

Herzlich willkommen
zum Live-Webcast

Keine Chance für Angreifer: Privilegierte Zugänge absichern



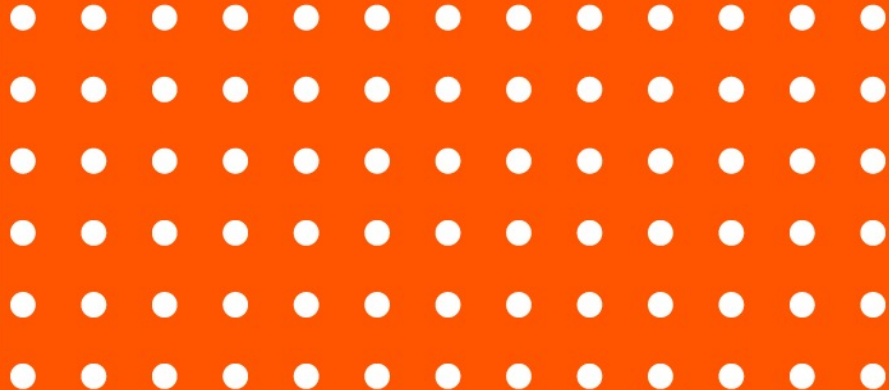
Sprecher: **Vladimir Obradovic**
Solutions Engineer,
BeyondTrust



Moderator: **Martin Seiler**
Heise Business
Services

AGENDA

- Herausforderung privilegierter Zugänge
- Die 7 wichtigsten Privileged-Access-Risiken
- Die Rolle von Privileged Access Management (PAM)





Herausforderung privilegierter Zugänge

Weitreichende Cyberattacken

Hacker attackieren Media Markt Saturn

08.11.2021, 16:43 Uhr | t-online, jnm



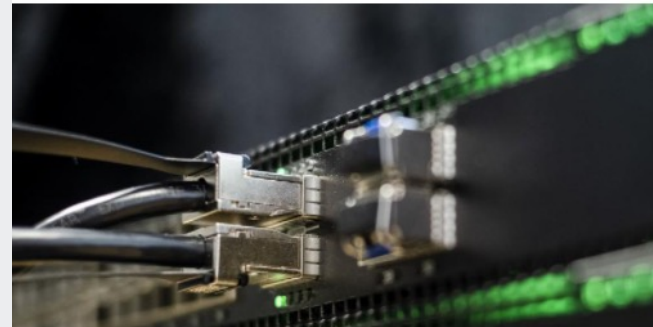
Hacker-Angriff auf Reiseveranstalter FTI: So groß ist der Schaden

Im Oktober hat das Touristikunternehmen FTI öffentlich gemacht, gehackt worden zu sein. Nun bekannte sich die Hacker-Gruppe Conti zu der Cyber-Attacke – und gibt einen Eindruck von dessen Ausmaß.

19.11.2021, 19:30 Uhr • 2 Min. Lesezeit

Erster Cyber-Katastrophenfall in Deutschland – Landkreis Anhalt-Bitterfeld lahmgelegt

Veröffentlicht am 10.07.2021 | Lesedauer: 3 Minuten



Cyber-Angriff auf Uniklinik Düsseldorf: #Shitrix schlug zu

Die Erpresser kamen über eine Sicherheitslücke im VPN-Gateway – wahrscheinlich schon vor Monaten.

Lesezeit: 3 Min. In Pocket speichern

🔊 🖨️ 💬 207



Zehntausende Kundendaten betroffen

Hacker stoßen erneut auf Sicherheitslücken bei Corona-Testzentren

Knapp 174.000 Buchungsbestätigungen und Testergebnisse aus 34 Testzentren von Coronapoint ließen sich ohne großen Aufwand von Unbefugten abrufen. Sie enthielten Namen, Adressen und mitunter auch Ausweisnummern.

23.06.2021, 16.45 Uhr

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



Umfrage



Umfrage

Was schätzen Sie, welcher Anteil der Unternehmen beispielsweise in den USA von betrieblichen Cyberattacken betroffen war?*

