AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Was ist PAM mit Zero Standing Privileges (ZSP)?

Jessica Warland
Security Engineer
AVANTEC AG

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Was ist PAM mit Zero Standing Privileges (ZSP)?

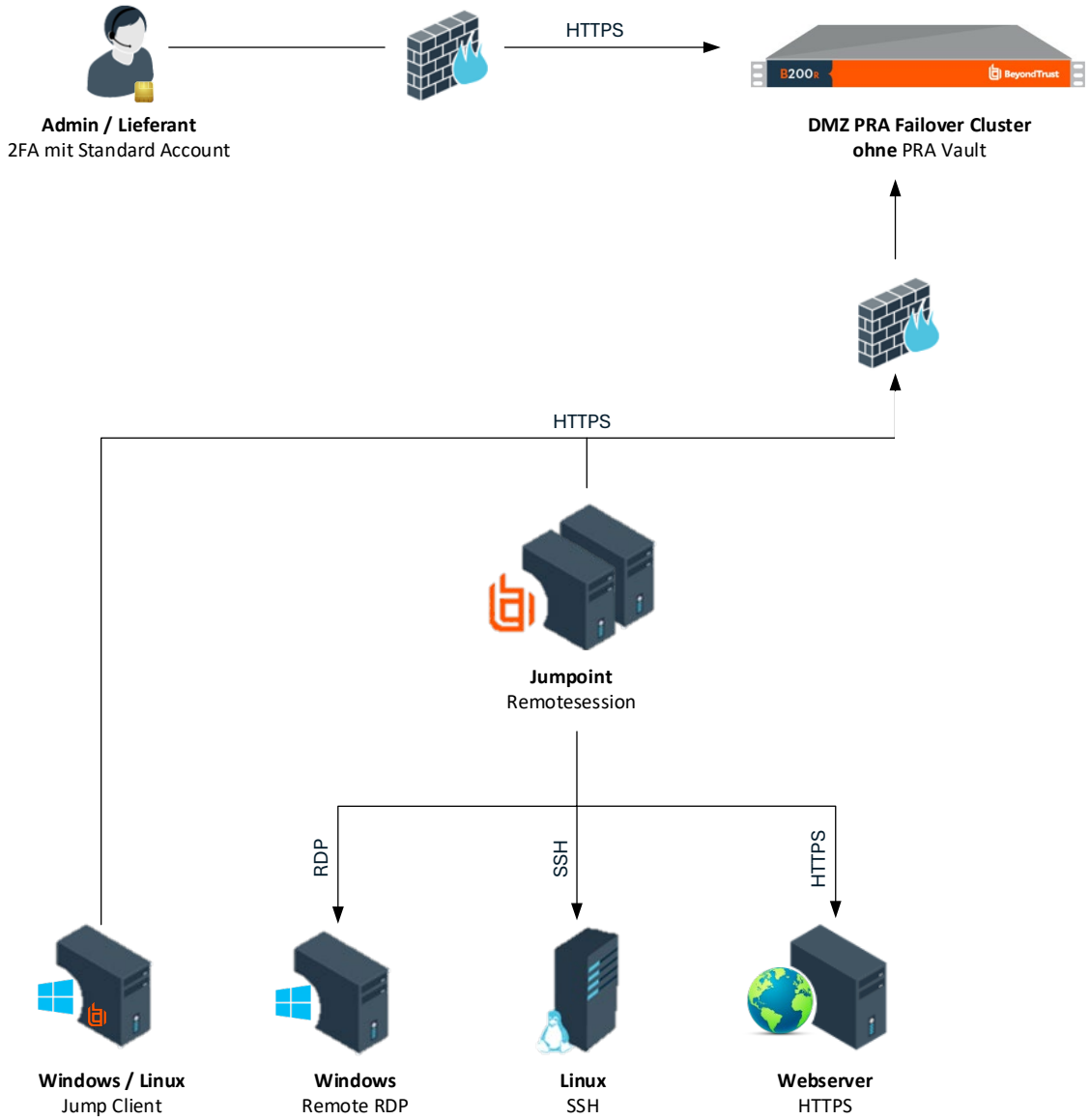
Michael Scherzinger
Senior Security Engineer | PAM Product Manager
AVANTEC AG

Agenda

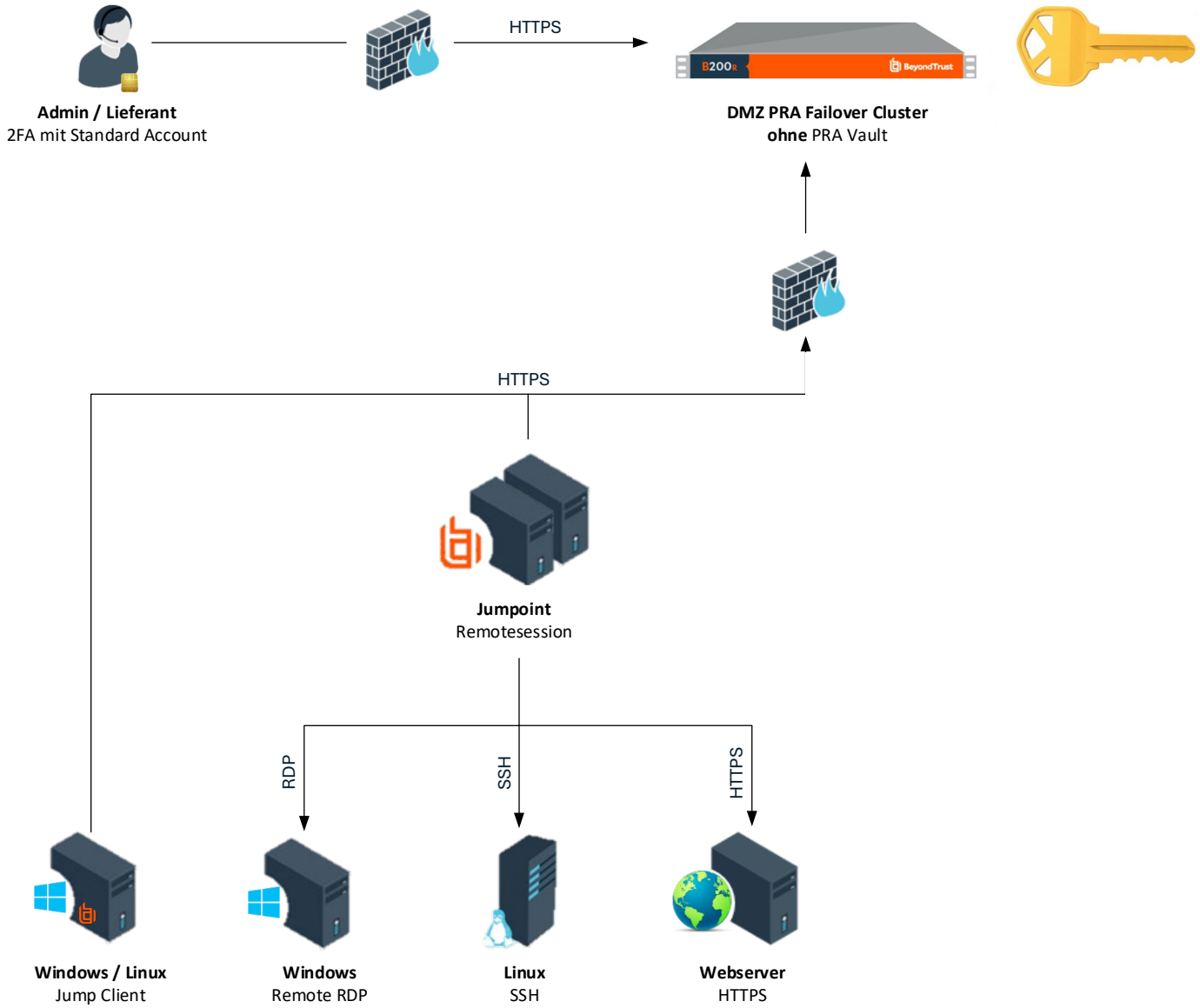
AVANTEC
Competence. Security. Trust.

