

A detailed illustration of a lion, rendered with a strong red color cast. The lion is shown from the side, facing right, with its mane and body fur clearly visible. The background is white.

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 Bunte

🔊 | 🖨️ | 💬 174



<https://www.heise.de/newsticker/meldung/Parteihack-Persoelliche-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>

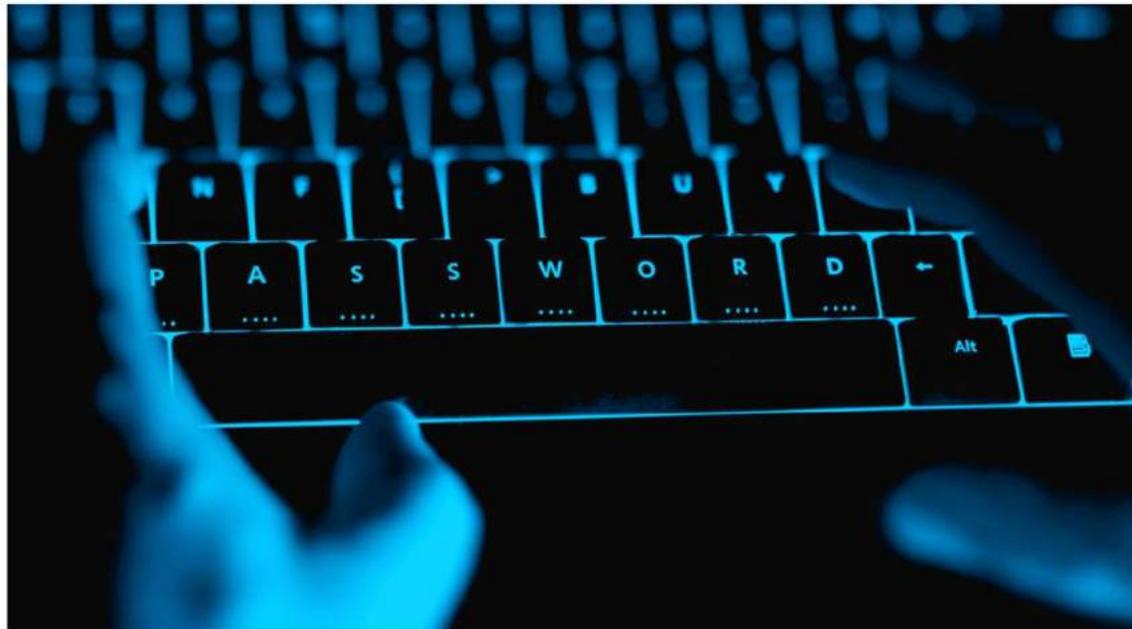
17.01.2019 09:59 Uhr | Security

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!



Zu einfach!

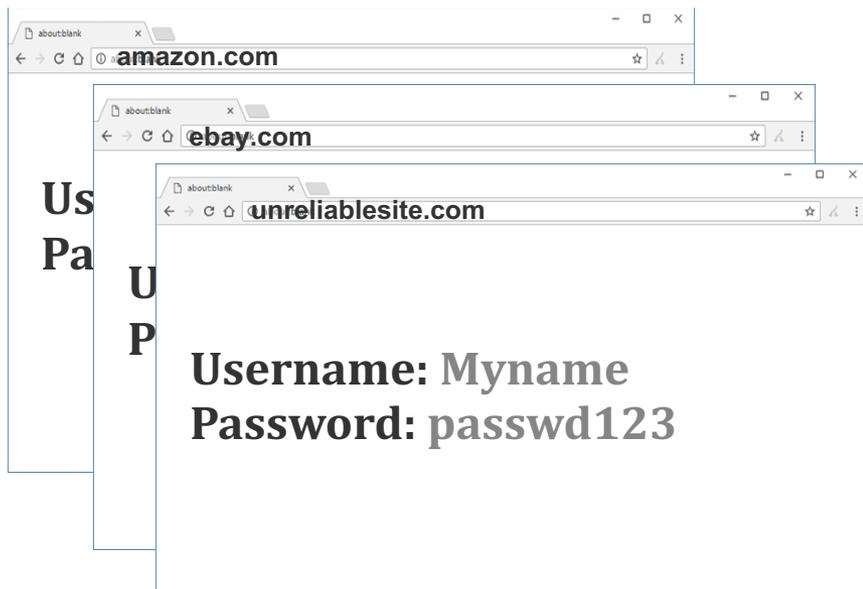


Eingabe im öffentlichen Wi-Fi oder Internet-Cafe!



Passwörter geraten schnell in falsche Hände

Nur 1 Passwort!



Malware Infektion!



Passwort vergessen!

Reset password

Please enter your email address to request a password reset.

EMAIL ADDRESS

RESET PASSWORD

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 das Kennwort gestohlen ist.