☐ 34 %

☐ 57 %

☐ 65 %

☐ 72 %

☐ 94 %


***in 2020**





94% der Unternehmen waren 2020 von Cyberattacken betroffen

The Rise of the Business Aligned Security Executive Report, Tenable, 2020



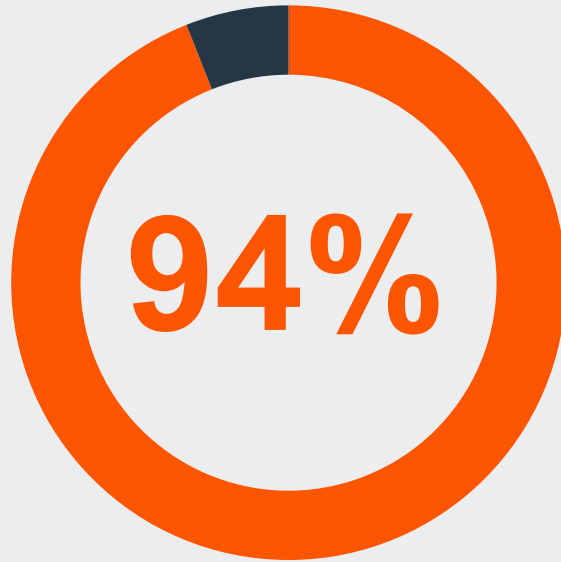


Die 7 wichtigsten Privileged-Access-Risiken

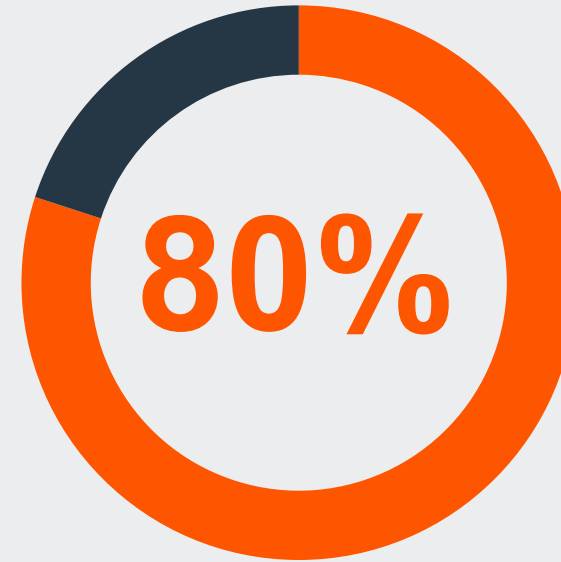


Hohes Tempo der digitalen Transformation

Digitaler Wandel jetzt, Sicherheit erst später...



Anteil der Organisationen mit
aktuellem, digitalen
Transformationsprojekt



Anteil der Cyberangriffe,
die auf gestohlene Anmelde-
daten zurückzuführen sind

Digitaler Wandel mit Sicherheitsrisiken

DIGITALE TRANSFORMATION UND CLOUD-NUTZUNG KÖNNEN HOHE SICHERHEITSRISIKEN SCHAFFEN

- Verlagerung auf Remote-Work-Strukturen und beschleunigte Cloud-Nutzung
- Sicherheitsfragen werden zum Teil vernachlässigt
- Remote-Mitarbeiter sind durch Einsatz eigener Endgeräte (BYOD) anfälliger und verursachen Schatten-IT

Wachstum der IT-Infrastruktur, Perimeter-Veränderungen, komplexeres Privilegien-Management.





Zunahme von Cloud-Anwendungen

*“Die meisten Unternehmen setzen drei oder mehr öffentliche Clouds ein...
das bedeutet ein vielfach höheres Sicherheitsrisiko.”*



Anstieg der Cloud-bezogenen
Cyberangriffe im Jahr 2020



Durchschnittliche Anzahl der von
Unternehmen genutzten Cloud-Dienste



aller Daten sind in der Cloud gespeichert
(oder werden dort verarbeitet).

Mehr potenzielle Zugangswege für Hacker

DER BREITE WECHSEL IN DIE CLOUD GIBT HACKERN MEHR ANGRIFFSOPTIONEN

- Nutzung mehrerer Clouds (PaaS, IaaS)
- Viele Cloud-Plattformen bieten nur grundlegende Kontrollmechanismen für Identity und Access Management (IAM)

Alibaba Cloud



Google Cloud

salesforce



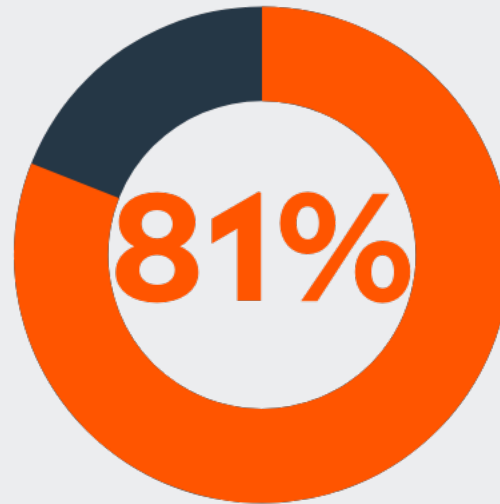


Riskante Passwortpraktiken

“Die unsichere Speicherung von Passwörtern und die fehlende Rotation haben nachweislich zu Phishing-Angriffen und Sicherheitsverletzungen geführt.”



