



# VPN-Wars: ZeroTrust schlägt zurück!

**Fabian Sander**

SASE Expert [fabian.sander@hpe.com](mailto:fabian.sander@hpe.com)

Telonic 27. März 2025

# Bekannte VPN Schwachstellen Stand März 2025

Quelle: ChatGPT

<u>Hersteller</u>	<u>CVE-Nummer</u>	<u>Beschreibung</u>	<u>Datum</u>
Palo Alto Networks	CVE-2025-0108	Authentifizierungs-Bypass in PAN-OS, der es Angreifern ermöglicht, Administratorzugriff ohne Benutzerinteraktion zu erlangen.	18. Februar 2025
SonicWall	CVE-2024-53704	Authentifizierungs-Bypass im SSL VPN, der es entfernten Angreifern ermöglicht, aktive SSL VPN-Sitzungen zu übernehmen und unbefugten Netzwerkzugriff zu erhalten.	7. Januar 2025
Ivanti	CVE-2025-0282	Kritische Schwachstelle im Connect Secure Appliance, die es nicht authentifizierten Angreifern ermöglicht, Remote-Code-Ausführung durchzuführen.	8. Januar 2025
Ivanti	CVE-2025-0283	Schwachstelle im Connect Secure Appliance, die es lokal authentifizierten Angreifern ermöglicht, ihre Privilegien zu eskalieren.	8. Januar 2025
Fortinet	CVE-2024-55591	Autorisierungs-Bypass in FortiOS, der es Angreifern ermöglicht, ohne entsprechende Berechtigungen auf Systeme zuzugreifen.	15. Januar 2025
Palo Alto Networks	CVE-2024-0012	Authentifizierungs-Bypass in der Management-Webschnittstelle von PAN-OS, der es Angreifern ermöglicht, Administratorzugriff ohne Benutzerinteraktion zu erlangen.	8. November 2024
Palo Alto Networks	CVE-2024-9474	OS-Befehlsinjektion in der Management-Webschnittstelle von PAN-OS, die zur Privilegieneskalation führen kann.	18. November 2024

