Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Sicherer Remote Zugriff mit Zscaler Private Access

24. Juni 2025

Mike Schumak, Partner Consulting Sales Engineer

Remotes Arbeiten hat sich in der heutigen Arbeitswelt etabliert.

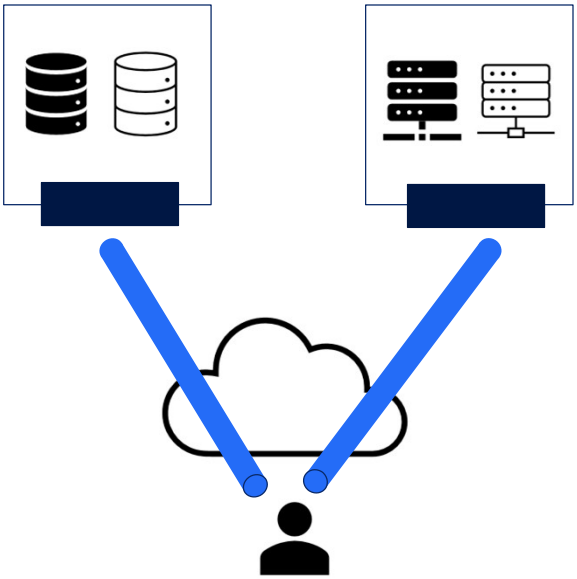
Road Warrior, Home-Office, Wartungspersonal, Business to Business

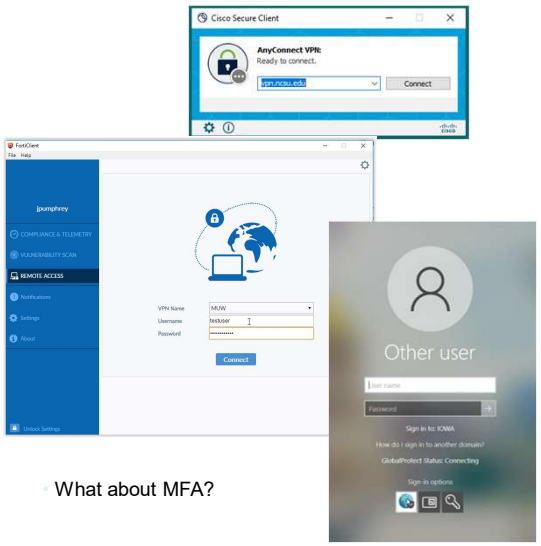
AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Life of a VPN user…

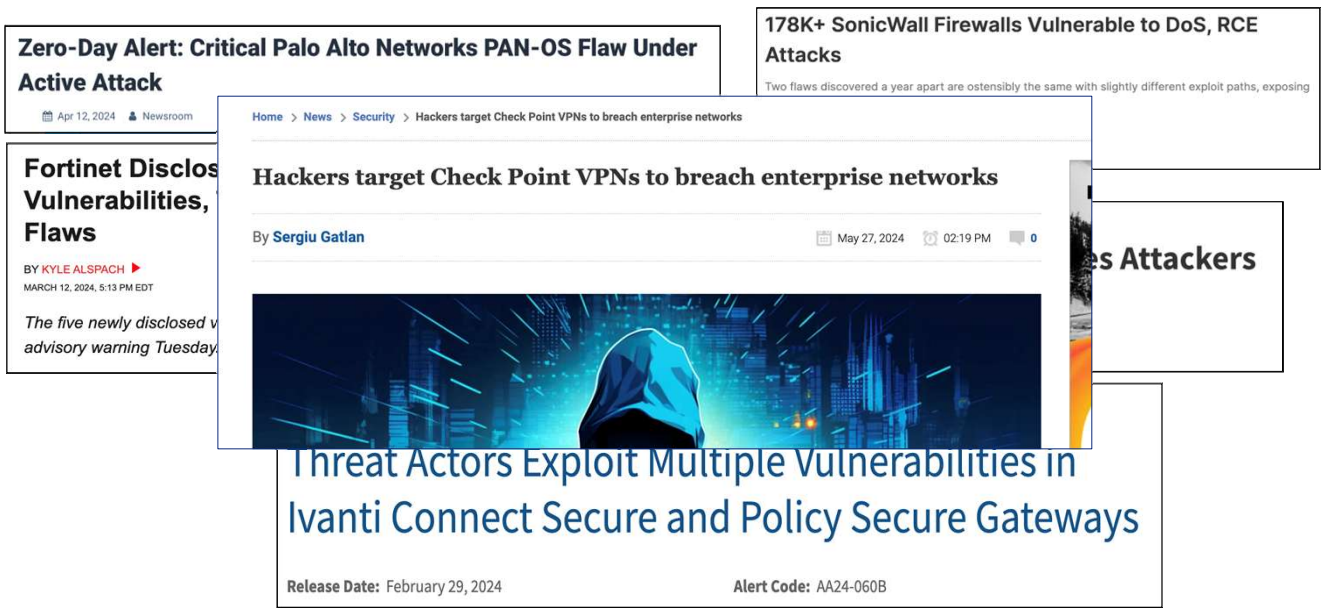
User needs to be educated about the correlation Target-Ressource <> VPN-Endpoint





What about MFA?