Anzahl der Passwörter, die sich eine Person durchschnittlich merken muss



der Angriffe betreffen entweder gestohlene oder schwache Passwörter.



Konten von Opfern eines Datenlecks verwendeten „123456“ als Passwort.

Verizon Data Breach Investigations Report, 2019
National Cyber Security Centre (NCSC) Survey, 2019

Abruf (und Aktualisierung) komplexer Passwörter

DIE STÄNDIGE NEUERSTELLUNG VON KOMPLEXEN PASSWÖRTERN KANN MITARBEITER ÜBERFORDERN

- Phishing-Attacken und Sicherheitsverletzungen durch unsichere Passwortspeicherung und fehlende Rotation
- Überforderung der Mitarbeiter im Geschäftsalltag führt zur unsicheren Speicherung von Passwörtern oder zur Nutzung gleicher Kennwörter
- Schwache Passwörter erleichtern das Eindringen in Netzwerke und erhöhen dadurch die Ransomware-Gefahr erheblich

**Einige der häufigsten
Passwörter
im Jahr 2020...**

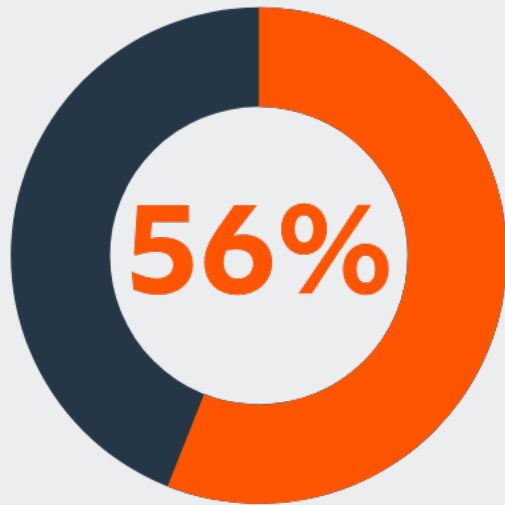
**...und Hacker
knacken sie in
Sekunden!**



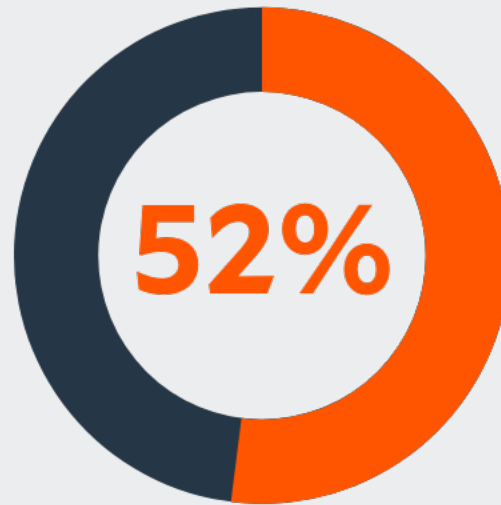


Zu weit gefasste Adminrechte

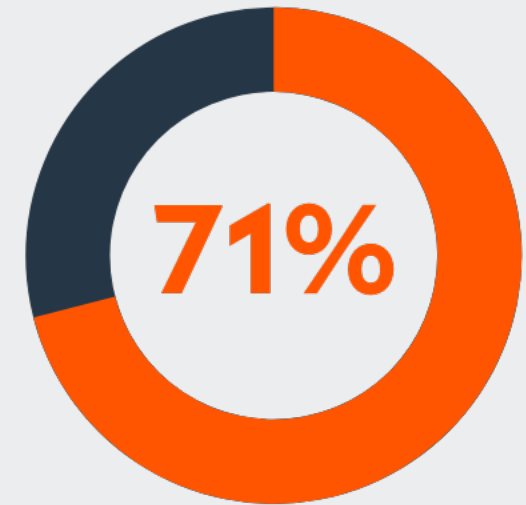
*“Administratorrechte sind die Schlüssel zu Ihrem Königreich.
Erhält diese jeder in Ihrem Unternehmen, vergrößert sich Ihre Angriffsfläche.”*



der kritischen Microsoft-Schwachstellen im Jahr 2020 hätten durch die Entfernung von Admin-rechten verhindert werden können.



der Unternehmen erwarten, dass privilegierte Nutzersitzungen in den nächsten zwei Jahren erheblich zunehmen werden.



glauben, dass ihr Unternehmen die Least Privilege-Protokolle auf Endgeräten und Servern verbessern könnte.