# Kündigungen und Disziplinarmaßnahmen

---

## Südwestfalen-IT zieht Konsequenzen

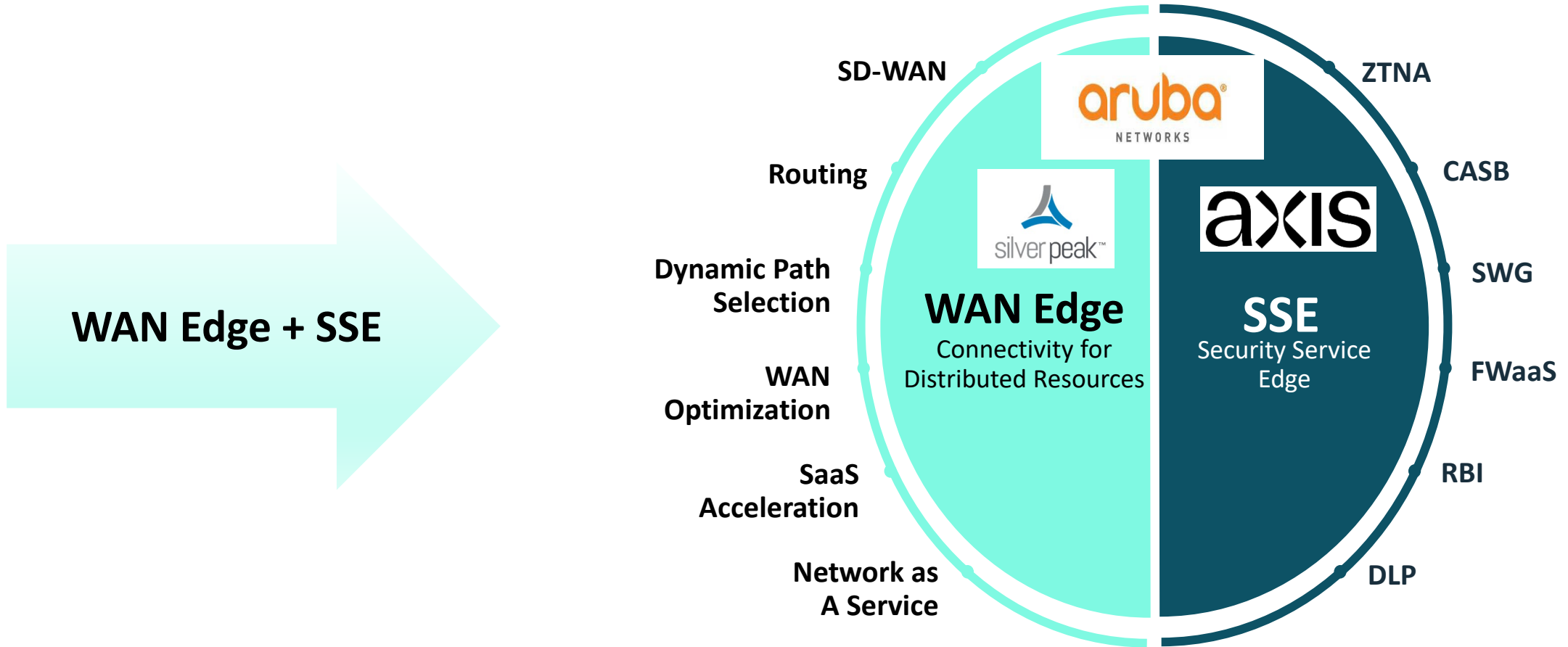


*Die Südwestfalen-IT hat personelle Konsequenzen nach dem Cyber-Angriff aus dem letzten Jahr gezogen.*

*Foto: BS/fotomek, stock.adobe.com*



# Was ist SASE? Secure Access Service Edge



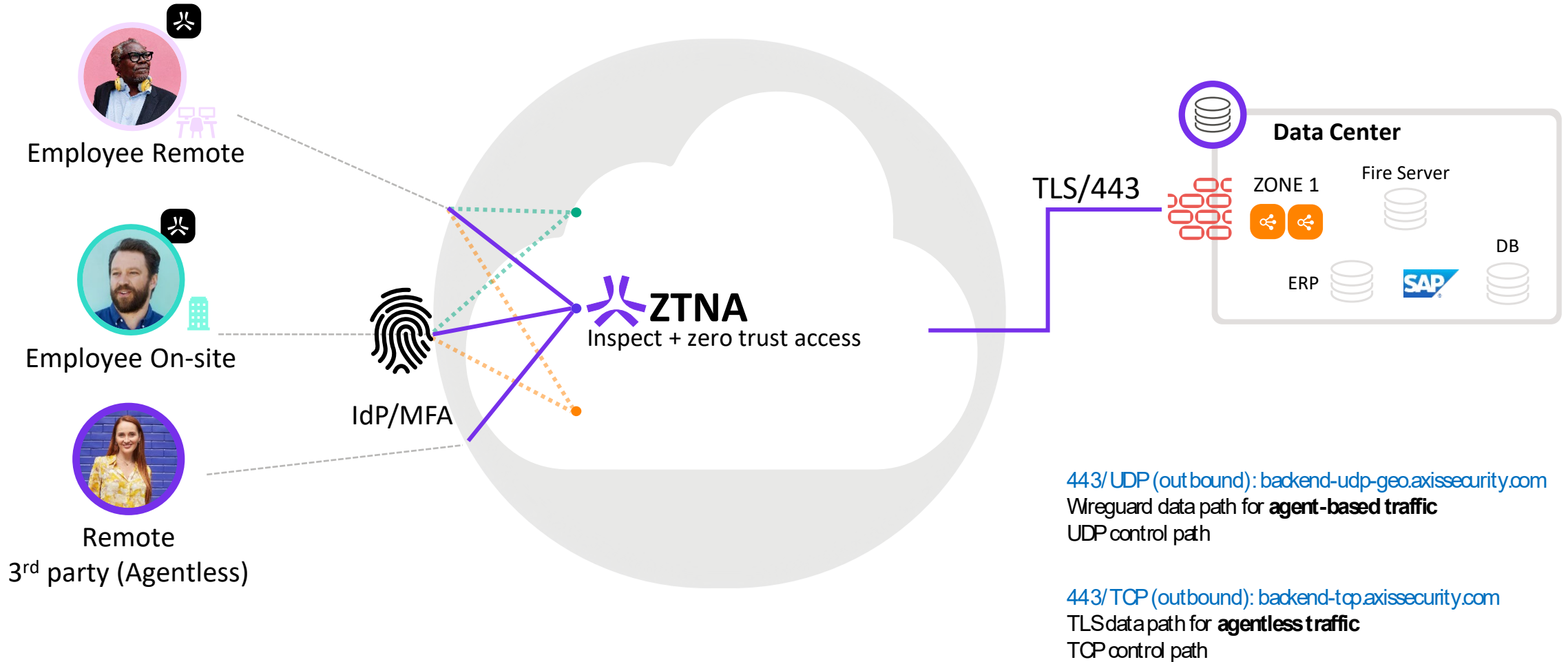
“ Security Service Edge (SSE) sichert den Zugang zum Web, zu Cloud-Diensten und privaten Anwendungen. Zu den Funktionen gehören Zugangskontrolle, Schutz vor Bedrohungen, Datensicherheit, Sicherheitsüberwachung und Kontrolle der akzeptablen Nutzung, die durch netzwerkbasierende und API-basierende Integration durchgesetzt wird. **SSE wird in erster Linie als Cloud-basierender Dienst bereitgestellt** und kann auch Komponenten vor Ort oder agentenbasierte Komponenten umfassen ”