- Was ist PAM?
- Warum brauchen wir PAM mit ZSP (Zero Standing Privilege)?
- Problem der Umsetzung
- Lösungsansatz
- So funktioniert Entitle
- Unser Lösungsansatz
- Architektur
- Live Demo
- Q&A

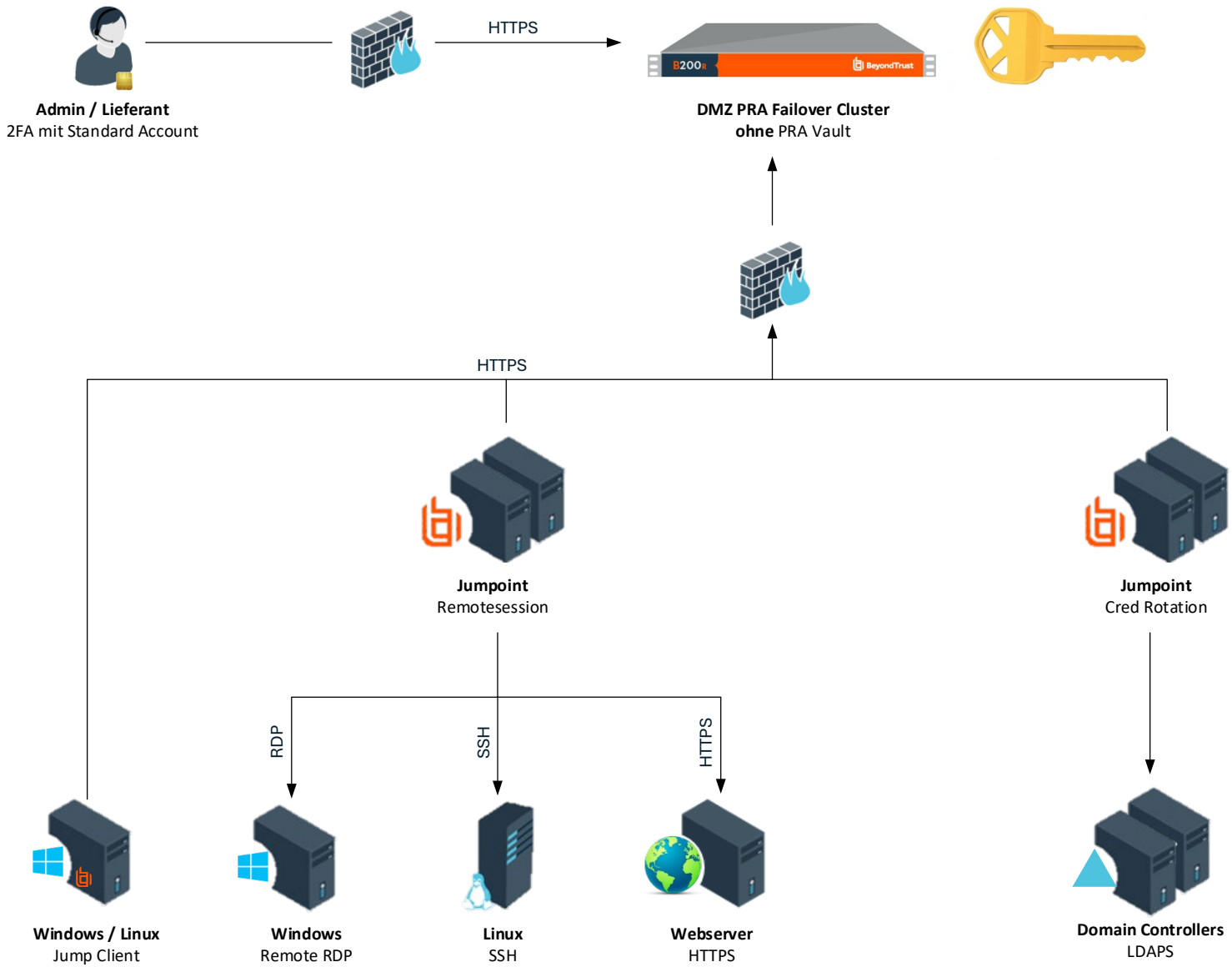
PAM Konzept


HTTPS
B200
BeyondTrust
Admin / Lieferant
2FA mit Standard Account
DMZ PRA Failover Cluster
ohne PRA Vault
HTTPS
Jumpoint
Remotesession
RDP
SSH
HTTPS
Windows / Linux
Jump Client
Windows
Remote RDP
Linux
SSH
Webserver
HTTPS