Mehr Adminrechte. Größere Angriffsfläche.

ZU WEIT GEFASSTE NUTZERPRIVILEGIEN FÜHREN ZU (UNNÖTIGEN) RISIKEN

- Riskante Vergabe vollständiger Zugriffsprivilegien
- Verschaffen sich Hacker mithilfe uneingeschränkter Adminrechte die Kontrolle, können sie weitere Angriffe per Network Lateral Movement starten und deutlich höhere Schäden verursachen
- Mehr Nutzer mit Adminrechten = größere Angriffsfläche



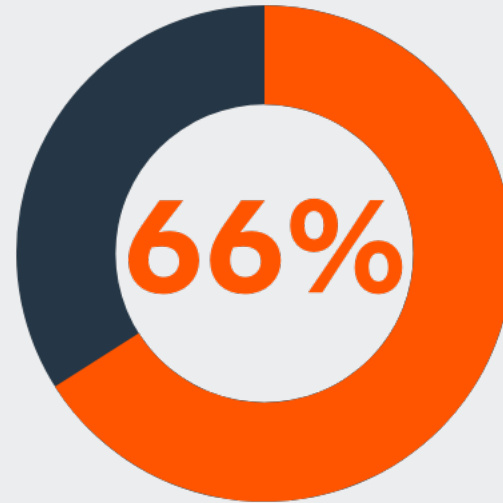


Interne Nutzer als Schwachstelle

“Cyber-Angriffe werden oft durch unzureichende Cybersicherheitsmaßnahmen bei Drittanbietern oder durch die Nachlässigkeit der Mitarbeiter verursacht. Oft ist das Ziel, dem Unternehmen finanziellen Schaden oder Rufschädigung zuzufügen.”



Verlust von Cisco, um Schäden zu beheben, die durch den unbefugten Zugang eines ehemaligen Mitarbeiters entstanden sind



der Unternehmen weltweit halten Insider-Angriffe oder versehentliche Verstöße für wahrscheinlicher als Angriffe von außen.



Durchschnittliche Gesamtkosten von Insider-Vorfällen im Jahr 2020

Interne Nutzer als Schwachstelle

HAUPTSÄCHLICH WERDEN CYBERANGRIFFE VON INNEN HERAUS DURCHGEFÜHRT

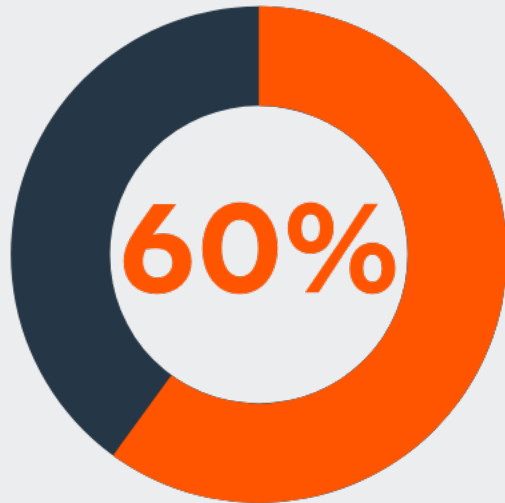
- „Interne Angreifer“ zählen zu den Hauptursachen von Cyberattacken
- Angreifer mit Insider-Wissen können aktuelle oder ehemalige Angestellte sein, die Sicherheitsinformationen einer Organisation besitzen
- Diebstahl oder Löschung wichtiger Daten sowie die Weitergabe von Informationen an Wettbewerber



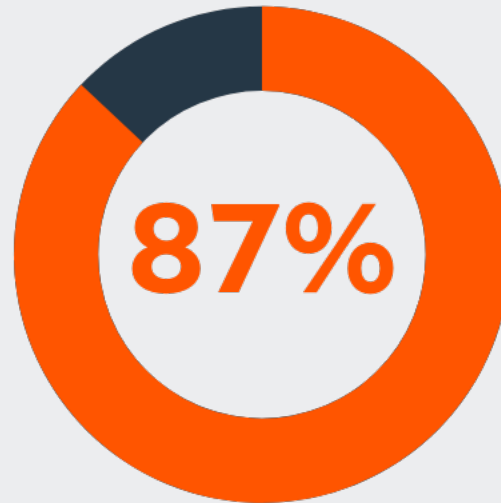


Selbstüberschätzung

“Selbst die sorgfältigsten Mitarbeiter könnten auf einen realistischen Phishing-Betrug per E-Mail oder über soziale Medien hereinfallen.”



der Unternehmen haben im Jahr 2020 Daten durch einen Phishing-Angriff verloren.