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

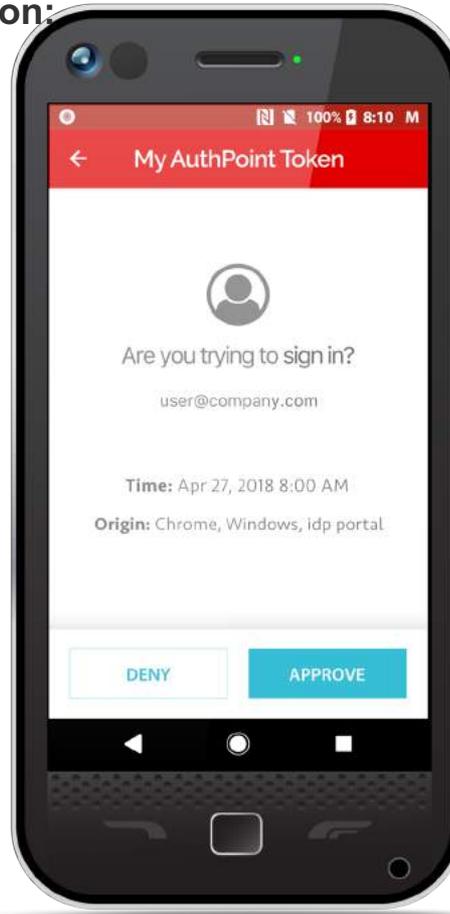
Was ist Multi-Faktor-Authentifizierung?

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)

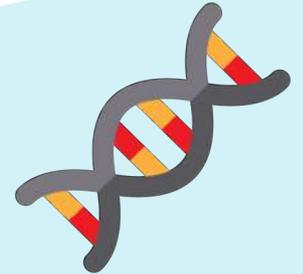
Password

•••••

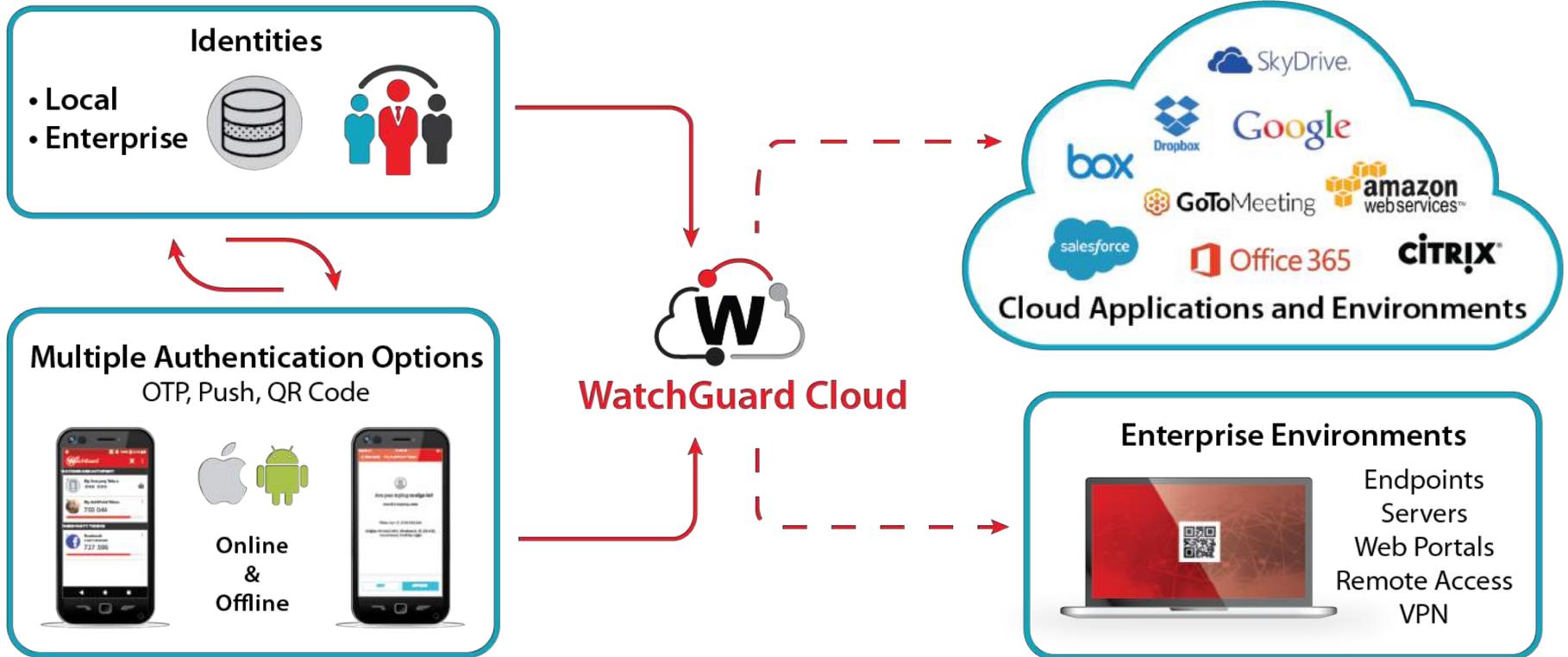


AuthPoint-Faktoren:

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

The screenshot displays the WatchGuard Cloud dashboard interface. At the top left is the WatchGuard logo and a hamburger menu icon. The page title is "Dashboard". On the right, there is an "Account Name" field with a help icon, a phone icon, and a user profile icon.