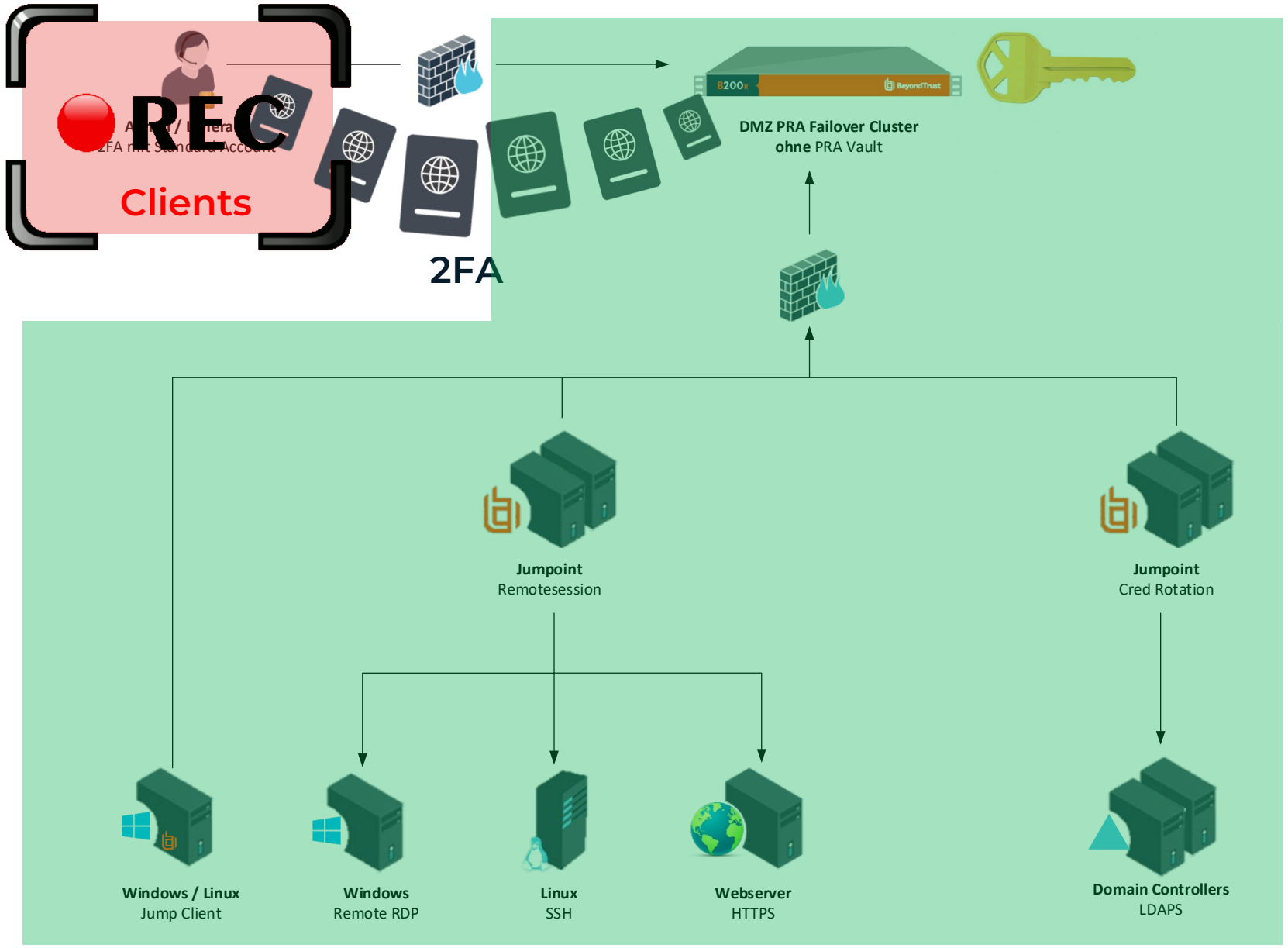
PAM Konzept


HTTPS
B200
BeyondTrust
Admin / Lieferant
2FA mit Standard Account
DMZ PRA Failover Cluster
ohne PRA Vault
HTTPS
Jumpoint
Remotesession
RDP
SSH
HTTPS
Windows / Linux
Jump Client
Windows
Remote RDP
Linux
SSH
Webserver
HTTPS

PAM Konzept


HTTPS
Admin / Lieferant
2FA mit Standard Account
DMZ PRA Failover Cluster
ohne PRA Vault
HTTPS
Jumpoint
Remotesession
Jumpoint
Cred Rotation
RDP
SSH
HTTPS
Windows / Linux
Jump Client
Windows
Remote RDP
Linux
SSH
Webserver
HTTPS
Domain Controllers
LDAPS