Anstieg der Phishing-Angriffe auf Finanzmitarbeiter im Jahr 2020



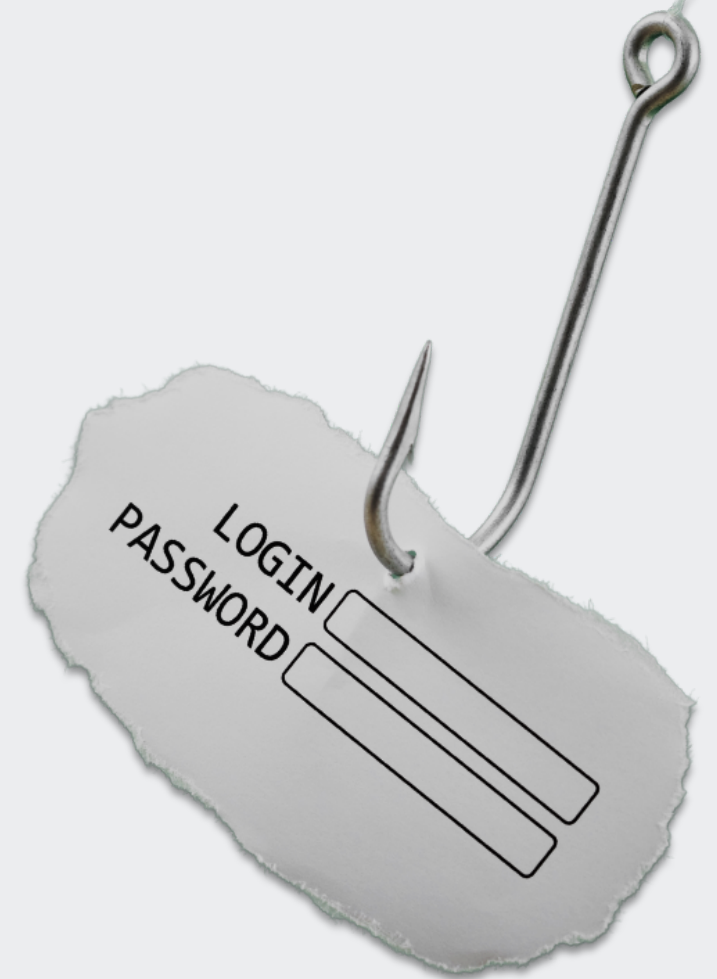
vom FBI gemeldete Phishing-Vorfälle in den USA im Jahr 2020.

2021 State of Phishing Report, Proofpoint,
Abnormal Quarterly BEC Report Q2, FBI Internet Crime Report 2020

Unsere Mitarbeiter sind immer vorsichtig!

DAS BEWUSSTSEIN FÜR CYBERSICHERHEIT IST WICHTIG, REICHT ABER NICHT

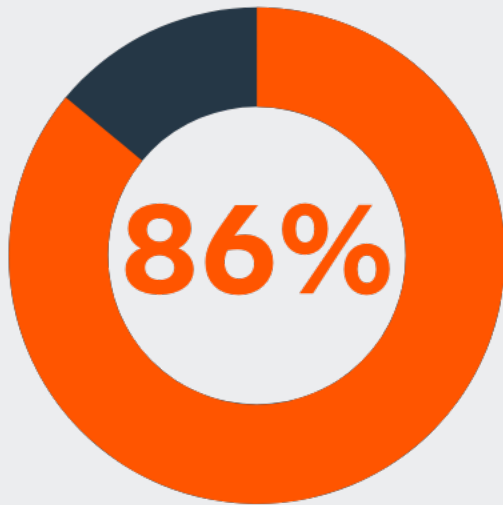
- Phishing-Attacken sind häufigstes Cybersicherheitsrisiko mit Mitarbeitern als Zielpersonen
- Bei ausgefeilten Deepfake-Angriffsmethoden können auch gut geschulte Anwender anfällig sein
- Nicht vergessen: Ein Fehler genügt für einen gravierenden Sicherheitsverstoß!



