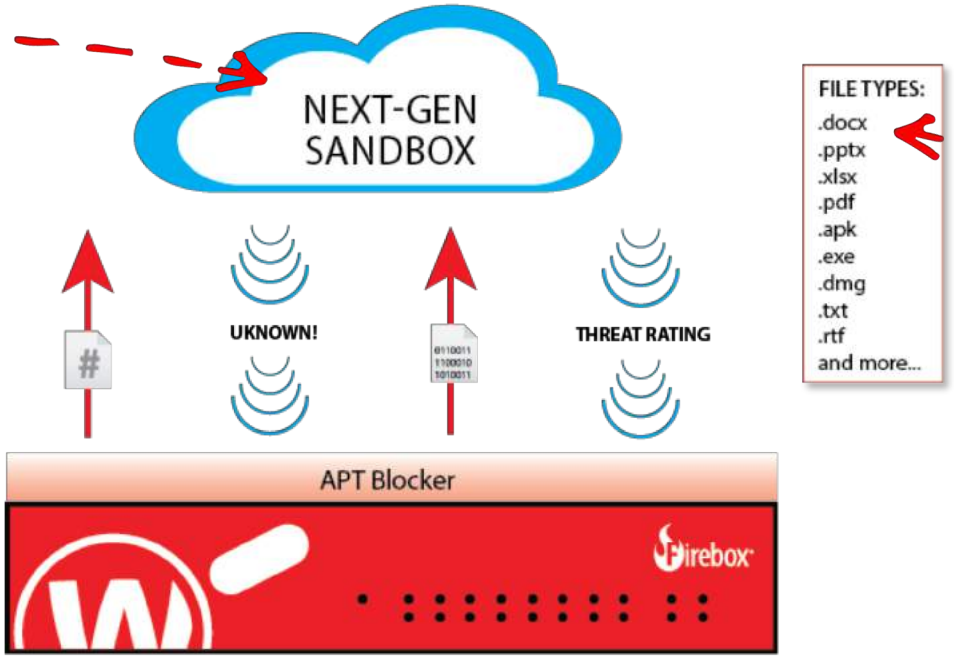


DOS Header
NT Header
File Header
Section Headers
Export Directory
Import Directory
Resource Directory
Relocation Directory
Debug Directory
Packer Used
Compiler Type
Compiler Language
File size
PE size
Image section headers
Functions called
Kernel hooks
Image Paths
Image Resource Directory
Bitmaps
Icons
Strings
RCData
Icon Groups
Version Info…

```
lea     rcx,[rdi+20h]
mov     qword ptr [rdi+8],r13
mov     qword ptr [rdi+10h],r13
mov     qword ptr [rdi+18h],r13
mov     qword ptr [rcx+20h],r12
mov     qword ptr [rcx+18h],r13
lea      rdx,[rsp+258h]
or       r9,0FFFFFFFFFFFFFFFFh
xor      r8d,r8d
mov     word ptr [rcx+8],r13w
mov     ebx,r14d
```