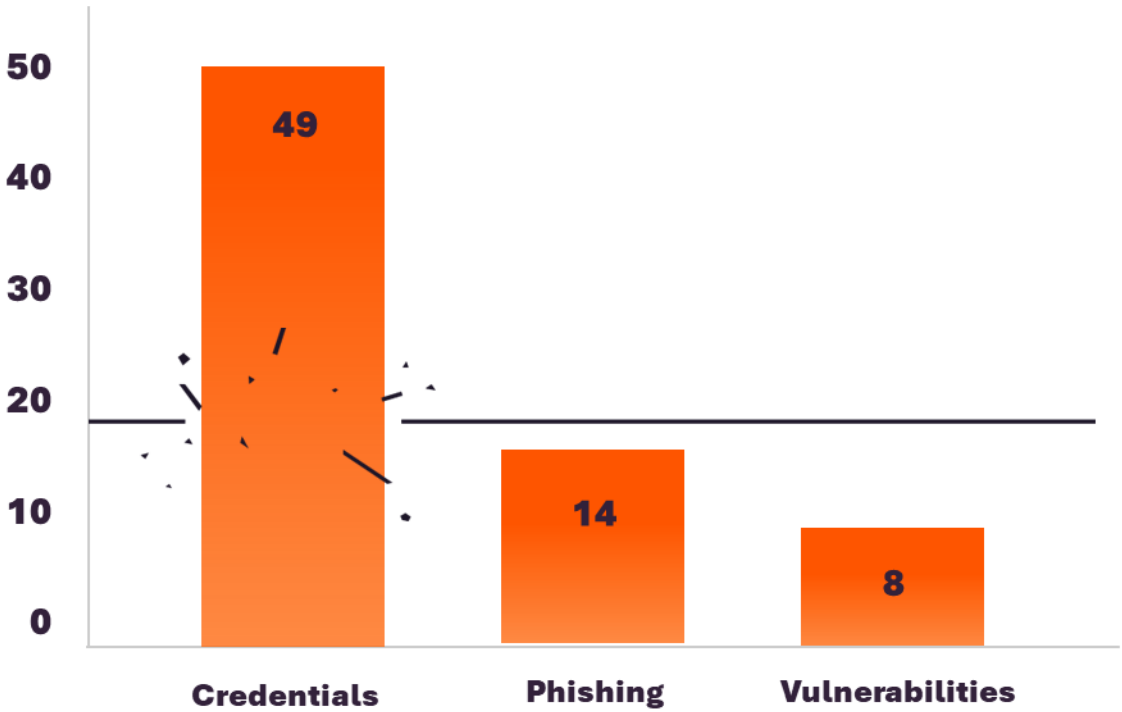
Ziele von PAM



- Auf dem Client keine administrative Credentials
- 2FA
- Nachvollziehbarkeit
- Admin Passwörter von PAM verwaltet

1 von 2 Angriffen beinhaltet die unbefugte Nutzung von Identitäten

AVANTEC
Competence. Security. Trust.



Verizon Data Breach Investigations Report (DBIR) 2023

The New York Times

Uber Investigating Breach of Its Computer Systems

The company said on Thursday that it was looking into the scope of the apparent hack.

TechCrunch

Security

Okta says hundreds of companies impacted by security breach

Microsoft

Switzerland ranks ninth in Europe for cyberattack frequency

1 von 2 Angriffen beinhaltet die unbefugte Nutzung von Identitäten

Und dennoch werden 99 % der aktiven Berechtigungen nicht genutzt.

*State of Cloud Permission Risks

The New York Times

Uber Investigating Breach of Its Computer Systems

...at it was looking into the scope

...f companies
...breach

Microsoft

Switzerland ranks ninth in Europe for cyberattack frequency

AVANTEC
Competence. Security. Trust.

Zero Standing Privileges

Reduktion der Angriffsfläche – sichtbar gemacht

50

verwaltete Server

≤ 2

Server gleichzeitig aktiv

8 h

max. Tagesnutzung pro Admin

Zugriffsmuster pro Server pro Woche

Jede Zelle = 15 Min

Server #01 — Auswertung

- Aktiver Zugriff
- Privileg ungenutzt

168 h

Privileg verfügbar (24/7 die ganze Woche)

≈ 5,5 h

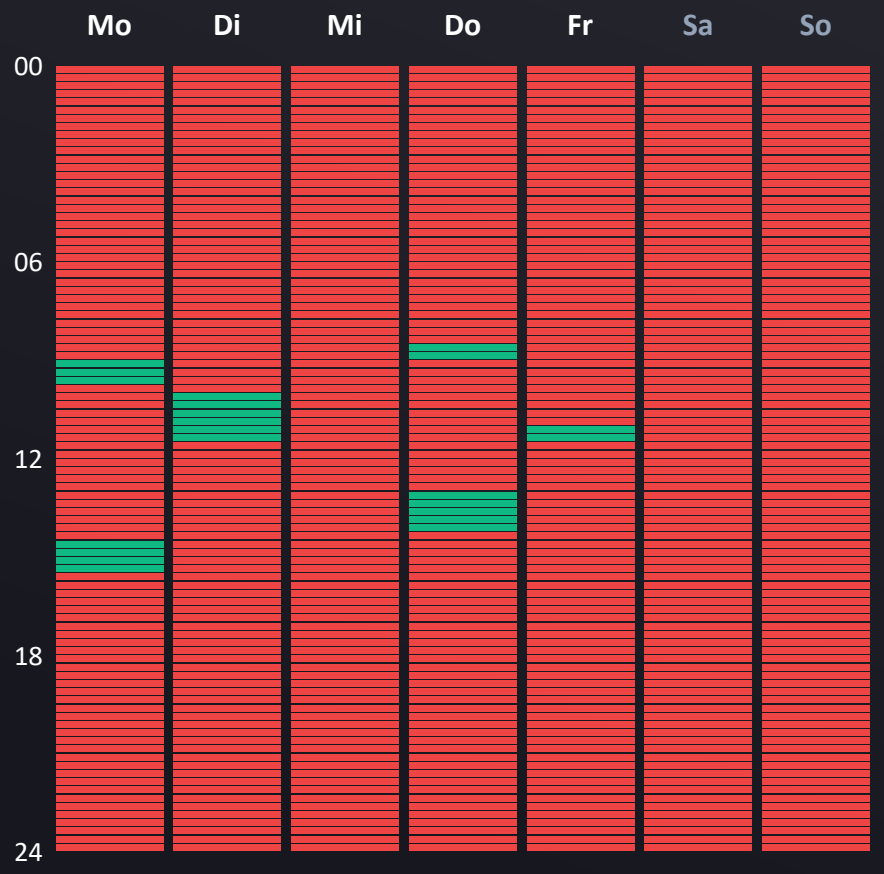
tatsächlicher Zugriff

Standing vs. Zero Standing Privileges

Beispielmodell für einen Server

Standing Privileges

Admin hat 24/7 Zugriff = 24/7 Risiko



168 h Risiko-Exposition / Woche

Zero Standing Privileges

Admin erhält Zugriff nur bei Bedarf – sonst Null

≈ 5,5 h nur reale Zugriffe

- Aktiver Zugriff
- Unnötige Angriffsfläche
- Geschützt durch ZSP (Keine Berechtigung vorhanden)

Hochgerechnet auf alle 50 Server

Missbrauchspotenzial pro Adminaccount

Ohne ZSP: 8'320 Stunden Angriffsfenster — pro Woche pro Admin

50 Server gesamt, pro Woche

8'400 h
Privileg verfügbar (50 × 168 h)

≈ 80 h
tatsächlicher Zugriff (Summe)