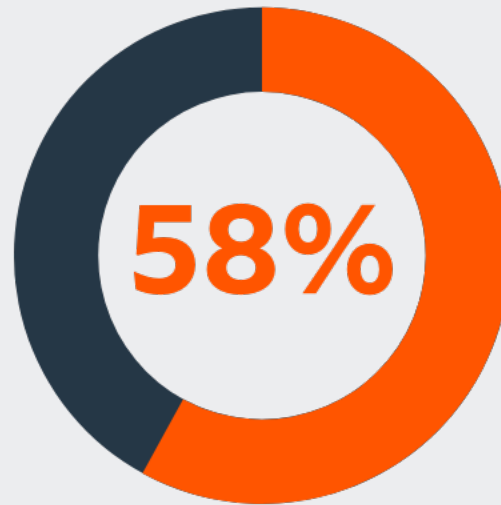


Unterbesetzte IT-Servicedesks

“Die Anforderungen, die durch die Pandemie und die massive Verlagerung zum mobilen Arbeiten entstanden sind, haben die Last auf IT-Teams erhöht.”



der Servicedesk-Teams geben an, dass der Einsatz einer Remote Support-Lösung ihre Produktivität erhöht.



der Unternehmen halten es für wahrscheinlich, dass sie aufgrund von Drittanbieter-Zugriffen einen Sicherheitsverstoß erlitten haben.



benötigt der interne Support durchschnittlich für eine erste Antwort auf eine interne Supportanfrage.

Mehr Ressourcen für IT-Servicedesks

MIT DEM WACHSTUM ANDERER ABTEILUNGEN KOMMT AUCH DAS IT-TEAM UNTER DRUCK

- IT-Servicedesks sind oft unterfinanzierte Geschäftsbereiche
- Anfragen beim IT-Servicedesk nehmen durch internes Wachstum zu
- Wandel hin zu Homeoffice-Strukturen führt zu erhöhtem Bedarf an Remote-Zugriffen
- Auch die Einbeziehung externer Dienstleister fällt in den Aufgabenbereich des IT-Servicedesks





Die Rolle von Privileged Access Management (PAM)

Risikominimierung mit Privileged Access Management (PAM)

- Eine effektive PAM-Strategie unterstützt Organisationen beim **Schutz häufiger Angriffspunkte**.
- Im Unterschied zu herkömmlichen PAM-Ansätzen erlaubt der **Universal Privilege Management-Ansatz von BeyondTrust**, dass alle Aspekte beim privilegierten Zugriff abgesichert werden.
- Das PAM-Produktportfolio von BeyondTrust ist eine **integrierte Gesamtlösung** für mehr Visibilität und Kontrolle über alle Konten- und Nutzerprivilegien.