\*Gartner, "Magic Quadrant for Security Service Edge," February 15, 2022

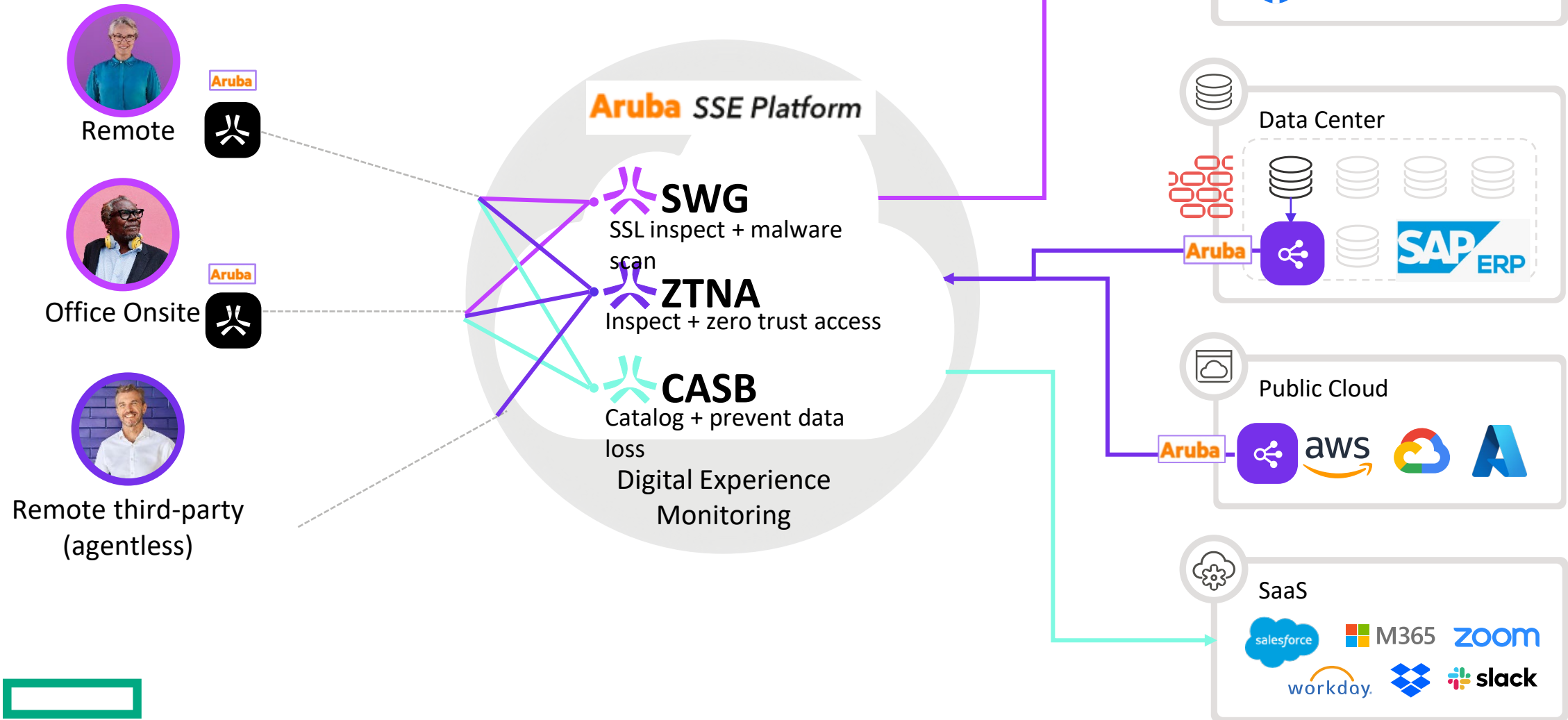
**Gartner**

# One Platform

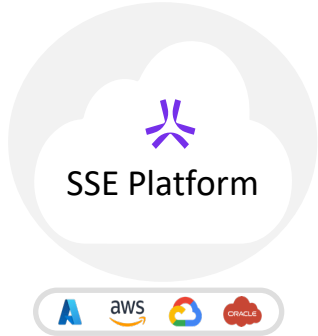
Connectivity to internal and external resources