8'320 h
Missbrauchsfenster pro Woche

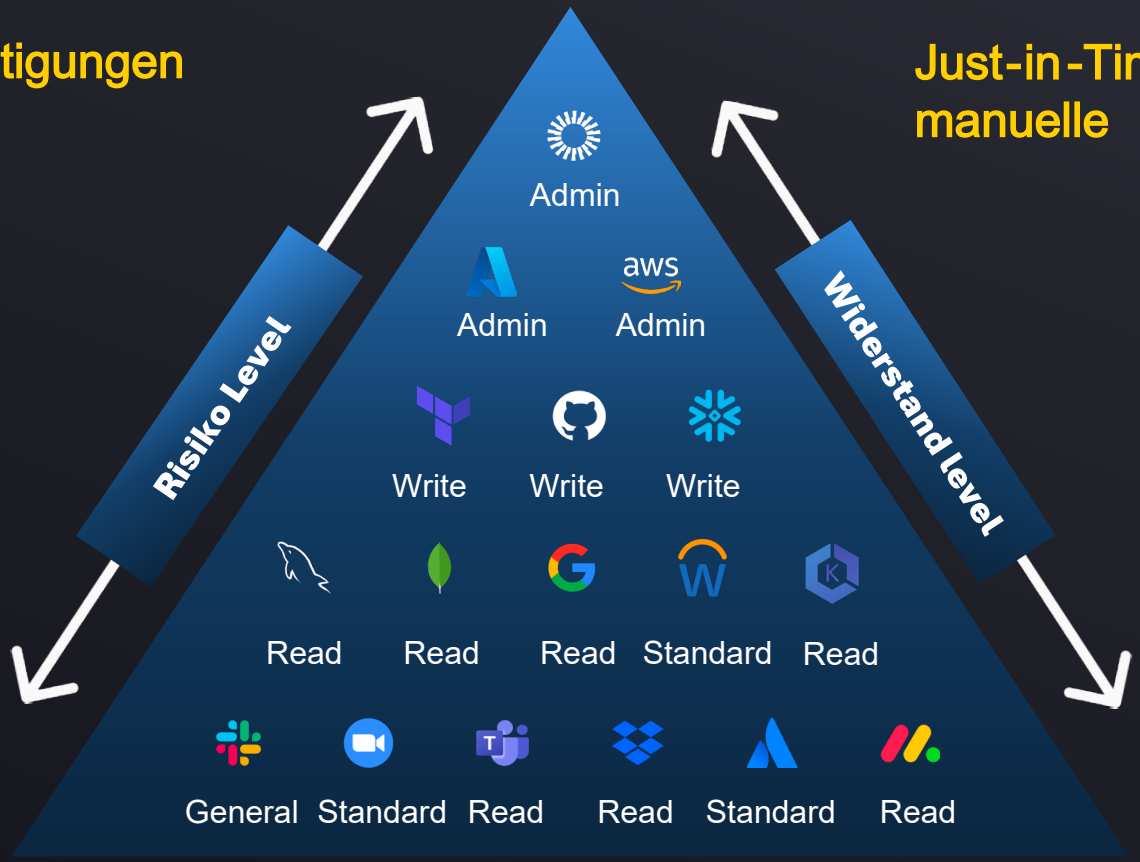
99 %
der Zeit unnötig privilegiert

Zugriffskontrollen je nach Risiko lockern oder verschärfen

AVANTEC
Competence. Security. Trust.

Privilegierte Berechtigungen
Sensible Daten

Just-in-Time-Zugriff und
manuelle Genehmigungen



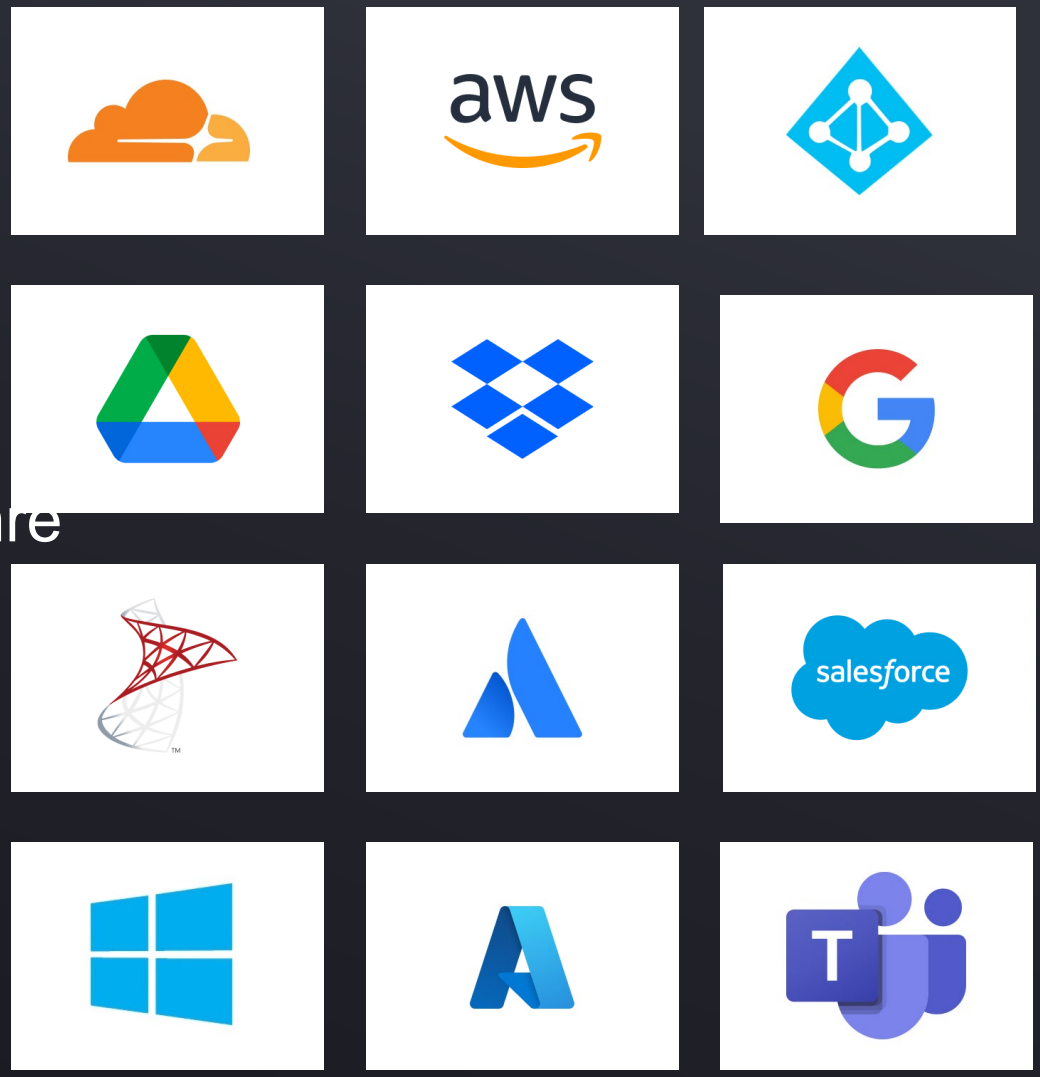
Allgemeine
Berechtigungen
Allgemeine Daten

