BeyondTrust

Sechs Dinge, die Sie zum Schutz vor Ransomware-Angriffen wissen sollten

17. Mai 2022

Laszlo Stadler
Senior Solutions Engineer

Ransomware-Bedrohungen

WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

In ganz England hat ein Kryptotrojaner am Freitag zahlreiche Krankenhäuser lahmgelegt. Und das ist offenbar nur die Spitze des Eisbergs einer globalen Welle von Infektionen mit Wana Decrypt0r 2.0 oder einfach WannaCry.

Zeitungsproduktion gestört

Funke Mediengruppe wurde mit Erpressungstrojaner angegriffen

Zahlreiche Computer gingen vom Netz, von bekannten Tageszeitungen wie der »WAZ« erschienen nur Notausgaben: Die Funke Mediengruppe kämpft weiter mit den Folgen einer Ransomware-Attacke.

23.12.2020, 14.54 Uhr

Der Aufstieg der Ryuk Ransomware

19. Januar 2021

RANSOMWARE

Colonial Pipeline über kompromittiertes Passwort gehackt

Der kürzlich gehackte Pipelinebetreiber Colonial äußert sich zu dem Vorgehen der Ransomware-Gruppe Darkside.

7. Juni 2021, 11:24 Uhr, Moritz Tremmel

IT-Angriff legt Schwerin und Landkreis lahm

Der IT-Dienstleister für Schwerin und einen Landkreis musste nach einem Ransomware-Angriff offline gehen. Die Bürgerbüros sind vorerst geschlossen.

15. Oktober 2021, 13:00 Uhr, Sebastian Grüner/ dpa

Ransomware-Angriffe auf Krankenhäuser - Sind Leben in Gefahr?

18. Oktober 2021

Sechs Dinge, die Sie über Ransomware wissen sollten

1

Ransomware ist Malware

Encryptors

Lockers

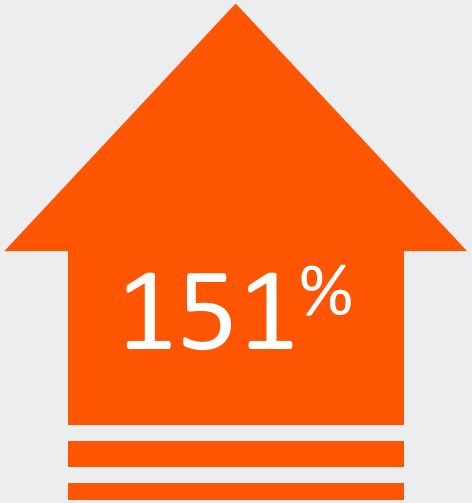
Doxware
(Extortion)

Scareware

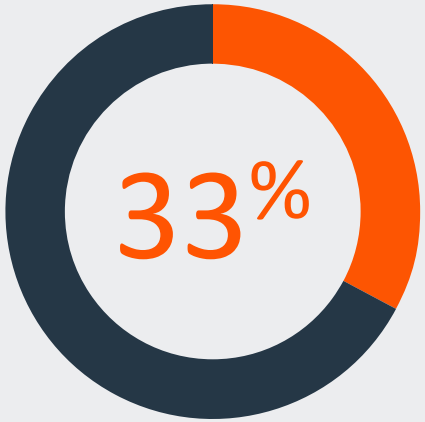
RaaS

2

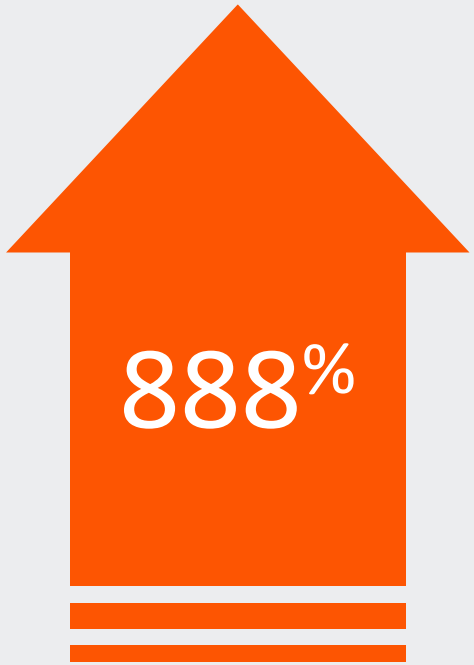
Ransomware-Angriffe nehmen zu



Zunahme von Ransomware in den ersten 6 Monaten in 2021[1]