# Aruba EdgeConnect SSE



# Komponenten der Lösung.



Compute POP, Management Konsole, Richtlinie, Konfigurationen, Mandantenfähigkeit, User Portal, Integrationen, Monitoring



Interner und externer Identitätsanbieter. OATH 2.0, SAML, SCIM, Entra ID, Okta, Ping, 2FA

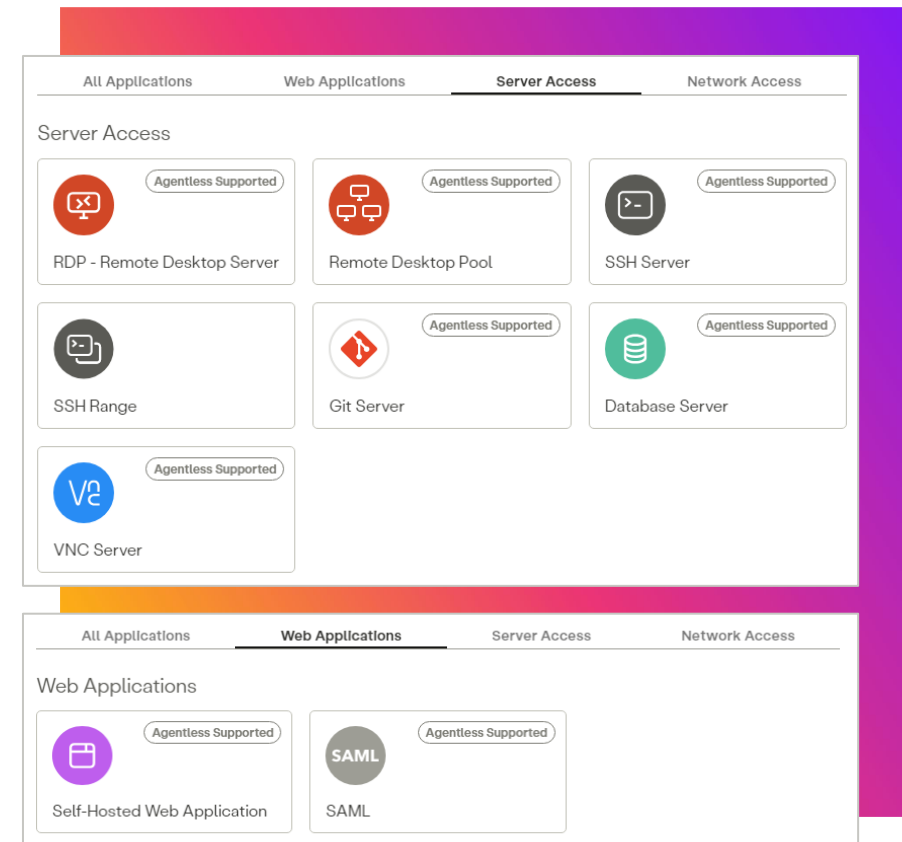
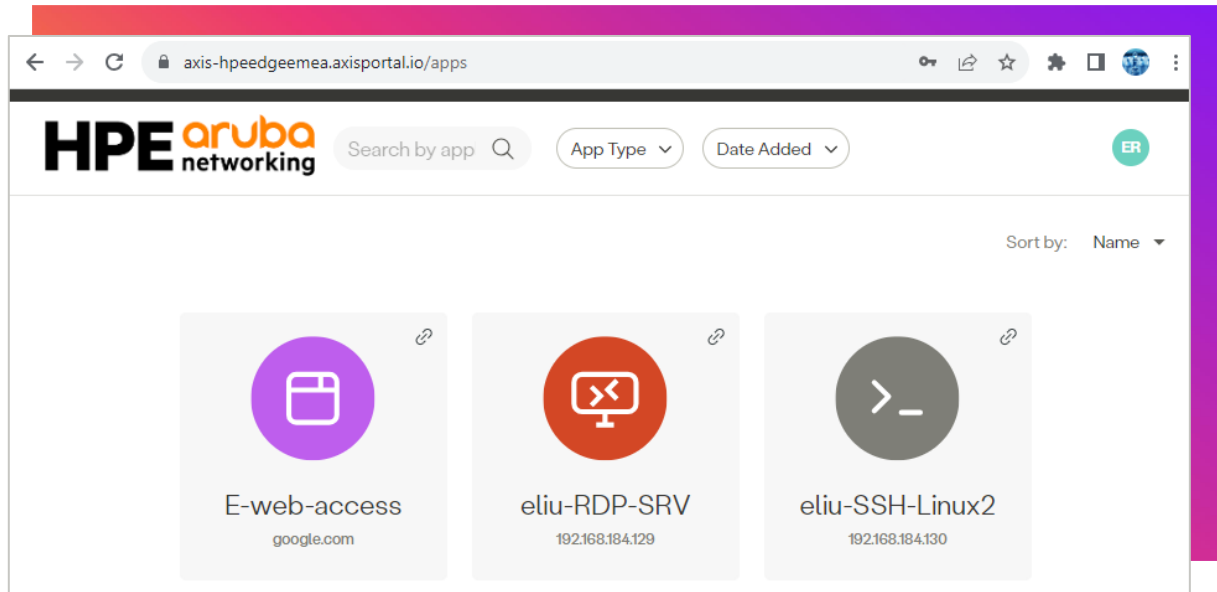