Unbefristeter Zugriff und
automatische
Genehmigungen

Just-in-Time-Zugriffsverwaltungs-plattform

Stellen Sie automatisch essenzielle, zeitlich begrenzte und granulare Berechtigungen für Ihre Cloud-SaaS- und On-Premise-Infrastruktur bereit.

Gebrauchsfertige Integrationen mit Dutzenden von Systemen
entitle.io/integrations



So funktioniert es mit Entitle

Plattform für Just -in-Time-Zugriffsverwaltung

AVANTEC
Competence. Security. Trust.

Datenquellen

IdP

HRIS

On Call Mgmt

Selbsbediente Zugriffanfrage

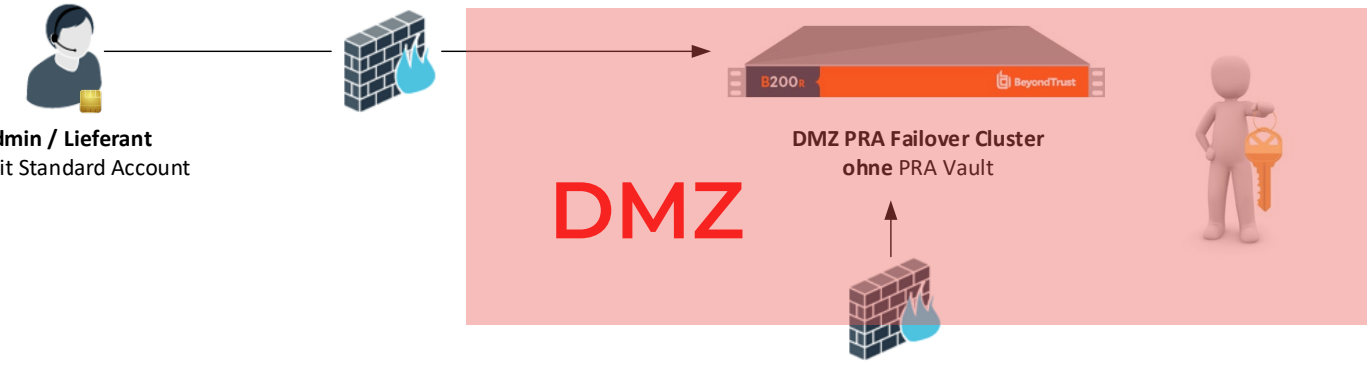
No-Code-Richtlinien -Engine

Zero-Touch-Bereitstellung

Governance -Zugriffsüberprüfung

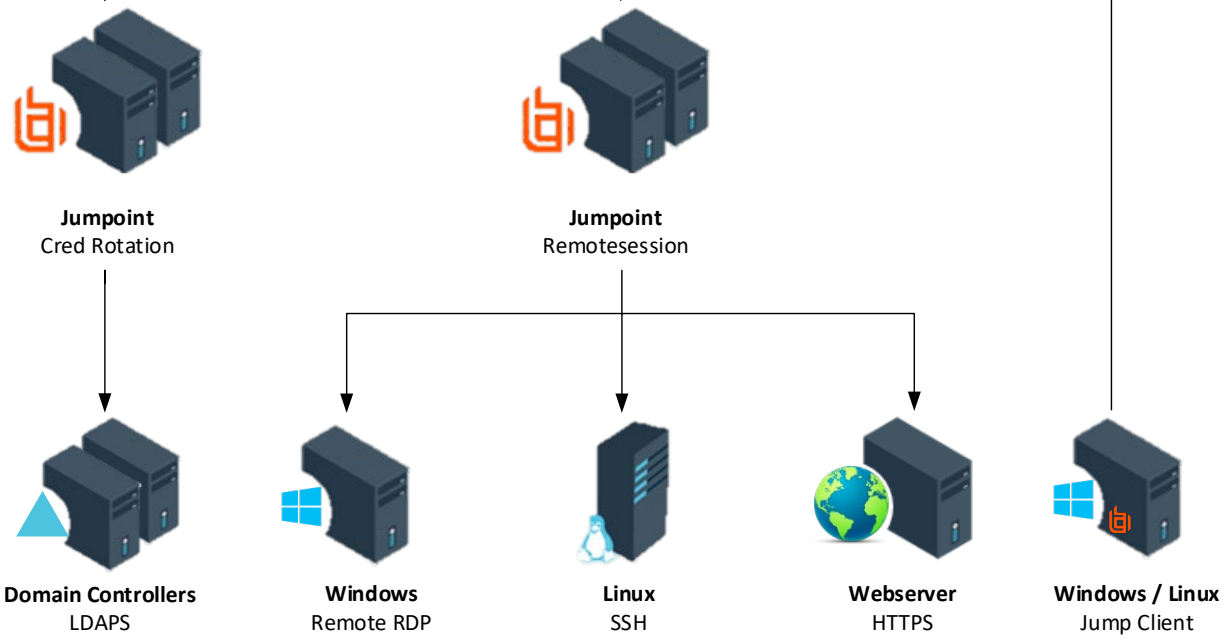
Änderungen werden protokolliert und stehen für Zugriffsüberprüfungen und Compliance-Berichte bereit.

ARCHITEKTUR



AVANTEC
Competence. Security. Trust.