Umfrage



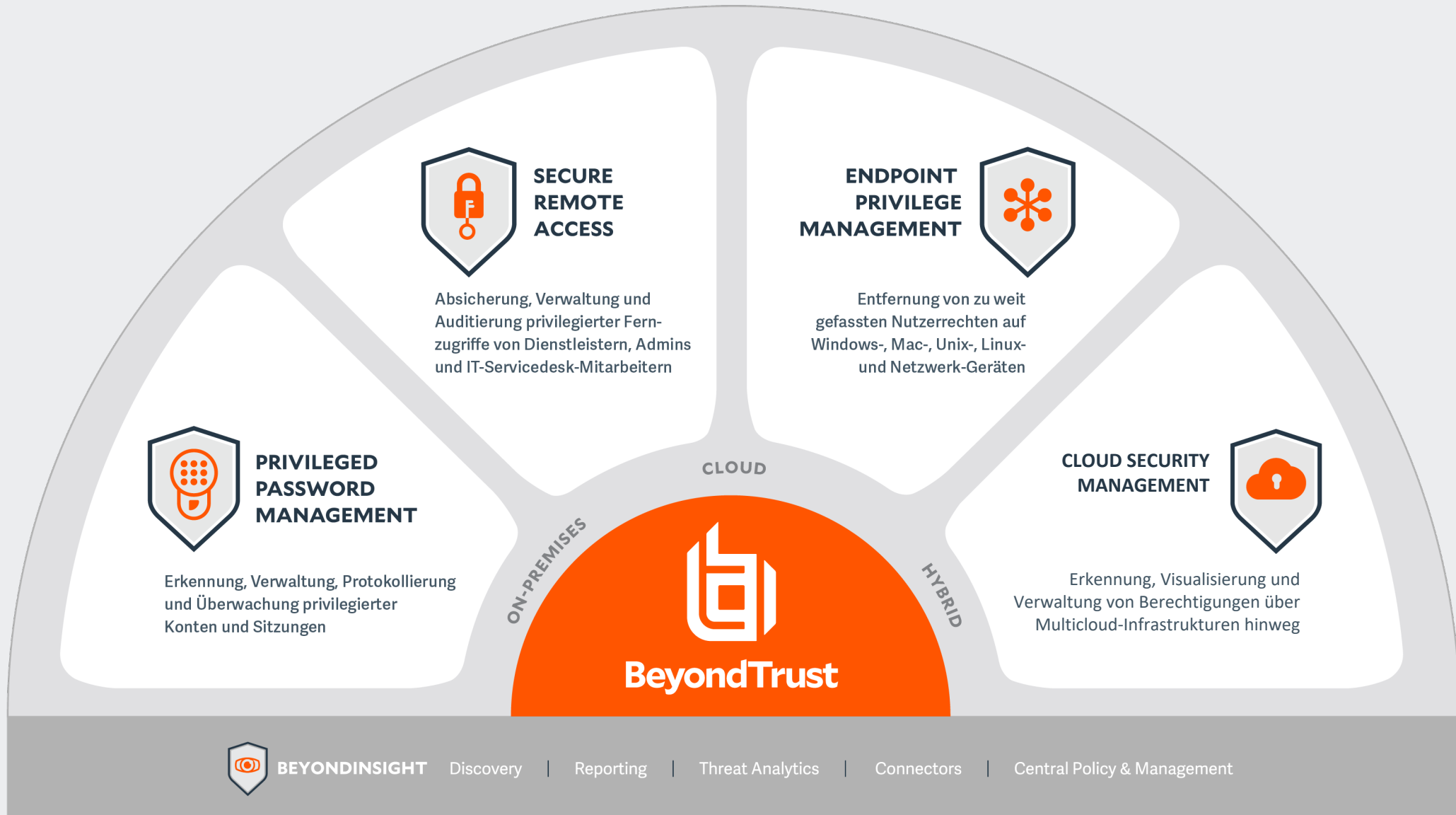
Umfrage

Welcher dieser Bereiche ist für Ihre IT-Sicherheitsstrategie am kritischsten?

1. Unternehmensweite Durchsetzung einer starken Passwortrichtlinie
2. Multi-Faktor Authentifizierung
3. Entfernung von lokalen Adminrechten (Least Privilege)
4. Application Whitelisting
5. Absicherung von externen Zugriffen