Anstieg der Ransomware-Familien YoY[2]



Anstieg von dateiloser Malware in 2020[3]

1 Cyberthreat Report: Mid-Year Update. SonicWall. July 2021.
2 The State of Ransomware. TrendMicro. March 2021
3. Internet Security Report – Q4 2020. WatchGuard. March 2021

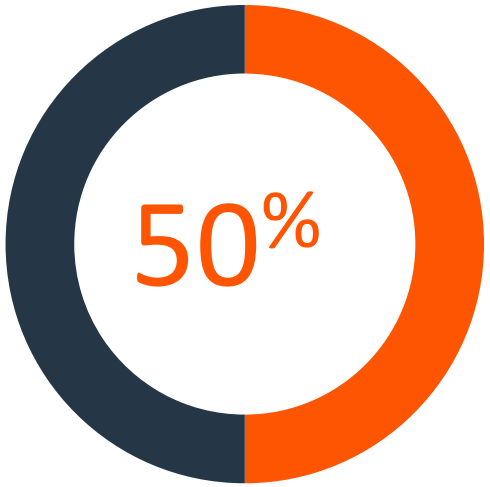
3 Die Angriffsfläche nimmt stark zu

ANGRIFFSVEKTOREN SIND VORHANDEN

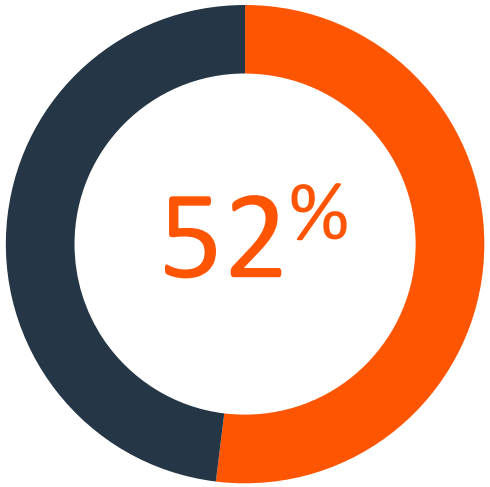
- Mehr Schwachstellen
- Mehr Fernzugriffe
- Mehr Privilegien
- Mehr Schatten-IT
- Mehr “BYOD / BYOT”
- Mehr Cloud, DX, Machine Identities, etc.

3 Die Angriffsfläche nimmt stark zu

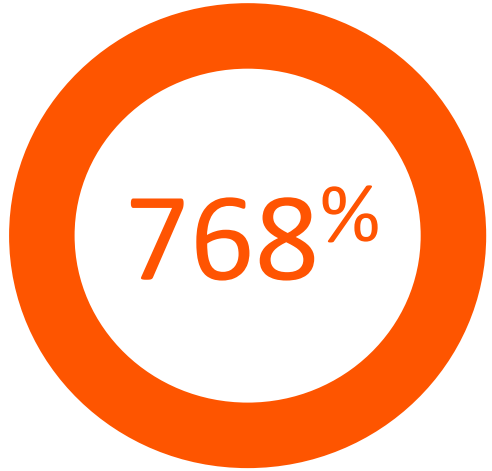
MEHR FERNZUGRIFFSMÖGLICHKEITEN



Zunahme der dem Internet ausgesetzen RDP-Ports in Q1 2020[1]



aller Ransomware-Angriffe im Jahr 2020 nutzten öffentlich zugängliche RDP-Server, um sich einen ersten Zugang zu verschaffen[2]



Anstieg der RDP-Angriffe zwischen Q1 und Q4 2020[3]