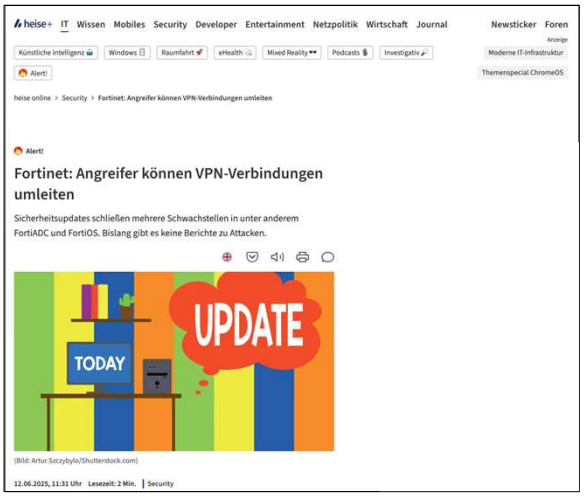
2024 has seen a series of critical firewall and VPN vulnerabilities



AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

2025 is not different…



Nutzen Angreifer eine Schwachstelle (CVE-2024-54019 / EUVD-2025-17801, CVSS **4.4**, Risiko "**mittel**") in FortiClientWindows erfolgreich aus, können sie etwa via DNS-Spoofing VPN-Verbindungen umleiten. Solche Attacken sollen ohne Authentifizierung möglich sein.

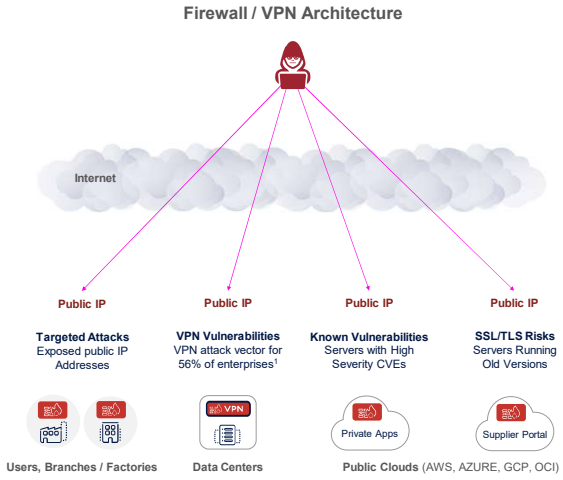
FortiOS ist unter anderem über eine Lücke (CVE-2024-50562 / kein EUVD, CVSS **4.4**, Risiko "**mittel**") attackierbar und Angreifer können sich unbefugt Zugriff auf das SSL-VPN-Portal verschaffen. Dafür müssen sie aber im Besitz eines entsprechenden Cookies sein.

https://www.heise.de/news/Fortinet-Angreifer-koennen-VPN-Verbindungen-umleiten-10441108.html

Im VPN-Client GlobalProtect filtert die Log-Funktion unter macOS einige Zeichen nicht korrekt, wodurch nicht-Admins ihre Rechte zu "root" ausweiten können (CVE-2025-4232, CVSS **8.5**, Risiko "**hoch**")

https://www.heise.de/news/Palo-Alto-stopft-hochriskante-Luecken-in-PAN-OS-und-GlobalProtect-10442194.html