Detailanalyse mit APT Blocker

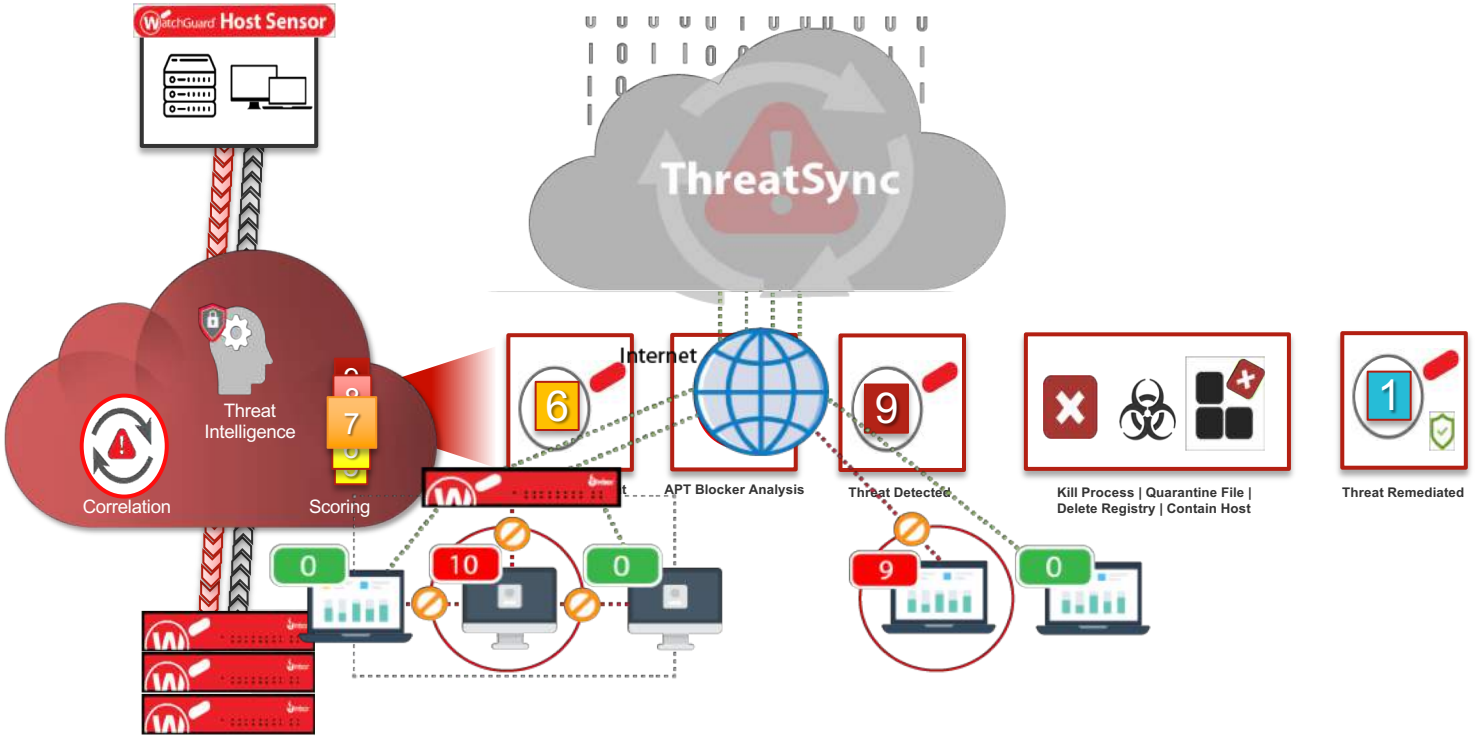
Weiterleitung potenziell gefährlicher Inhalte an Cloud-Sandbox



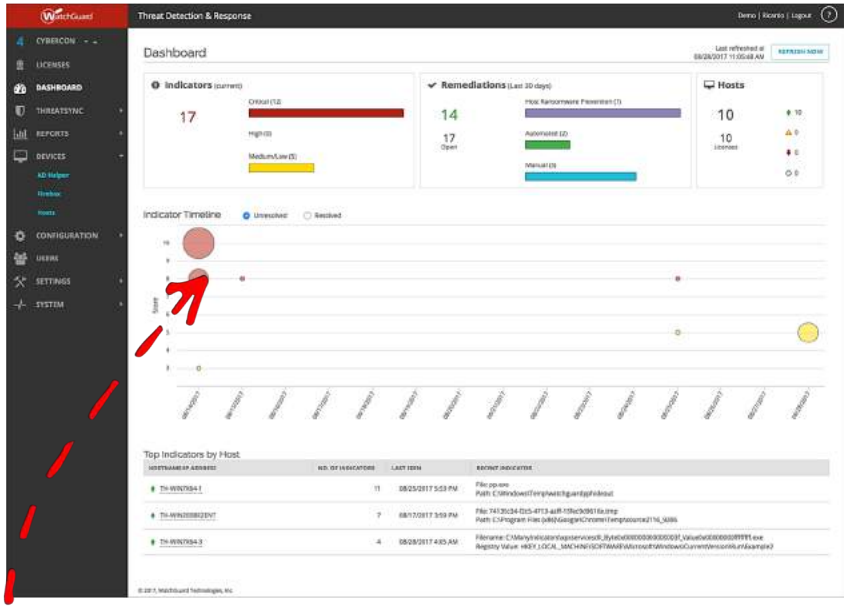
Gründliche Analyse einer Vielzahl von Dateitypen