[1] Cybercriminals Actively Exploiting RDP to Target Remote Organizations. McAfee May 2020
[2] Ransomware Uncovered 2020/2021. Group-IB. March 2021
3. ESET Threat Report Q4 2020. Feb. 2021

4 Ransomware ist ein erfolgreiches Geschäftsmodell

Trends, die die Gewinnraten für Ransomware erhöhen

- "Naming & Shaming" - Angreifer machen einen Angriff oft bei den Kunden des Opfers und in den Medien bekannt, um das Opfer zur Zahlung zu zwingen.
- **Anstieg von 396%** der durchschnittlichen Auszahlungen für Ranswomware im Jahr 2021 (570.000 USD) gegenüber 2019 (115.000 USD)[1]
- Cybersecurity-Versicherung erhöht Auszahlungschancen
- Die Kosten für Ausfallzeiten oder das Reputationsrisiko sind zu hoch
- Ransomware-as-a-Service nimmt zu

1. Unit 42 Ransomware Threat Report, Palo Alto Networks. 2021

5 Die Zahlung des Lösegelds beendet nicht die Bedrohung

- Keine Garantie, dass der Angreifer den Zugang zu den Daten zurückgibt
- Zugang zu den Daten kann ermöglicht werden, aber die Daten könnten auch wieder verkauft (dies war 2020 verstärkt der Fall) oder erneut verschlüsselt werden.

“Blood in the Water”-Effekt

- Wenn die Grundursache (ungepatchte Sicherheitslücke, unsachgemäß verwaltete Berechtigungen, unsicherer Fernzugriff) nicht behoben wird, kann (wird) ein anderer geschickter Ransomware-Betreiber das selbe Opfer ausnutzen

6 Ransomware ist nicht komplex

„Ransomware ist keine Zauberei - sie kann nur mit den Rechten des Benutzers oder der Anwendung, die sie startet, ausgeführt werden.

Darin liegt ihre Schwäche und unsere Chance, Tools zu nutzen, um sie einzudämmen, bevor sie loslegt.“