Konnektoren bieten eine sichere Schnittstelle zwischen dem privaten Netzwerk und der SSE Cloud.



Der Agent wird auf dem PC des Anwenders installiert.

# Agentenloser Zugriff auf Unternehmens-Apps



**Webbasierte EdgeConnect SSE-Bereitstellung ohne Agenten**, um den Zugriff auf Web-, RDP-, SSH-, IoT, Git- und DB-Anwendungen mit einer nahtlosen Benutzererfahrung und granularer Transparenz und Kontrolle zu ermöglichen, ohne dass Software auf dem Client installiert werden muss

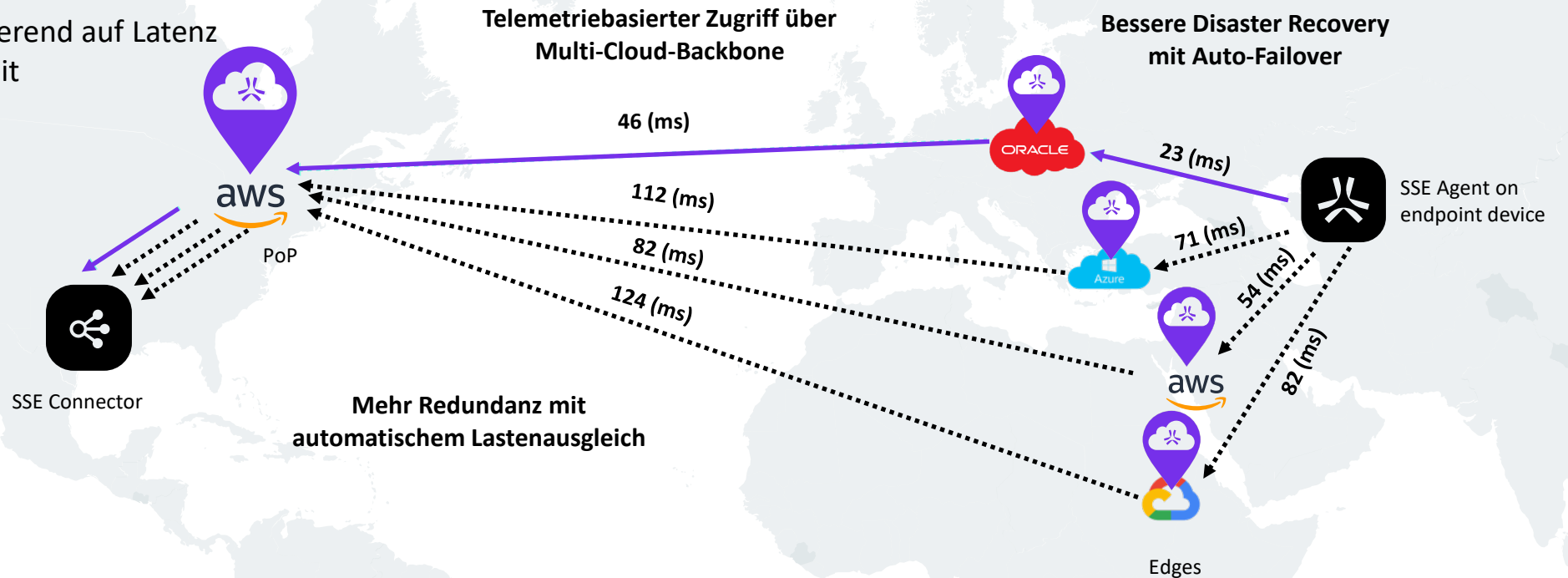
- **Nicht verwaltete Geräte:** Optimiert für 3rd-Party-Benutzer, BYOD
- **Temporärer Zugriff:** z. B. Auftragnehmer, Remote Maintenance