A dark sidebar on the left contains the following navigation items: Dashboard (highlighted), Reports, Logs & Events, Alerts & Indicators, Configure Services, and Administration.

The main content area features a welcome message: "Welcome to WatchGuard Cloud!" followed by a brief mission statement. Below this are eight data cards arranged in a 2x4 grid:

- Authentications:** 23 Failed Authentications (with a red exclamation mark icon) and 150 Successful Authentications.
- Resources:** A bar chart showing usage for SAML (11), RADIUS (6), Logon App (4), and Others (1).
- Licensed Users:** 55 of 125 licenses used, with 70 unallocated licenses. Includes an "Allocate User License" button.
- Denied Push Notifications:** 8 Denied notifications. A note explains: "This could occur because a token was not available or incorrect, or the request timed out."
- Users:** 28 Active Users. Subtext: "1001 licensed users, 973 unused user licenses". Includes an "Add Users" button.
- License Details:** 1001 Active Users. Subtext: "8 months until your license expires on 2019-12-15".
- Tasks:** A list of task statuses: Completed (15), Pending (0), Failed (14), and Scheduled (3). Filtered for "Last 24 Hours".
- Support:** Options for "Phone Support" (for critical issues) and "Online Support" (for non-critical issues).

A red-tinted background featuring a globe with a network of white lines and glowing nodes, suggesting global connectivity and security.

Live Demo



**Falsch geklickt
Wirkungsvoller Schutz vor Phishing**

Unterschiedliche Zielpersonen

Phishing Angriffe beziehen sich gezielt auf „Menschen“

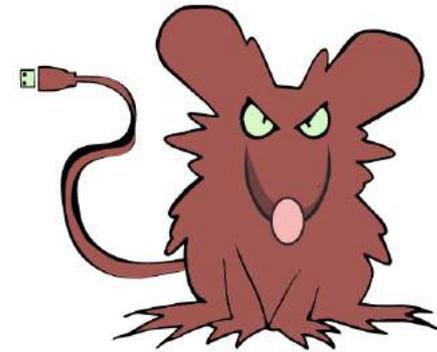


Die Folgen sind vielfältig

.....nicht nur Ransomware

The image shows two overlapping screenshots. The top one is a ransomware payment screen for 'Wana Decrypt0r 2.0'. It features a red background with a padlock icon and German text: 'Oops, your files have been encrypted!', 'Was geschah mit meinem Computer?', 'Kann ich meine Dateien wiederherstellen?', and 'Payment will be raised on 6/1/2017 14:39:55'. A countdown timer shows '02:23:59:56'. The bottom screenshot is a VirusTotal scan of a file named '10_Dezember_2016_12_31_23_Uhr.doc'. It shows '16 / 59' engines detected the file as malicious. The detection table is as follows:

Detection	Details	Relations	Community
Arcabit	HEUREVBA.Trojan	CAT-Qui-Moul	W97M/Encrpt.Hur
Engame	malicious (high confidence)	Fortinet	VBA/Agent.LIBtridd
GData	Macro.Trojan.Downloader.ShadowS	Ikarus	Trojan.VBA.Agent
McAfee	W97M/Downloader.egg	McAfee GW Edition	Enhance/Downloader.egg
Microsoft	Trojan/DotNet/Fonttype.Arm	NANO Antivirus	Trojan.Dro.Vba-hauratic.buett
Qihoo-360	virus/malicious-gen/1080	SentinelOne	static engine-malicious
Symantec	OB.Downloader.gen172	TACHYON	Suspicious/W97M/Obfus.Gen6
Tencent	Hur/Macro.Genetic.Gen3	Zoner	Probably.W97/Defuncted
Ad-Aware	Clean	Avast Lab	Clean



Früher Konter gegen Phishing Attacken

DNSWatch DOMAINS ▾ REPORTS ▾ ALERTS JONAS SPIECKERMANN ▾

unocl45trpuoefftl.jageshere[.]club
[Firebox] T35-W-JSP [Interface] WAN_Wi-Fi (80.187.116.59)

CLASSIFICATION: **Ransomware** PROTOCOL: HTTP

Details | Discussion (1) | Domain Analysis | Malware Analysis | History | Connections

Victim Information	
Victim location ⓘ	[Firebox] T35-W-JSP [Interface] WAN_Wi-Fi (80.187.116.59)
Victim IP addresses ⓘ	10.0.1.2
Victim hostname	Unknown
Victim usernames	None

Destination Information	
Destination domains	unocl45trpuoefftl.jageshere[.]club
Destination port	80