Korrelation - Threat Detection & Response

Schutz bis zum Endpoint durch TDR

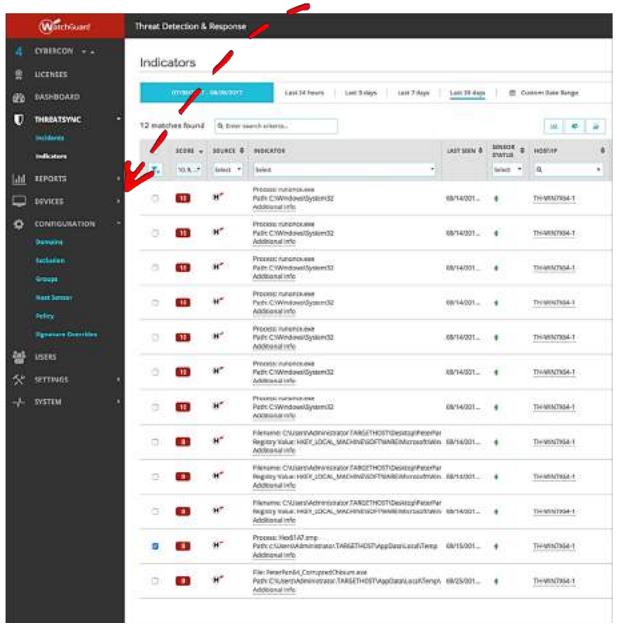


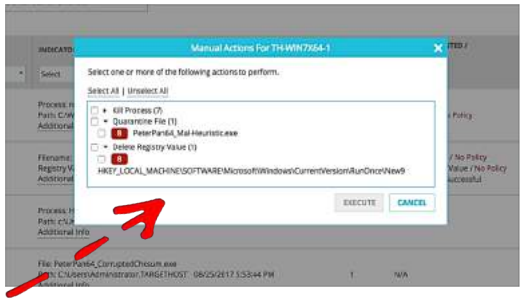
TDR - Den Überblick behalten und Abhilfe schaffen



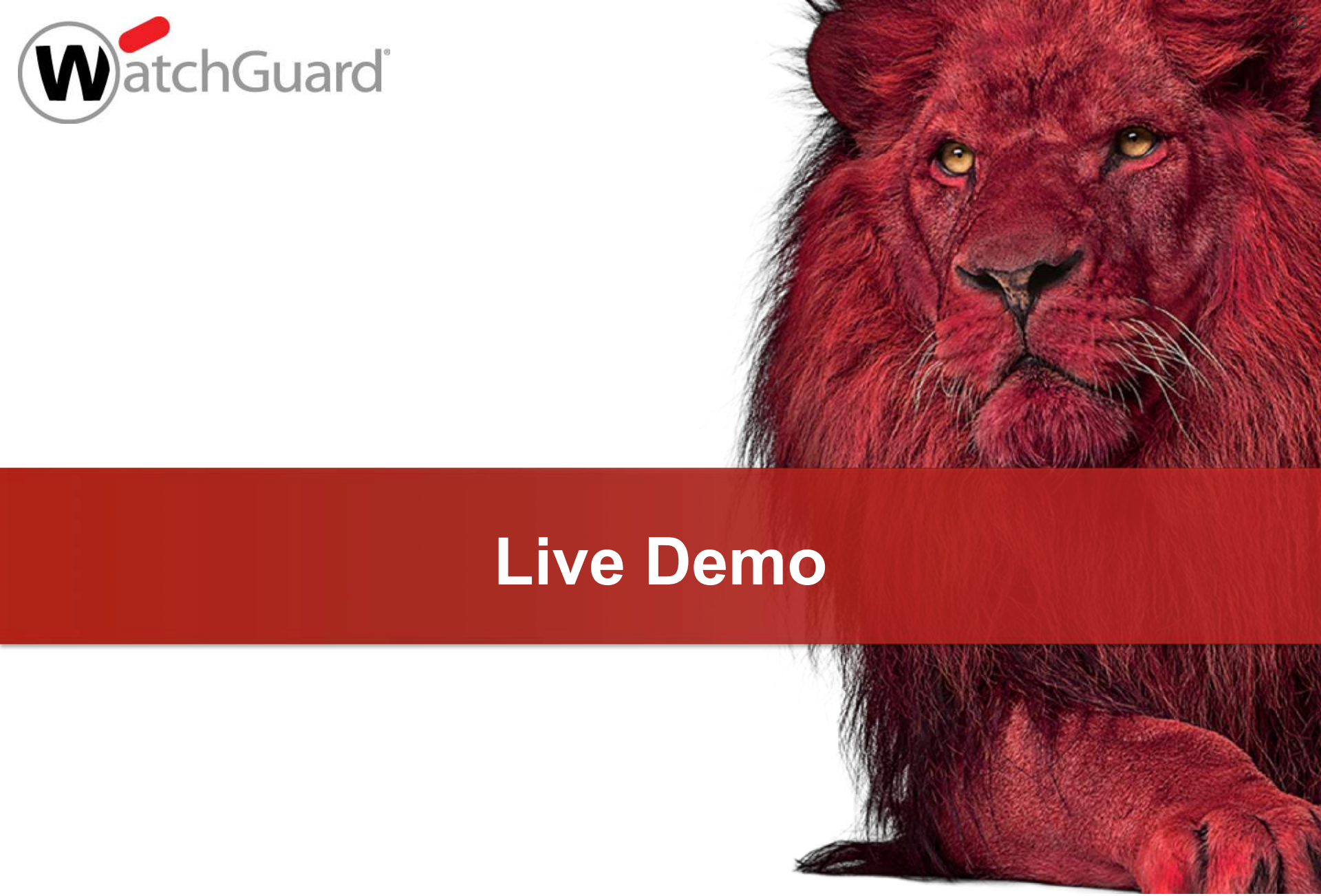
Schneller Überblick zu Bedrohungsaktivitäten im gesamten Unternehmen

Die Gefahr beurteilen





Beseitigung zahlreicher Bedrohungen



Live Demo

Wo sind eigentlich Ihre Daten?