What can be seen from the Internet will be probed and attacked



Attackers exploit vulnerabilities to establish a beachhead on your network

[1] ThreatLabz 2023 VPN Risk Reports

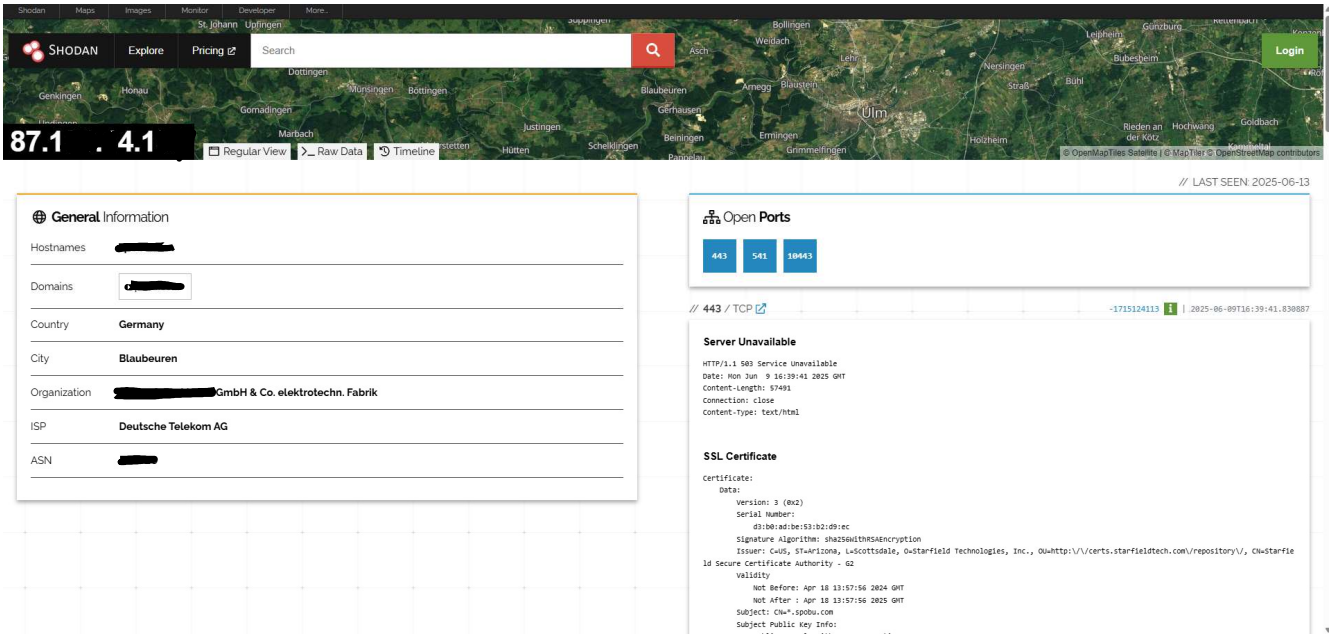
Zscaler Cyberthreat Protection Overview

The best protection is to minimize the attack surface.

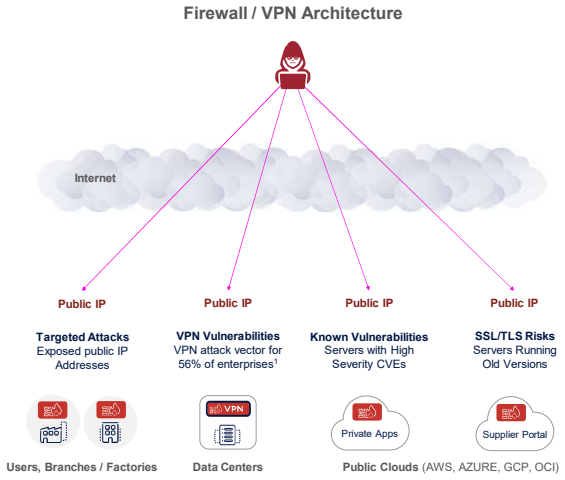
AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Shodan.io