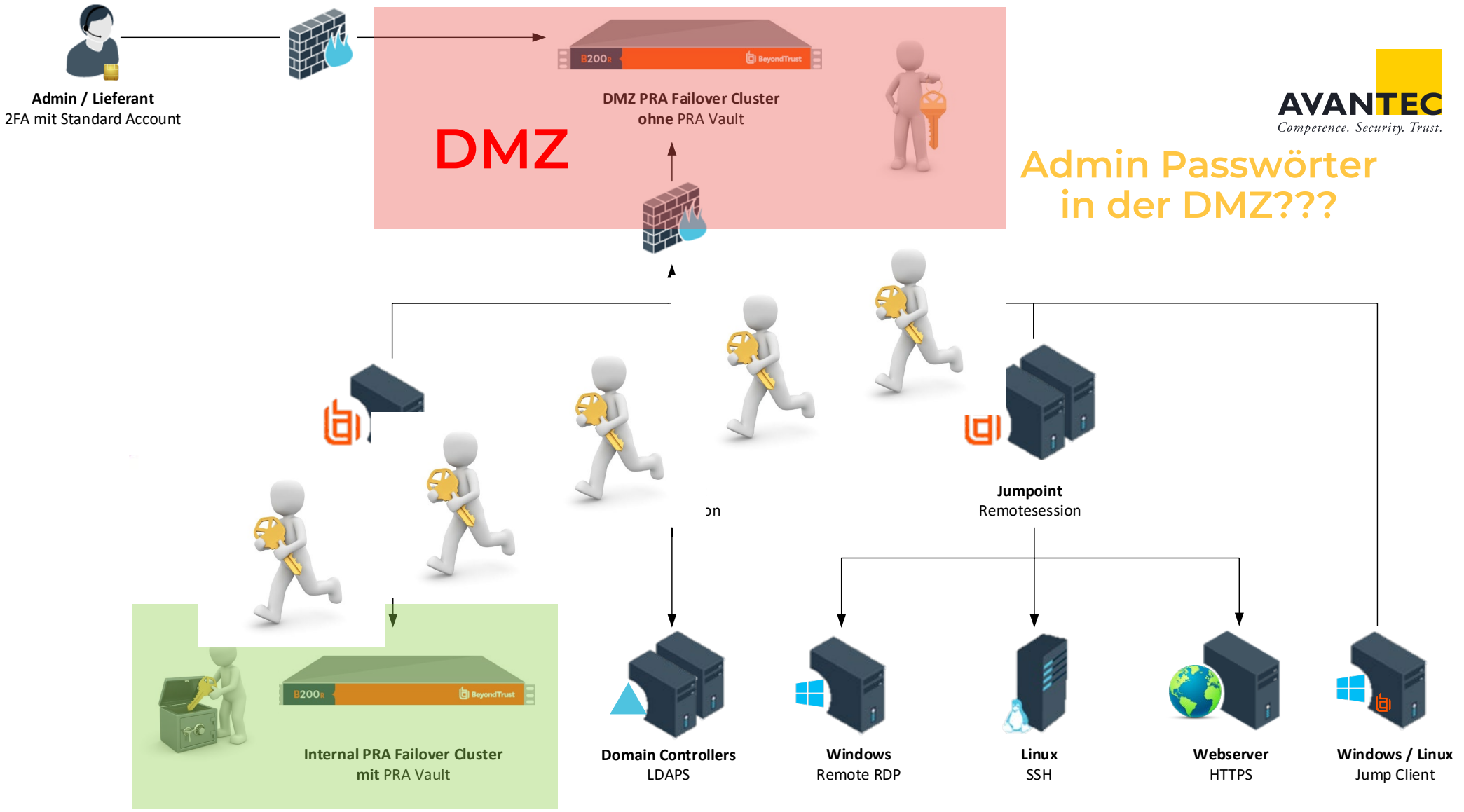
Admin Passwörter in der DMZ???