Malware Information	
Malware family	HTTP

Connection Information	
Status:	🔒 Closed
Number of connections:	1

Actions ⓘ

✓ RESOLVE ALERT

⏸ SILENCE ALERTS

First Seen	
When:	1 week, 6 days ago
Date:	2018-04-06 14:46:01 CEST

Schutz mit Awareness Training



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

Alert unocl45trpuoefft[.]ageshere[.]club
[Firefox] T3S-WJSP [Interface] WAN_WI-FI (80.187.116.59)

Classification: **Ransomware** Protocol: HTTP

Details Discussion (1) Domain Analysis Malware Analysis History Connections

Initial connection details

Netflow data

First seen:	vor 9 Monate, 2 Wochen 2018-04-06 14:46:01 CEST	Last seen:	vor 9 Monate, 2 Wochen 2018-04-06 14:47:02 CEST
Victim hostname:	Unknown	Destination hostname:	unocl45trpuoefft[.]ageshere[.]club
Victim IP address:	80.187.116.59	Destination port:	80
Victim port:	11301	Malware family:	HTTP

Initial Connection Bytes

Below is a hexdump of the first bytes sent by the victim to DNSWatch.

```
0000 47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 00 0A  GET / HTTP/1.1..
0010 48 6F 73 74 3A 20 75 6E 6F 63 6C 34 35 74 72 70  Host: unocl45trp
0020 75 6F 65 66 66 74 2E 61 67 65 73 68 65 72 65 2E  ueofft.ageshere.
0030 63 6C 75 62 00 0A 55 73 65 72 2D 41 67 65 6E 74  club..User-Agent
0040 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 4D  : Mozilla/5.0 (M
0050 61 63 69 6E 74 6F 73 68 3B 20 49 6E 74 65 6C 20  acintosh; Intel
0060 4D 61 63 2D 4F 53 20 58 20 31 30 2E 31 33 3B 20  Mac OS X 10.13;
0070 72 76 3A 35 39 2E 30 29 20 47 65 63 68 6F 2F 32  rv:59.0) Gecko/2
0080 30 31 30 30 31 30 31 20 46 69 72 65 66 6F 78 2F  0100101 Firefox/
0090 35 39 2E 30 0D 0A 41 63 63 65 70 74 3A 20 74 65  59.0..Accept: te
00A0 78 74 2F 68 74 6D 6C 2C 61 70 70 6C 69 63 61 74  xt/html,applicat
00B0 69 6F 6E 2F 78 68 74 6D 6C 2B 78 60 6C 2C 61 70  ion/xhtml+xml,ap
00C0 70 6C 69 63 61 74 69 6F 6E 2F 78 6D 6C 3B 71 3D  plication/xml;q=
00D0 30 2E 39 2C 2A 2F 2A 3B 71 30 30 2E 38 00 0A 41  0.9,*/*;q=0.8..A
00E0 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20  ccept-Language:
00F0 64 65 2C 65 6E 2D 55 53 3B 71 30 30 2E 37 2C 65  de,en-US;q=0.7,e
```

Connection Information

Status: Closed
Number of connections: 1

Actions

RESOLVE ALERT
SILENCE ALERTS

First Seen

When: vor 9 Monate, 2 Wochen
Date: 2018-04-06 14:46:01 CEST

Last Seen

When: vor 9 Monate, 2 Wochen
Date: 2018-04-06 14:46:01 CEST

Full list of connections

ACTIONS

VIEW



Live Demo



A red-tinted background featuring a globe with white grid lines and a network of white lines connecting various points on the globe, suggesting global connectivity and security.

Und wenn das nicht reicht?