What can be seen from the Internet will be probed and attacked



Attackers exploit vulnerabilities to establish a beachhead on your network

[1] ThreatLabz 2023 VPN Risk Reports

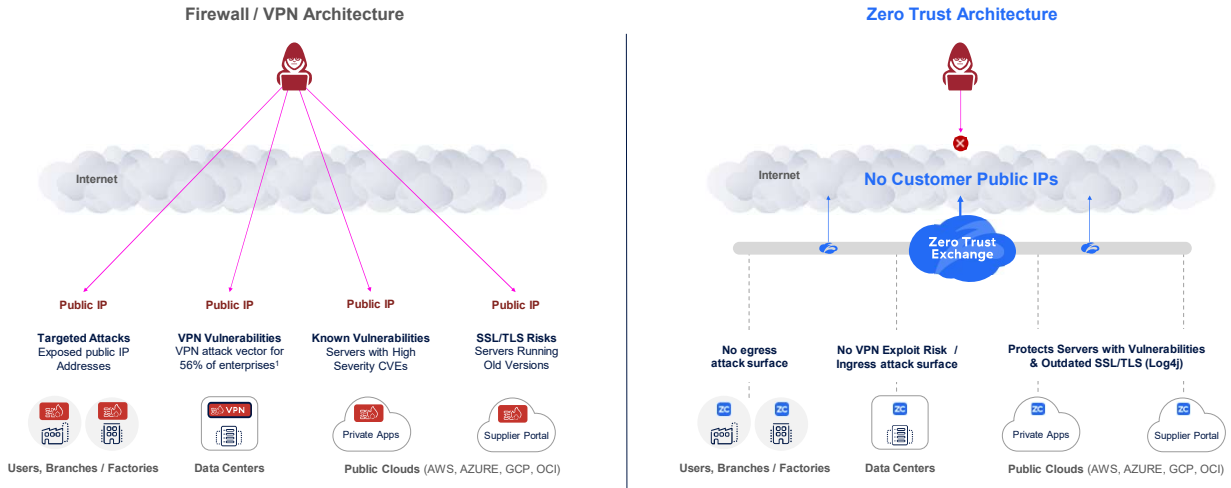
Zscaler Cyberthreat Protection Overview

The best protection is to minimize the attack surface.

AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Zscaler Minimizes the Attack Surface



Attackers exploit vulnerabilities to establish a beachhead on your network

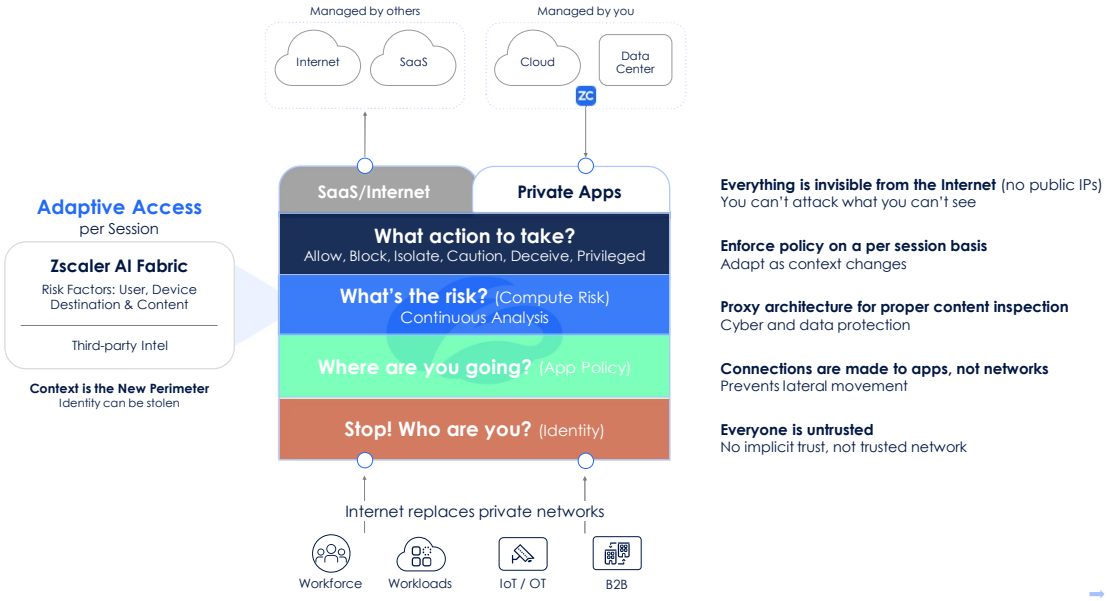
Your apps, branches, factories (including OT systems) are hidden from the Internet; they can't be attacked or exploited.

¹ ThreatLabz 2023 VPN Risk Reports

Zscaler Cyberthreat Protection Overview

The best protection is to minimize the attack surface.

How a Zero Trust Architecture Works



Everything is invisible from the Internet (no public IPs)
You can't attack what you can't see