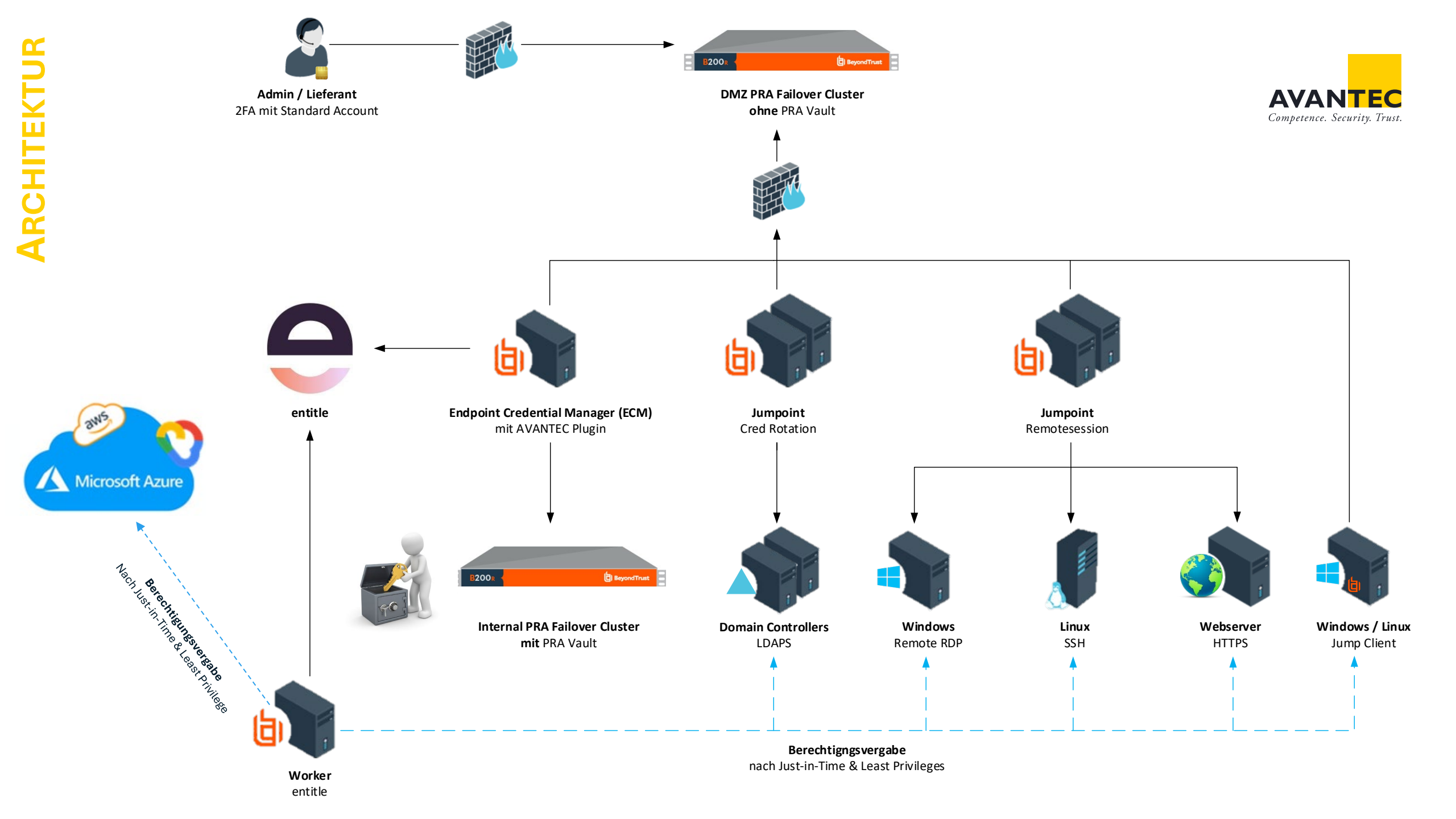
ARCHITEKTUR

AVANTEC
Competence. Security. Trust.

Admin Passwörter in der DMZ???



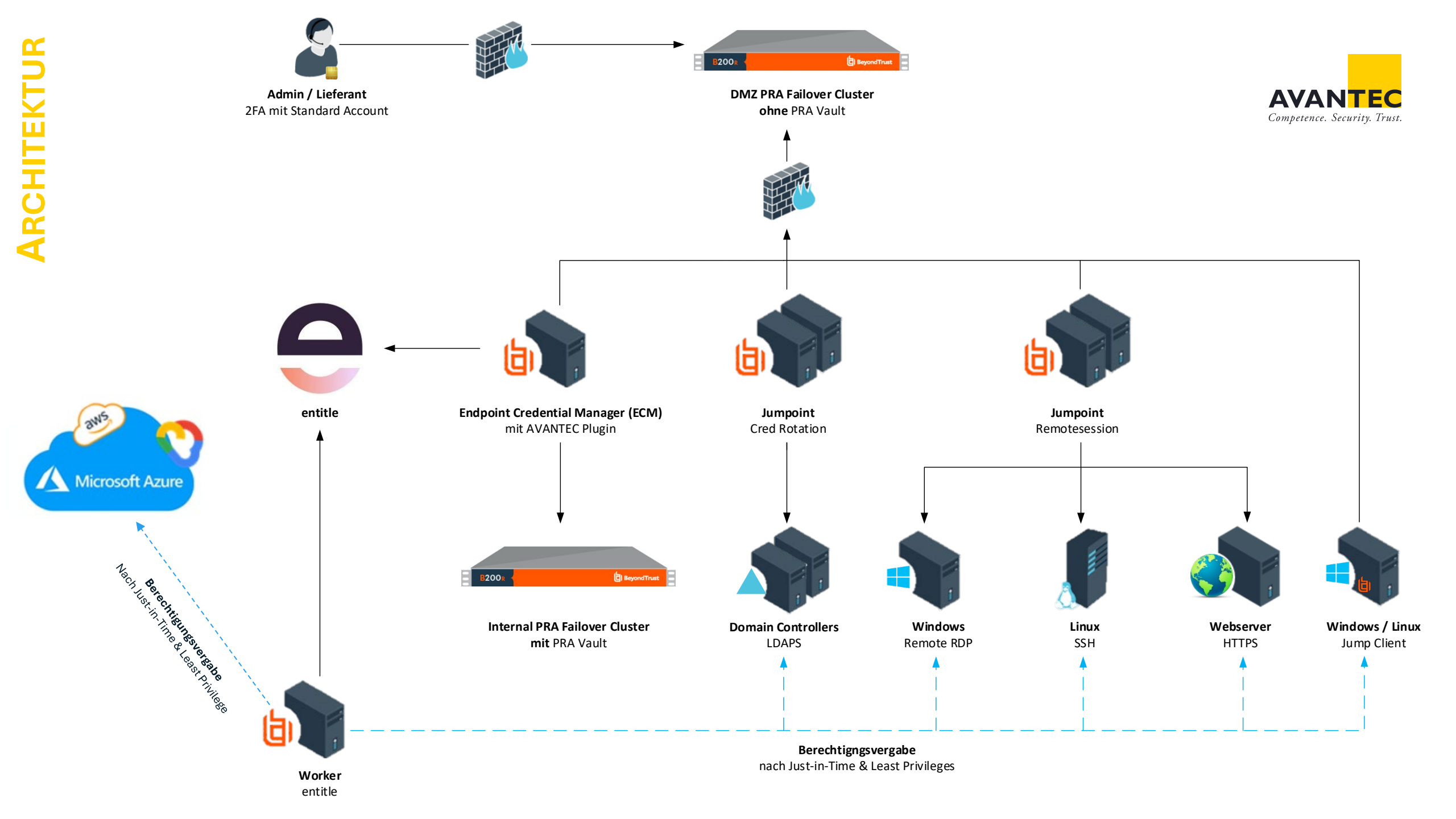
ARCHITEKTUR




AVANTEC
Competence. Security. Trust.
LIVE DEMO


AVANTEC
Competence. Security. Trust.
Q&A

ARCHITEKTUR



AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

DANKE

BeyondTrust · CHECK POINT · CROWDSTRIKE · digicert · netskope · THALES · tenable · xorlab · zscaler

AVANTEC
Competence. Security. Trust.

Nächste Session 14:45

Session 3

Zero Trust Branch (ZTB) mit Airgap – wozu ist das gut? — **Holdener, 5. OG**
Produkt: zscaler
Referenten: René von Arx, Raffael Späni

Thread Huntig Deep Dive: Von Hypothese zu Detection Engineering — **Frei, 4. OG**
Produkt: CROWDSTRIKE
Referent: Alessandro Salucci

Disaster Recovery im Cloud-Zeitalter — **Lehmann Steingruber, 5. OG**
Produkte: zscaler netskope
Referent: Matthias Geiser

Authentication – passwordless, strong, secure — **Odermatt, 4. OG**
Produkt: THALES
Referent: Dirk Gluch

Zscaler Automatisierung — **Cancellara, 4. OG**
Produkt: zscaler
Referent: Christian Schnittert