Allgemeiner Schutz vor Datendiebstahl und Verlust mit Total Security

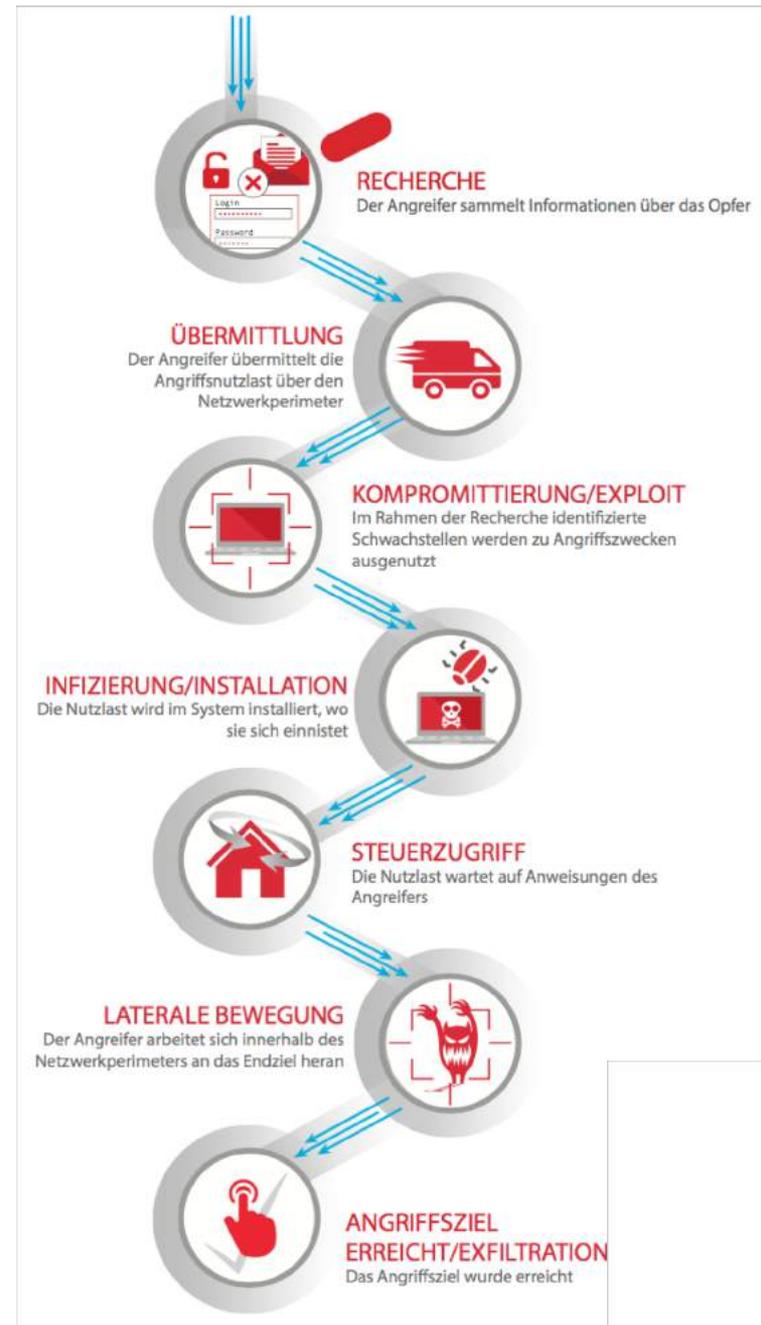
Verhinderte Angriffe in Deutschland



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

Ein mehrschichtiger Sicherheitsansatz

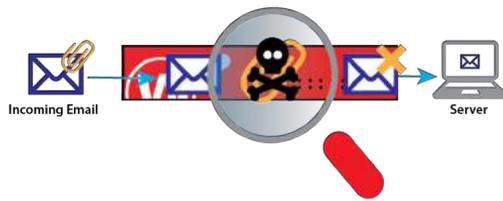
WatchGuard sprengt die Fesseln der Cyber Kill Chain® in jeder Bedrohungsphase – durch einen mehrschichtigen Sicherheitsansatz, intelligente **Abwehr**, die **Erkennung** von und **Reaktion** auf Bedrohungen, die gezielte Angriffe im Keim ersticken



Malware Erkennung am Gateway

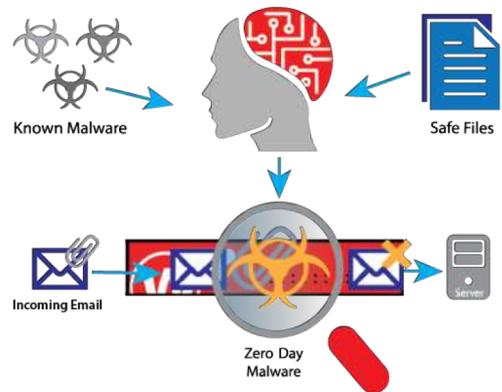
1. Gateway Antivirus

signaturbasierte AV Engine



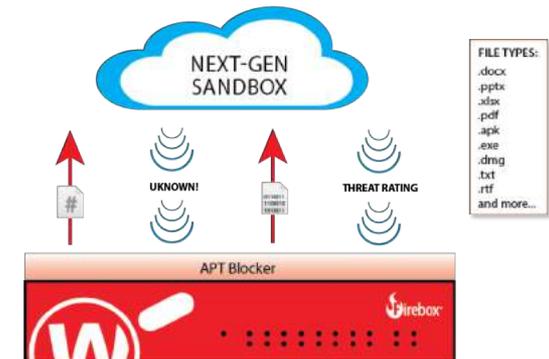
2. Intelligent AV

KI unterstützte Malware Erkennung



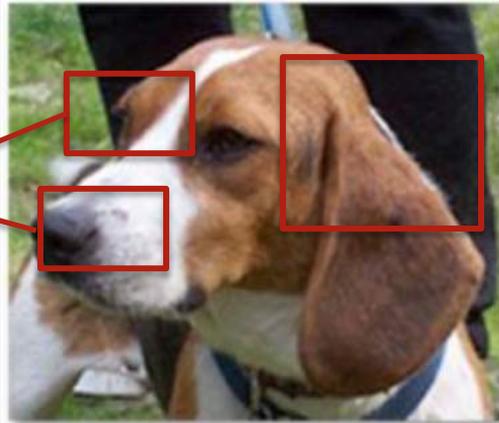
3. APT Blocker

Sandbox Technologie



Künstliche Intelligenz?