G. Mark Hardy, CISSP, CISA Präsident,
National Security Corporation

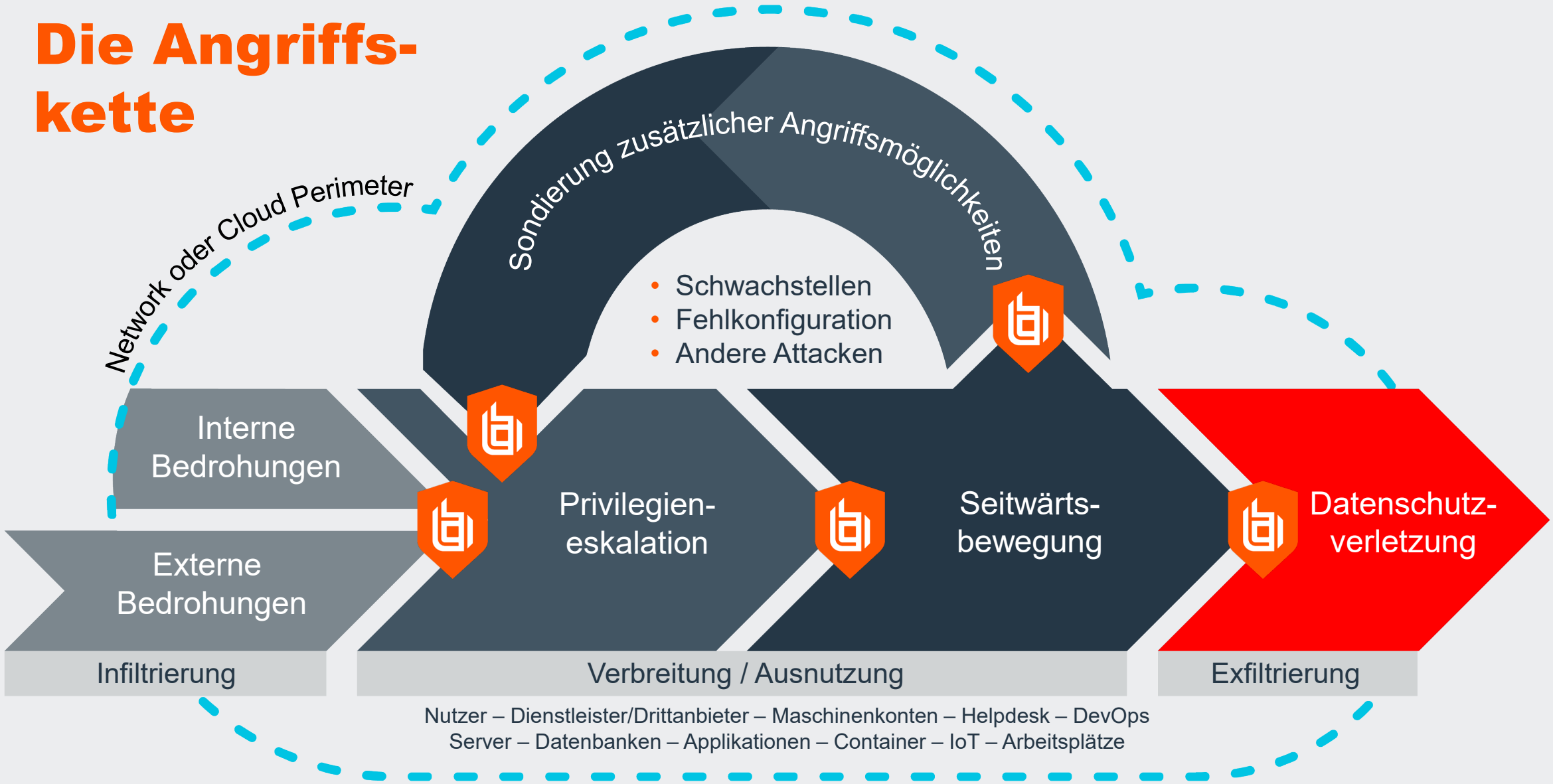
Schutz vor Ransomware

60%

der Angriffe werden von Antivirus-Software übersehen

2020 State of Endpoint Security, Ponemon

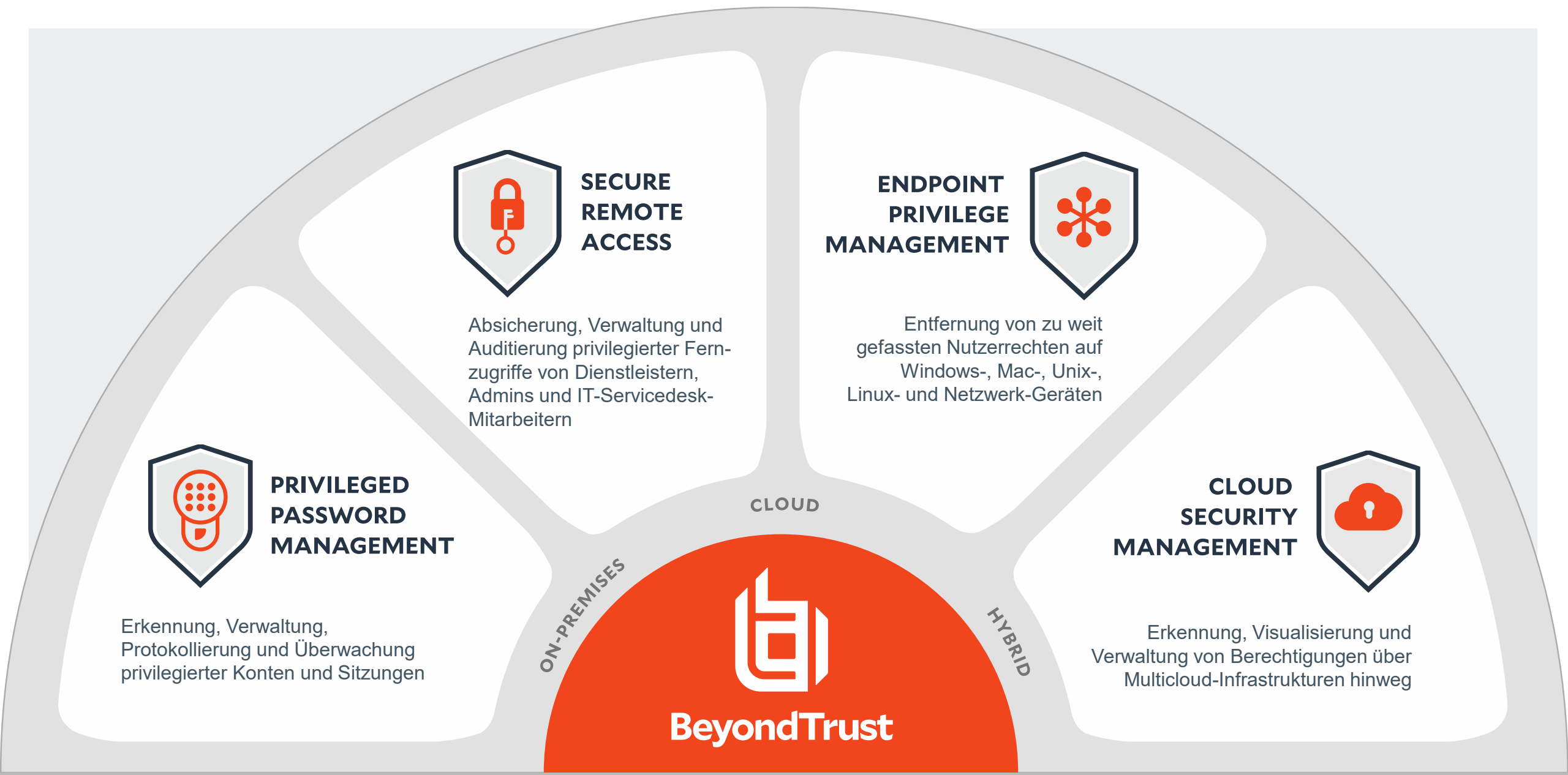
Die Angriffs-kette



BeyondTrust

Die Rolle von Privileged Access Management (PAM)

Schützen Sie Ihre IT-Umgebung vor Ransomware, Malware und anderen Bedrohungen


SECURE REMOTE ACCESS
Absicherung, Verwaltung und Auditierung privilegierter Fern-zugriffe von Dienstleistern, Admins und IT-Servicedesk-Mitarbeitern
ENDPOINT PRIVILEGE MANAGEMENT
Entfernung von zu weit gefassten Nutzerrechten auf Windows-, Mac-, Unix-, Linux- und Netzwerk-Geräten
PRIVILEGED PASSWORD MANAGEMENT
Erkennung, Verwaltung, Protokollierung und Überwachung privilegierter Konten und Sitzungen
CLOUD SECURITY MANAGEMENT
Erkennung, Visualisierung und Verwaltung von Berechtigungen über Multicloud-Infrastrukturen hinweg
CLOUD
ON-PREMISES
HYBRID
BeyondTrust
BEYONDINSIGHT Discovery | Reporting | Threat Analytics | Connectors | Central Policy & Management

Leistungsstarke, breit aufgestellte Ransomware-Abwehr

SCHUTZ VOR BEKANNTEN UND UNBEKANNTEN (ZERO-DAY-)BEDROHUNGEN

- Sperren Sie Fernzugriffswege und eliminieren Sie die riskante Verwendung von RDP, VNC und VPNs.
- Verhindern Sie die Ausführung von Ransomware, indem Sie die geringsten Rechte durchsetzen und die Anwendungskontrolle nutzen.
- Blockieren von bösartigem Code, der Ransomware-Nutzdaten an der Quelle überträgt
- Abwehr von Angriffen, die vertrauenswürdige Anwendungen und Makros ausnutzen
- Stoppen Sie eine Infektion in ihrem Verlauf, indem Sie „Lateral Movement“ verhindern
- Verhindern Sie Account-Hijacking durch die Verwaltung aller privilegierten Anmeldedaten

Vielen Dank

Gerne beantworten wir Ihre Fragen:

kontakt@beyondtrust.com

beyondtrust.com