Dropbox

37%
Accidental Loss

32%
Criminal Hacker

20%
Malcontent Insider

4%
IP-Stealing Nation State

4%
Hacktivists

Schutz vor Insidern durch Data Loss Prevention

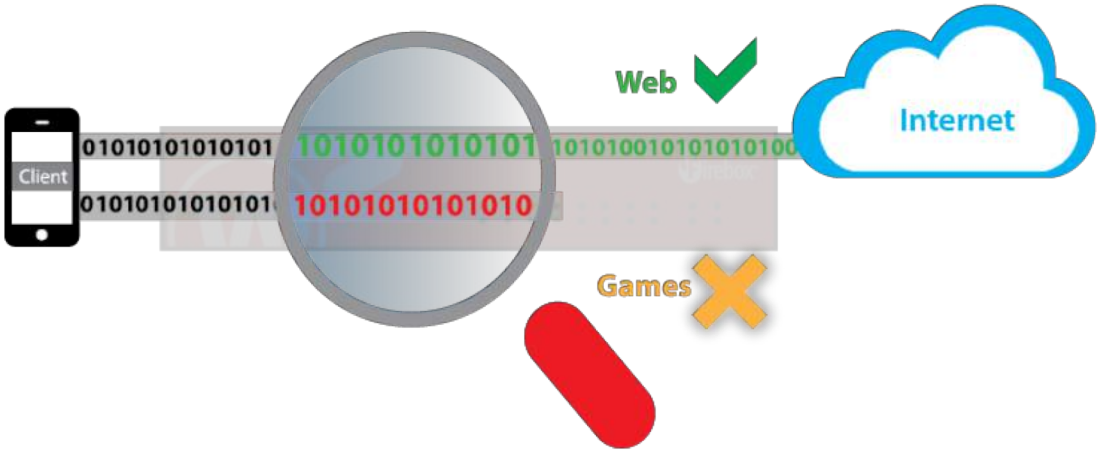
- Auch Mitarbeiter treffen falsche Entscheidungen
  - Unachtsamkeit
  - gezielter Diebstahl

- Schützen Sie sensible Daten vor dem Transfer in unkontrollierbare Cloud-Applikationen

Schutz vor Insidern durch Application Control

- Verhindern und steuern Sie die Applikations-Nutzung im Unternehmensumfeld

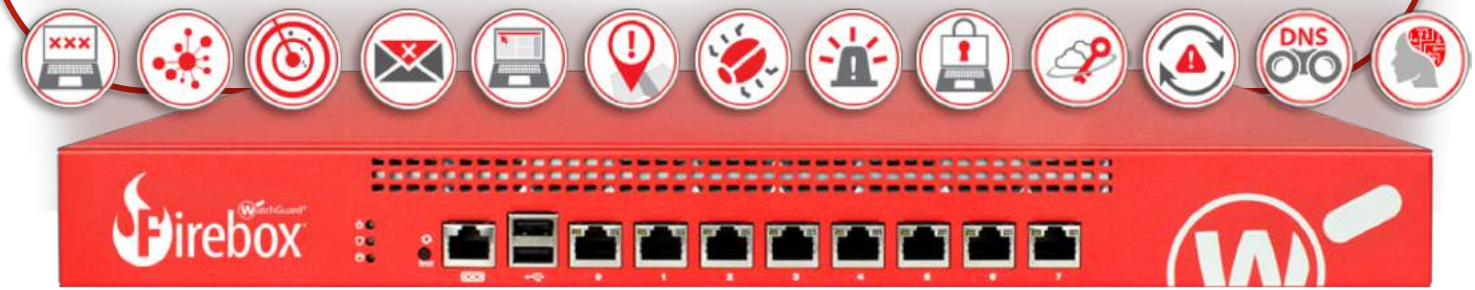
- Filesharing, P2P, Tunneling-Applikationen, etc.



Umfassender Schutz mit Total Security Suite

Features & Services	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection & Response	✓	
DNSWatch	✓	
Access Portal*	✓	
IntelligentAV*	✓	
Dimension Command	✓	
Support	Gold (24x7)	Standard (24x7)

*Available on Firebox M Series appliances



Vielen Dank!

NOTHING GETS PAST RED.