X = 0.9
Y = 0.2
Z = 0.5



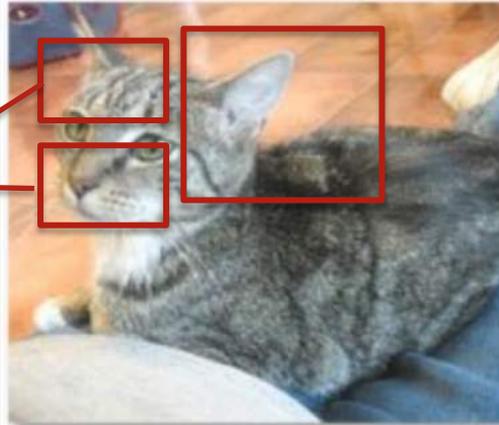
Dog: 94%

Cat: 31%

Bird: 2%

Boat: 0%

X = 0.6
Y = 0.5
Z = 0.9



Dog: 37%

Cat: 91%

Bird: 21%

Boat: 1%

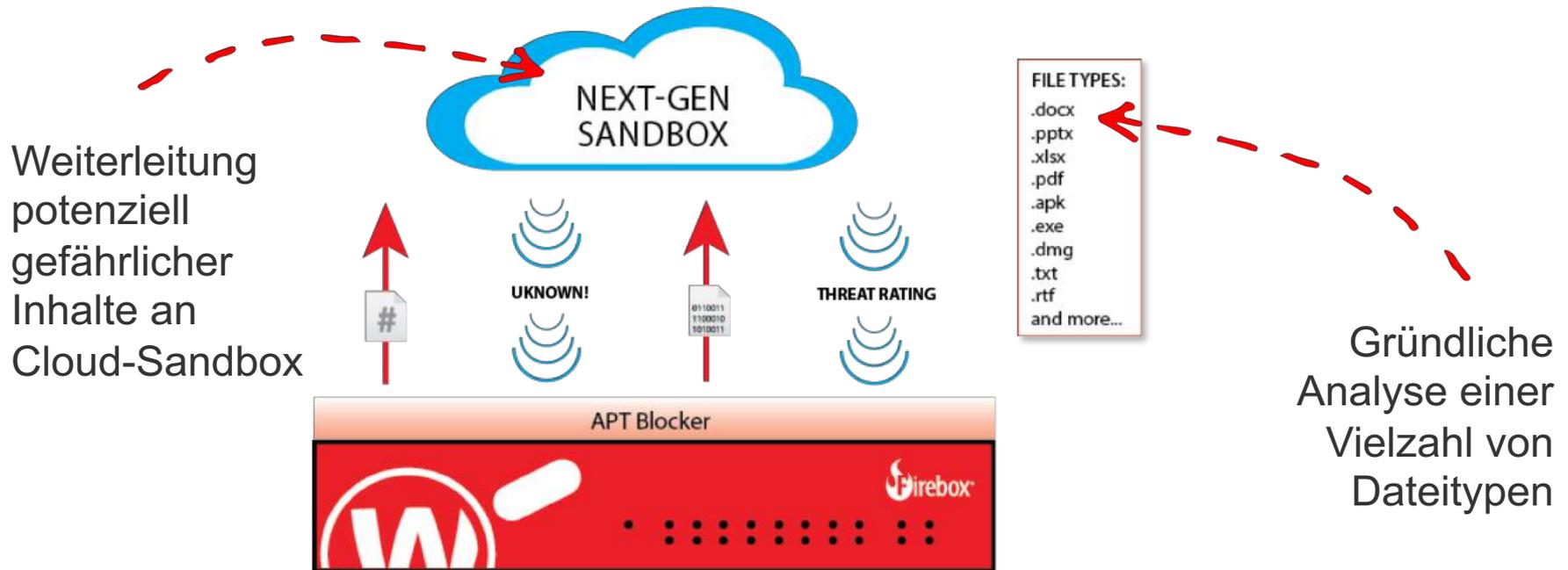
Schutz mit KI für Firebox : IntelligentAV



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...