Enforce policy on a per session basis
Adapt as context changes

Proxy architecture for proper content inspection
Cyber and data protection

Connections are made to apps, not networks
Prevents lateral movement

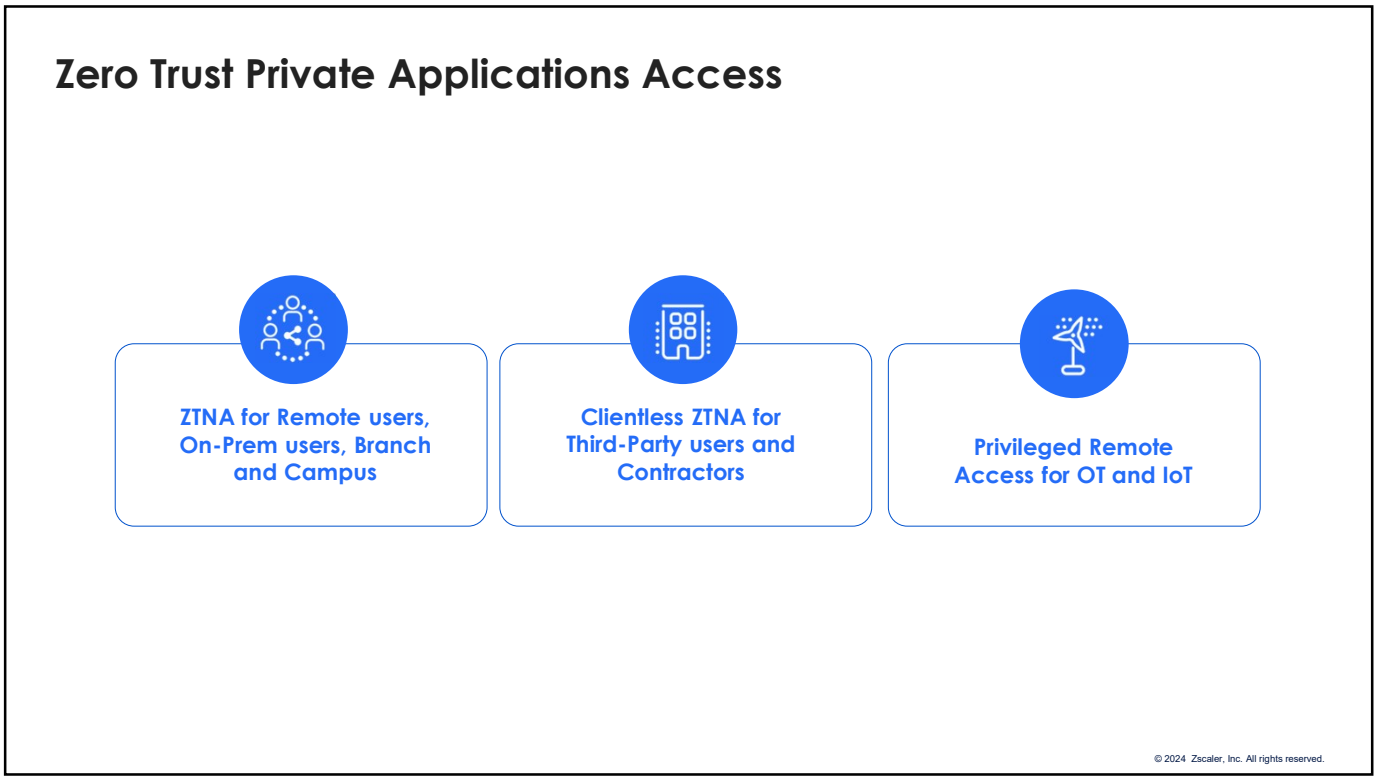
Everyone is untrusted
No implicit trust, not trusted network