# Cloud-Backbone für Hyper-Resilienz und Geschwindigkeit bei Remote-Arbeit

## Network-as-a-Service

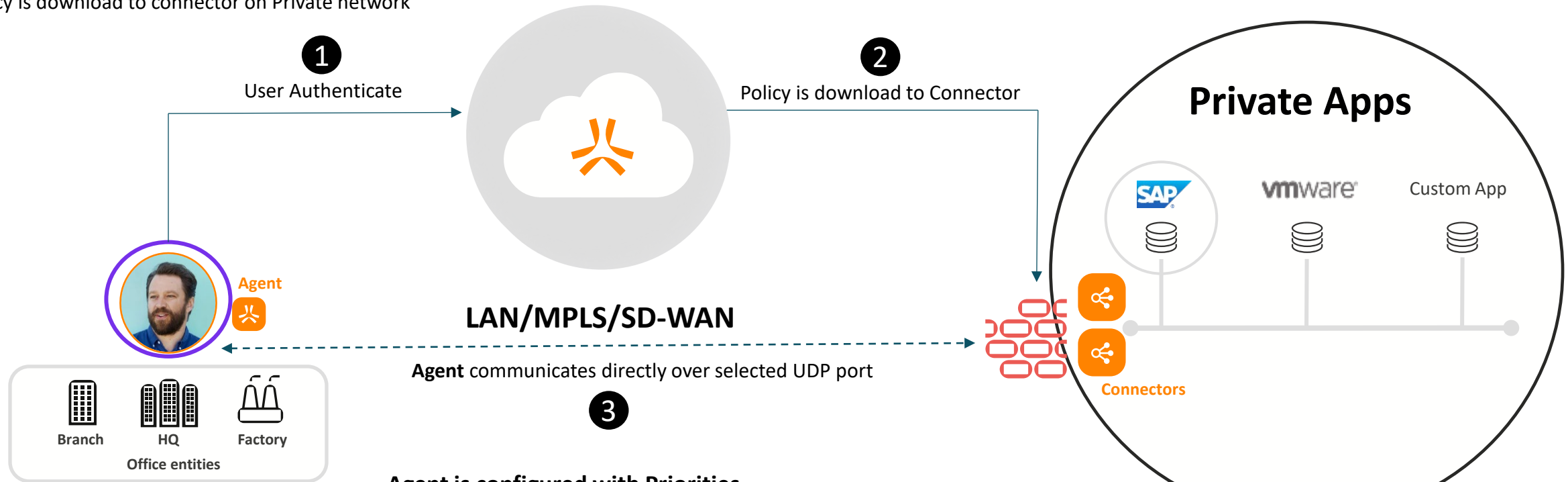
- Geo-proximity Routing
- Intelligentes Routing basierend auf Latenz
- Extrem hohe Verfügbarkeit



# Local Edge

## Process:

- 1- Authenticate with IdP
- 2- Policy is download to connector on Private network