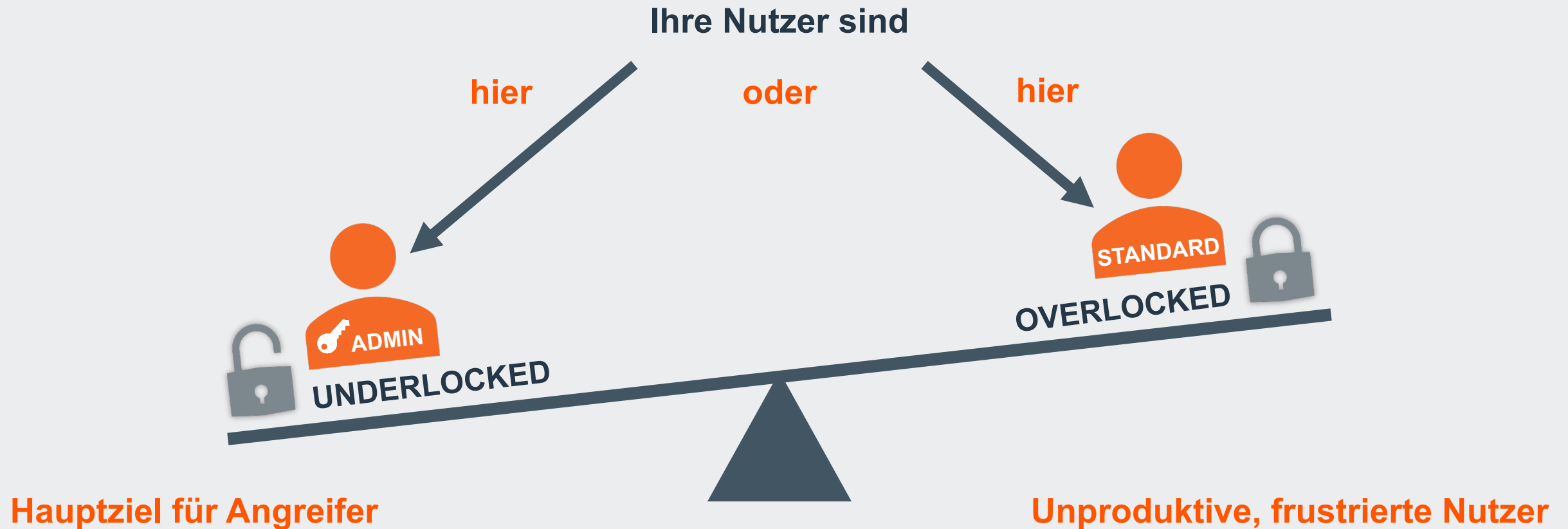


The BeyondTrust Solution



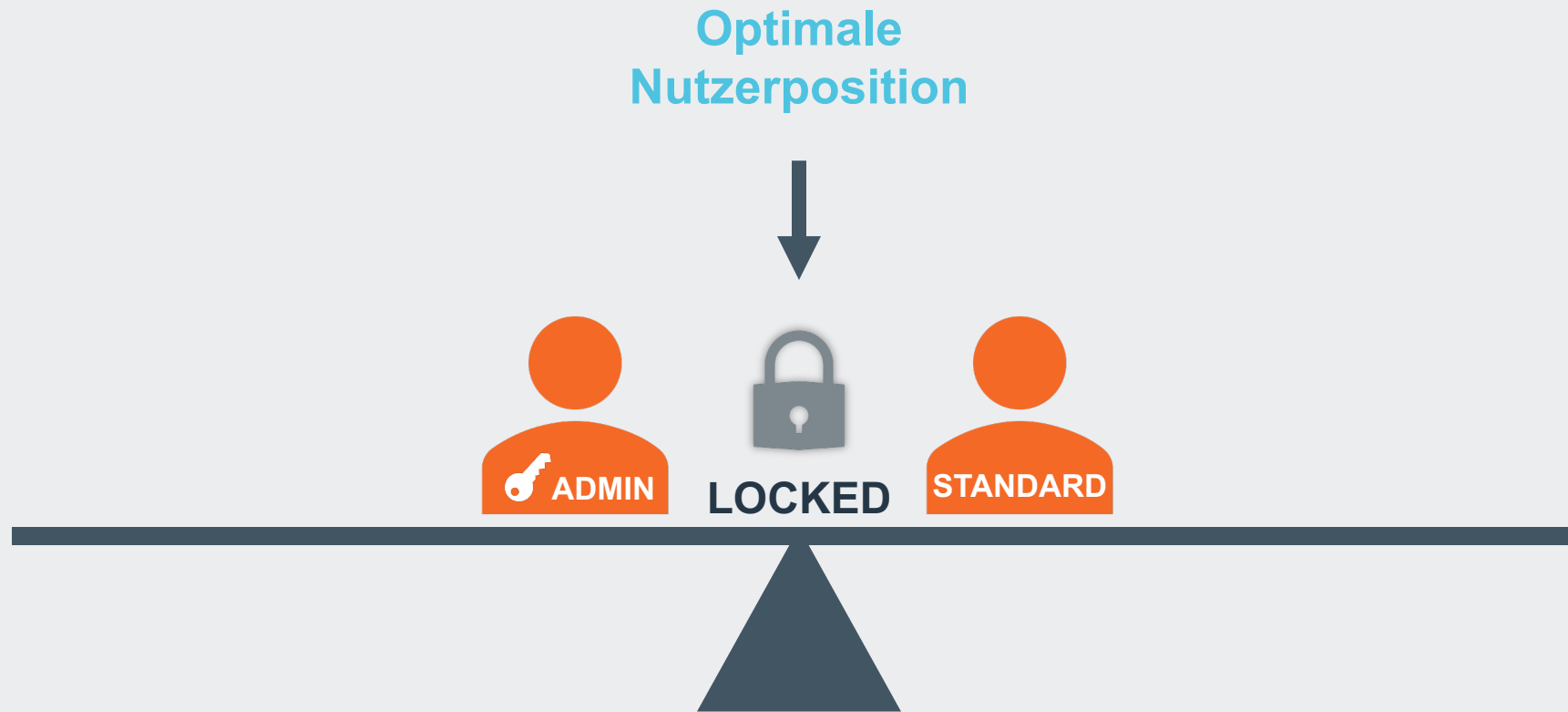
Gleichgewicht zwischen Sicherheit und Produktivität

DER UNMÖGLICHE KOMPROMISS?



Gleichgewicht zwischen Sicherheit und Produktivität

DER UNMÖGLICHE KOMPROMISS?



Abgesicherte und produktive Nutzer

Demo / Kostenlose Testversion

Secure Remote Access Lösung:
www.beyondtrust.com/secure-remote-access





VIELEN DANK



Bitte kontaktieren Sie uns, falls Sie weitere Fragen haben:
kontakt@beyondtrust.com