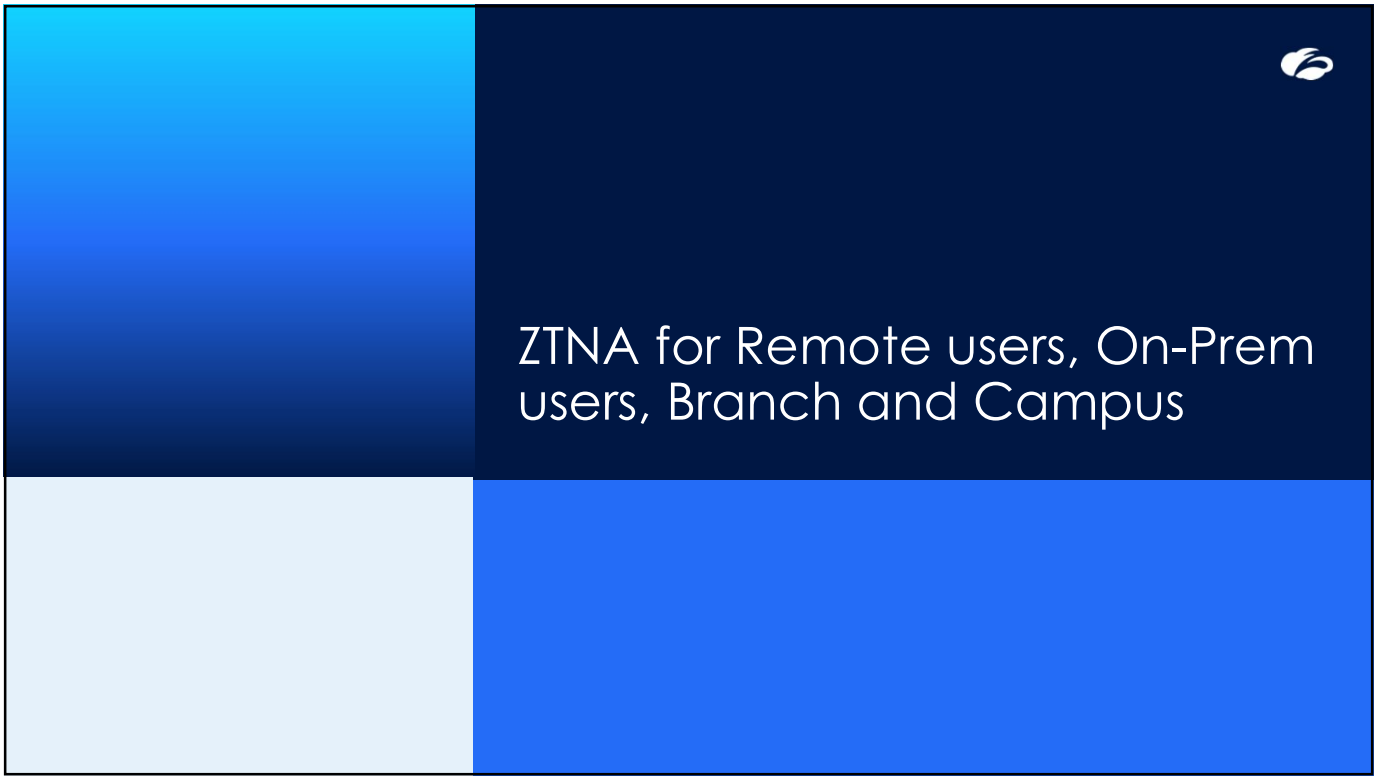
Back to Use Cases

Zero Trust architecture is the opposite of firewalls. It can't be bolted on firewalls and VPNs

AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025





AVANTEC
Competence. Security. Trust.

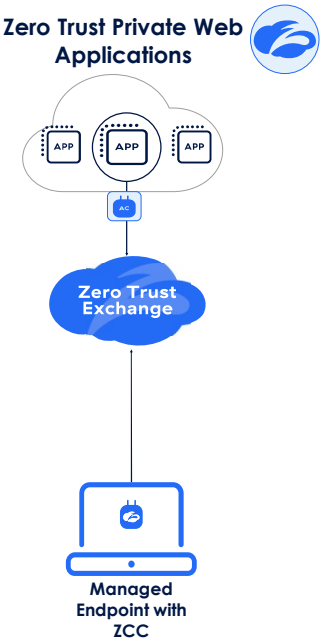
Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Easiest Possibility: Client with Zscaler Client Connector

Lightweight Agent (around 50 MB)

Available on all Major Operating Systems:
- Windows
- Mac
- Linux

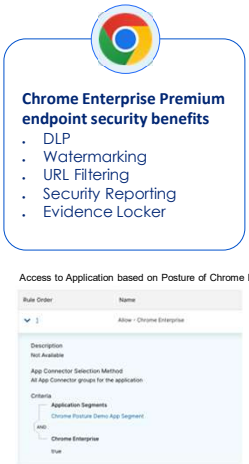
Available for all Major Phone OS:
- Android
- IOS

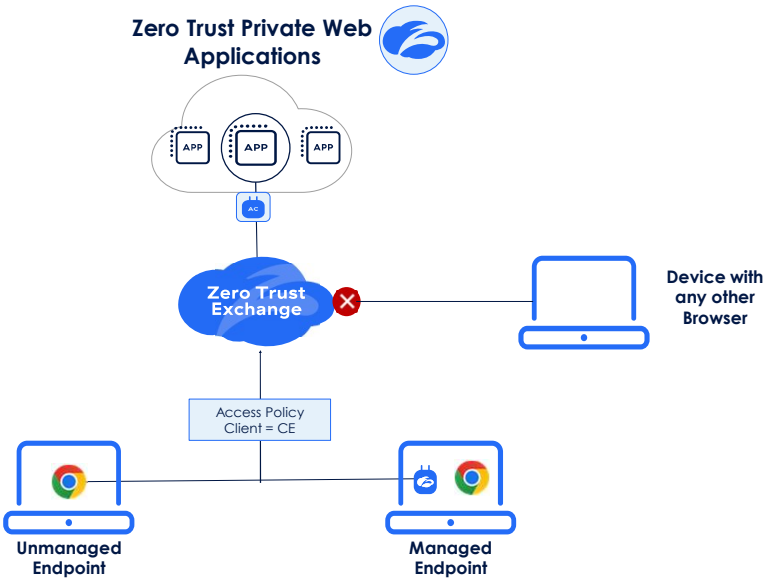


Chrome Enterprise + Zscaler Private Access

Chrome Enterprise Premium endpoint security benefits
- DLP
- Watermarking
- URL Filtering
- Security Reporting
- Evidence Locker