### Agent is configured with Priorities

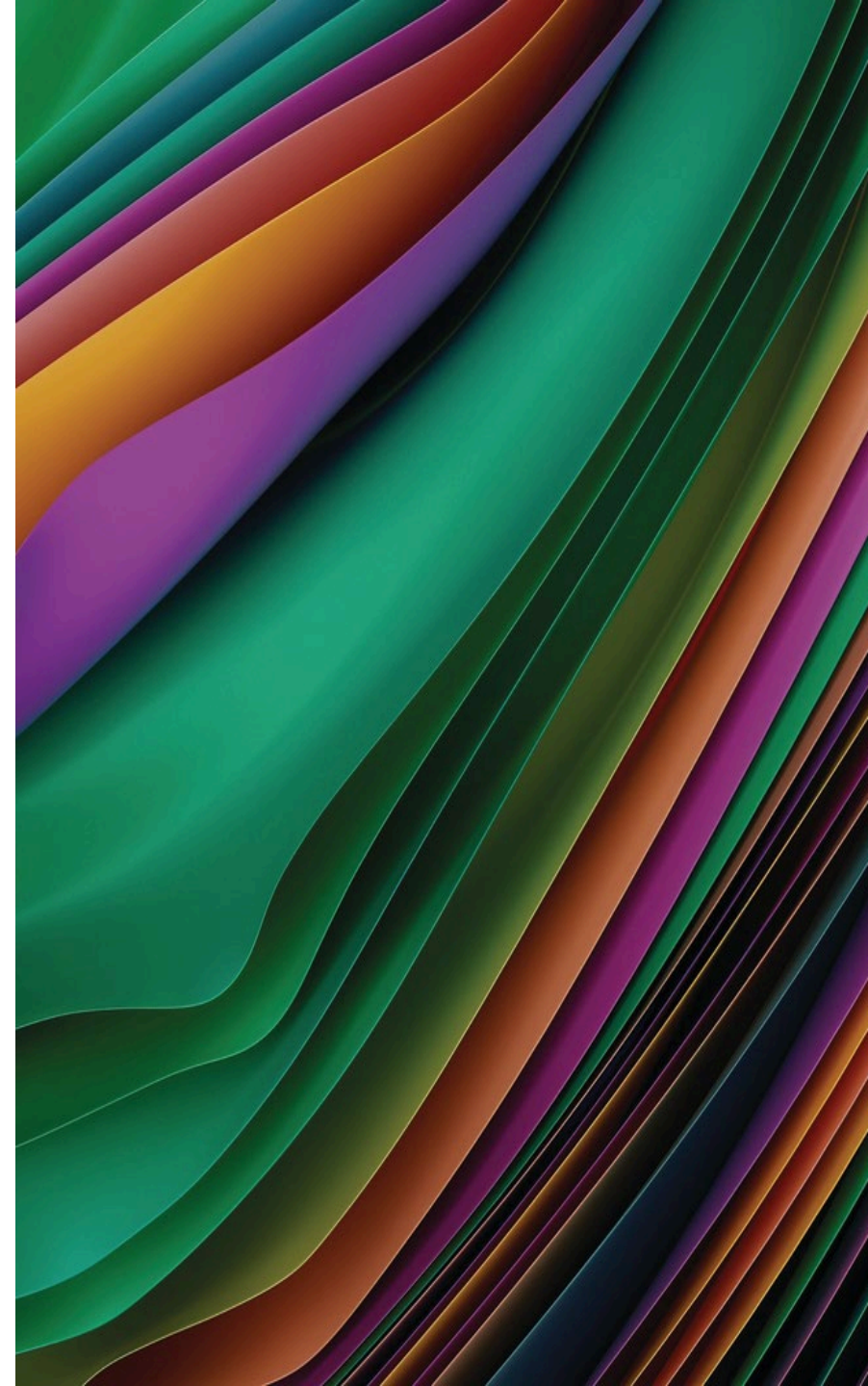
**1<sup>st</sup>. Priority:** Is traffic going to any RFC 1918 IP?

**Yes:** Traffic is handled by the SD-WAN Fabric

**No:** Traffic is sent to closest PoP if connector is not present

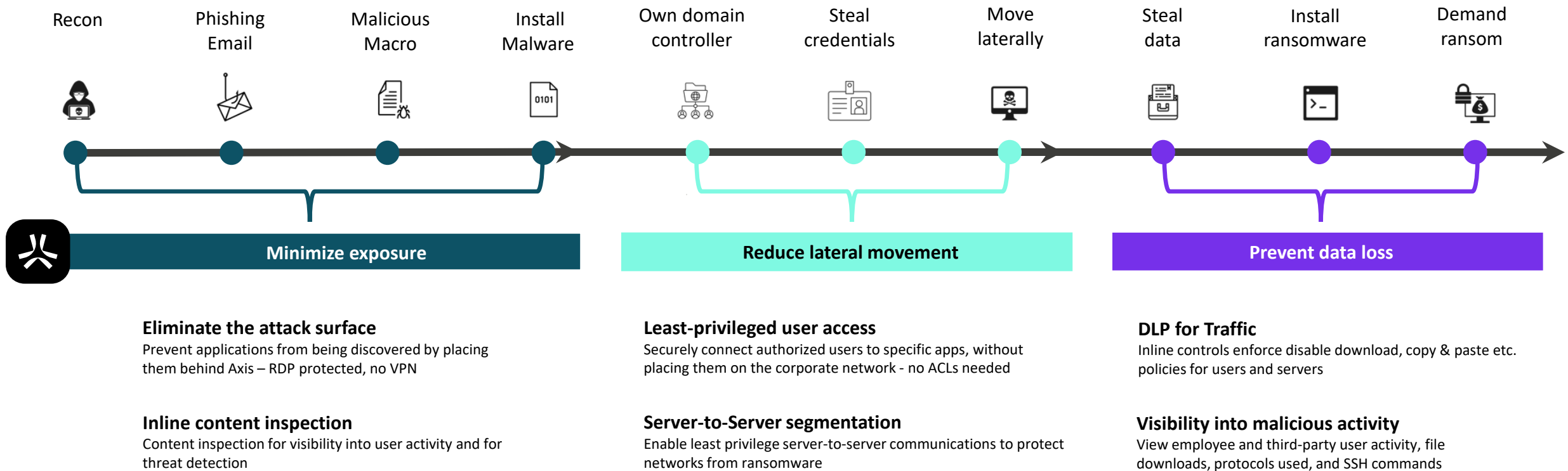
# Driver for Data Loss Prevention (DLP)