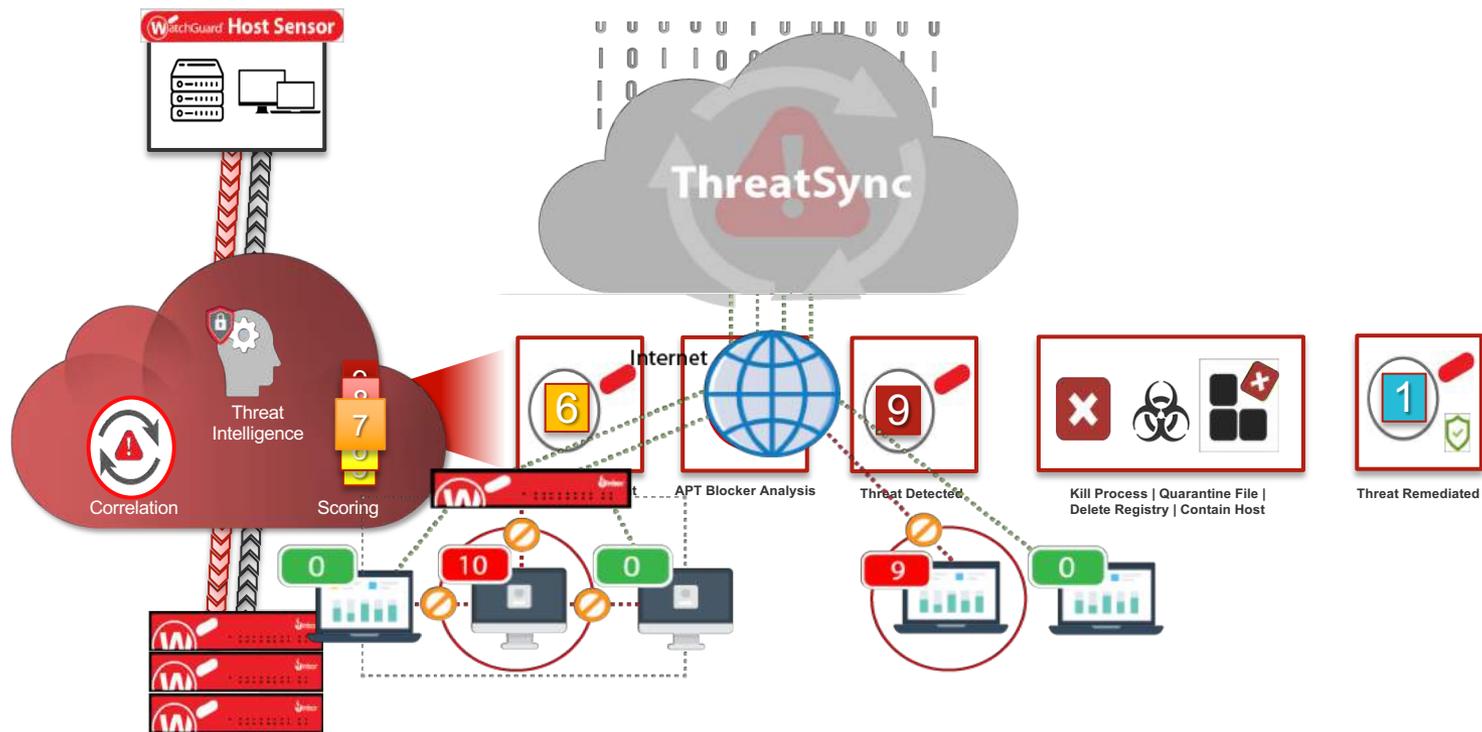
```
lea rcx,[rdi+20h]
mov qword ptr [rdi+8],r13
mov qword ptr [rdi+10h],r13
mov qword ptr [rdi+18h],r13
mov qword ptr [rcx+20h],r12
mov qword ptr [rcx+18h],r13
lea rdx,[rsp+258h]
or r9,0FFFFFFFFFFFFFFFFh
xor r8d,r8d
mov word ptr [rcx+8],r13w
mov ebx,r14d
```