Access to Application based on Posture of Chrome Enterprise





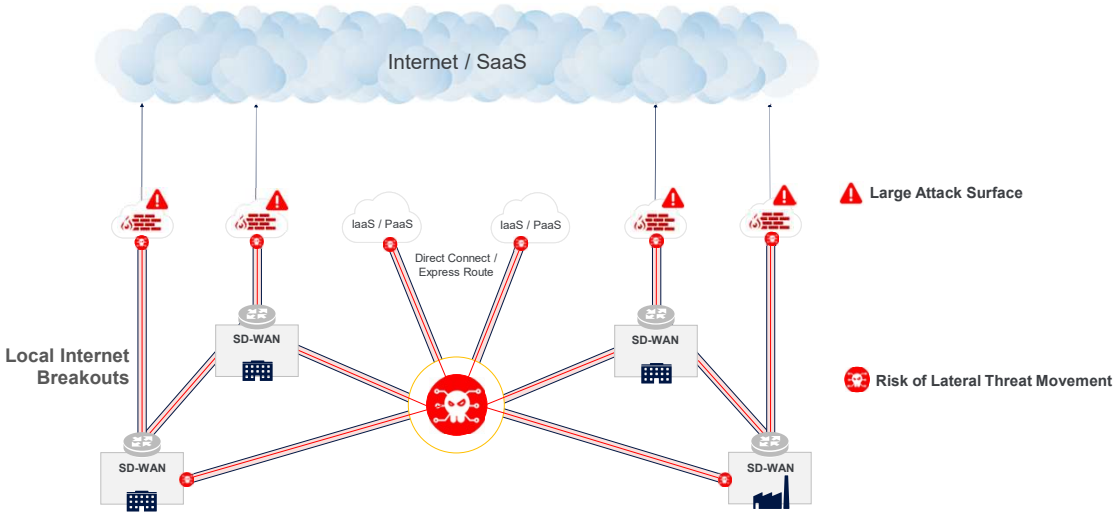
AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Chrome Posture Information

Name	Key	Value
Browser version	browser_version	126.0.6478.127
Key Trust level	key_trust_level	CHROME_BROWSER_HW_KEY
Operating System	operating_system	MAC_OS_X
Disk Encryption	disk_encryption	DISK_ENCRYPTION_ENCRYPTED
Host Firewall	os_firewall	OS_FIREWALL_ENABLED
Boot Mode	secure_boot_mode	SECURE_BOOT_MODE_ENABLED
Screen Lock	screen_lock_secured	SCREEN_LOCK_SECURED_ENABLED
Safe Browsing	safe_browsing_protection_level	STANDARD
EDR	crowd_strike_agent	true

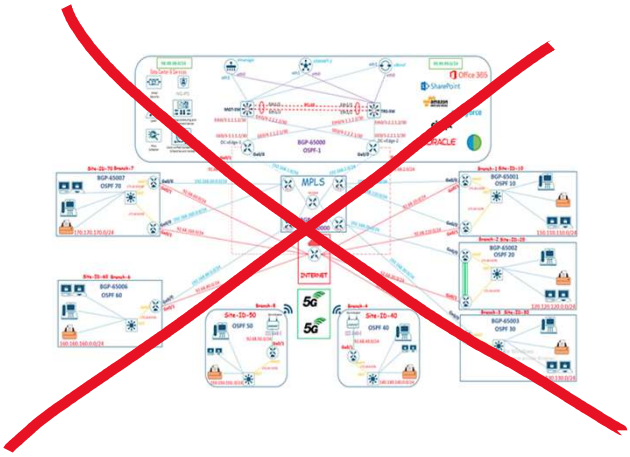
Danger of connecting Branches via VPN

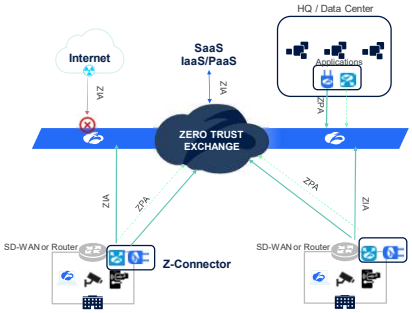


AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Connect Branches with Zero Trust instead of Side-to-Side-VPN





- **Enables Zero Trust access for non-user devices**
  Eliminates lateral threat movement and attack surface
- **No routable WAN required**
  Eliminates the need for maintaining overlay routing network
- **Reduces operational complexity and cost**
  Eliminates the need for virtual DMZs and a mesh of site-to-site VPNS