---



# Prevent ransomware with ZTNA, SWG and CASB combined

71% of orgs worldwide were affected by ransomware in 2023



# Was ist Zero Trust VPN?

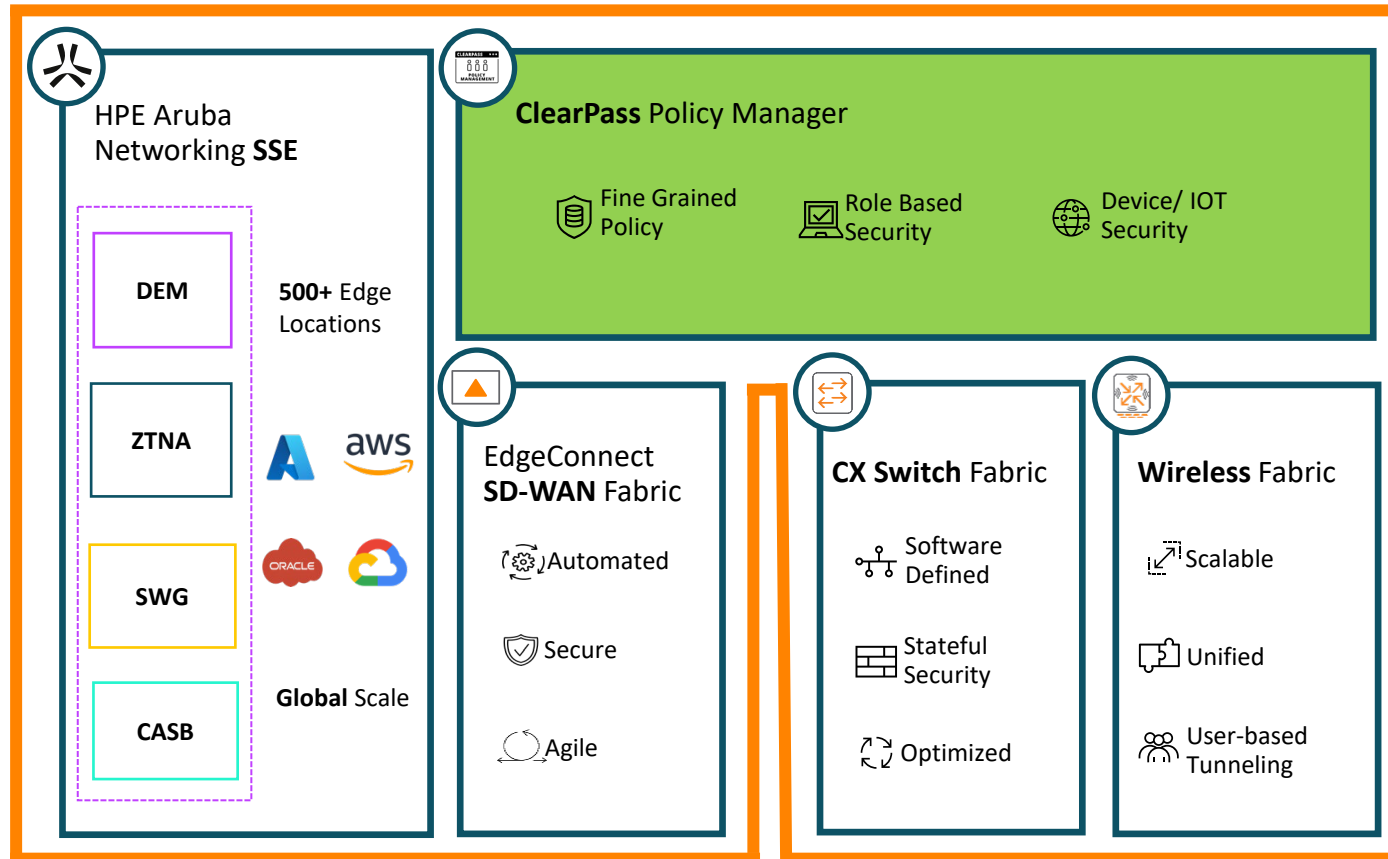
eine Allegorie



# Zero Trust everywhere - HPE Aruba Networking



## Unified SASE Platform



- Strikte Identitätsprüfung
- Minimale Berechtigungen
- Mikrosegmentierung
- Kontinuierliche Überprüfung
- Anomalie-Erkennung



**CUSTOMER FIRST**  
**CUSTOMER LAST**

**HPE** **aruba**  
networking