Detailanalyse mit APT Blocker

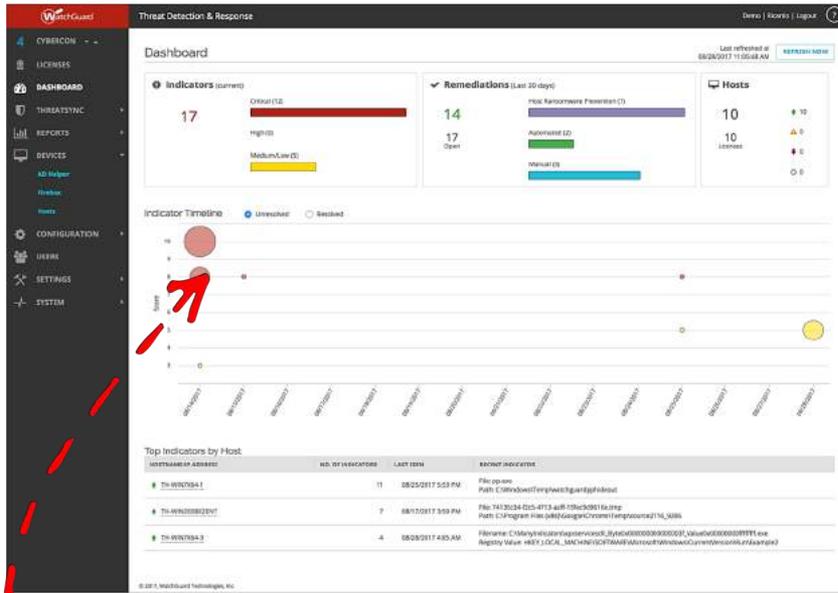


Korrelation - Threat Detection & Response

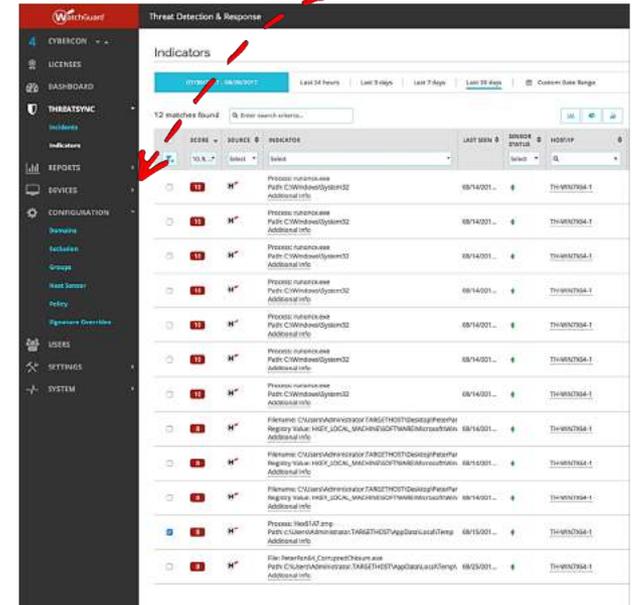
Schutz bis zum Endpoint durch TDR



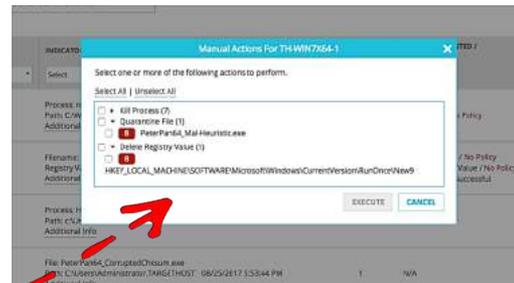
TDR - Den Überblick behalten und Abhilfe schaffen



Die Gefahr beurteilen



Schneller Überblick zu Bedrohungsaktivitäten im gesamten Unternehmen



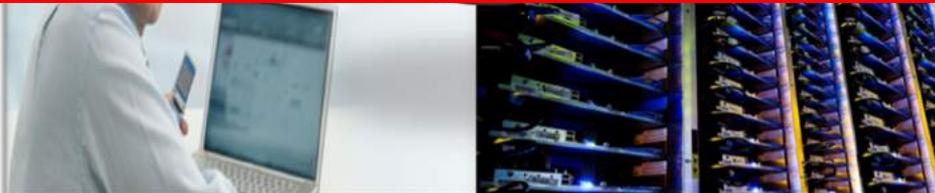
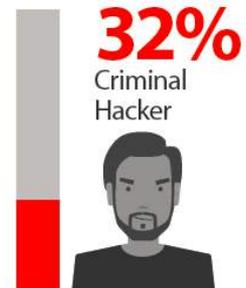
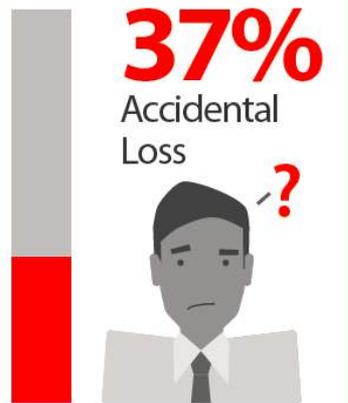
Beseitigung zahlreicher Bedrohungen



Live Demo



Wo sind eigentlich Ihre Daten?



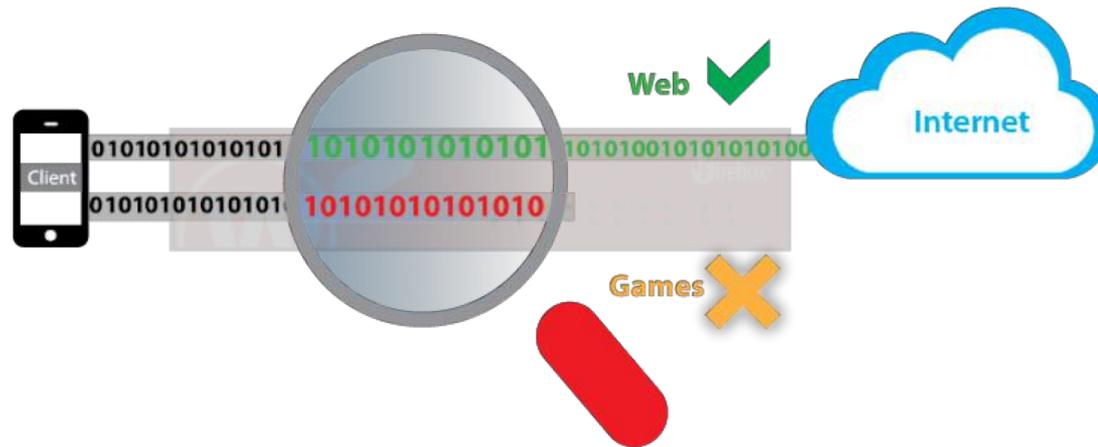
Schutz vor Insidern durch Data Loss Prevention

- 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.***