Clientless ZTNA for Third-Party Users and Contractors

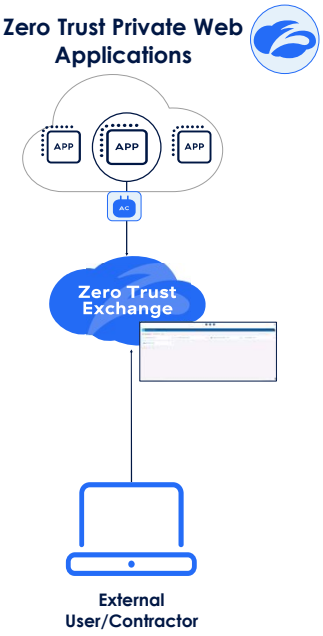
AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Clientless ZTNA for Third-Party Users and Contractors

Easy Access to Web applications inside the Organisation.

Additional Possibilities with Browser Isolation (i.e. Data Protection)



Privileged Remote Access for OT and IoT

AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

The problem

Legacy Networks and security fail for remote access

Increased remote access resulting in breaches and malware

Remote access has increased in a post-pandemic world along with the growth of outsourced, managed operations

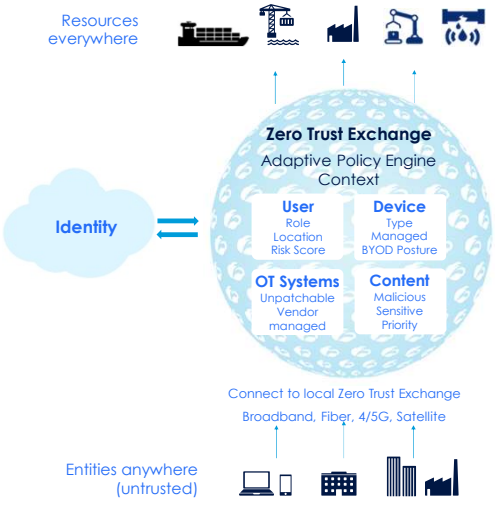
Legacy network security design creates a massive attack surface

Traditional firewalls and VPNs systems allow attackers to take advantage of excessive privileges and move laterally

Third-party and privileged users pose significant risk

Mitigating the risk from privileged users becomes a priority

The value of zero trust in OT/IT convergence



Old-world	VS.	Zero Trust Exchange
OT system access requires network access Risk of lateral threat movement		1 Zero network access Connect users to OT systems/apps, not corporate/OT networks, to prevent lateral movement
Publish OT systems on the internet Large attack surface		2 Zero attack surface Make OT systems invisible so they can't be attacked
Passthrough architecture Limited ability to inspect and protect		3 Zero passthrough connections Proxy architecture for better cyber threat and protection

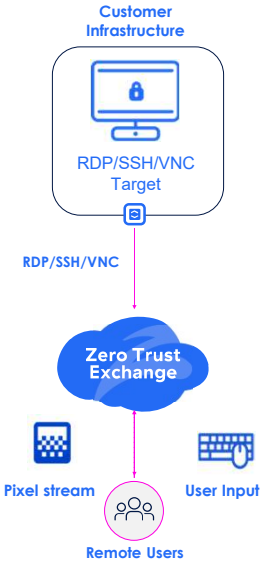
A zero trust architecture is the optimal approach for industrial network transformation.

AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Zscaler Privileged Remote Access

Clientless RDP, SSH and VNC Access with Powerful Data, Security and Session Controls



Time-bound access
- Access during an allotted window of time including business working hours constraints.

Sandboxed File Transfer
- Protect against zero-day threats and Advanced Persistent Threats (APTs) through Sandbox analysis.

Credential Vault and Mapping
- Store shared/privileged credentials of target systems in the Cloud Vault. Perform secret-less brokering using credential map policies.

Session proctoring, recording and playback
- Ushered access with control and transfer along with on-screen activity recording.

Zscaler Delivers a Strong ROI

Return on Investment (ROI)
289%

Reduction in security breaches
55%

Reduction in IT effort
Up to 75%

Annual Infrastructure cost savings
Up to $1.75M

Annual productivity savings with faster remote connectivity
15 hrs/remote user

Source :"The Total Economic Impact™ Of Zscaler Private Access (ZPA)," December 2024 a commissioned study conducted by Forrester Consulting on behalf of Zscaler.

AVANTEC
Competence. Security. Trust.

Sicherer Remote-Zugriff mit Zscaler Private Access
24. Juni & 3. Juli 2025

Next Steps

1. Use Case Discovery Meeting
2. Architecture Workshop

AVANTEC
Competence. Security. Trust.

THANK YOU!

AVANTEC
Competence. Security. Trust.