AVANTEC
Competence. Security. Trust.

Zero Trust Network Access

Christian Burgert
Senior Security Engineer
burgert@avantec.ch

Topics

AVANTEC
Competence. Security. Trust.

- ZTNA – Architektur (aus Sicht von Zscaler, jedoch allgemein)
- Notwendigkeit einer neuen Strategie
- Zscaler Portfolio (ZTNA)
  - Zscaler Internet Access (ZIA) Architektur & Konzept
  - Zscaler Internet Private (ZIA) Architektur & Konzept
  - Forwarding zu Zscaler
- Zusammenspiel Best-of-Breed

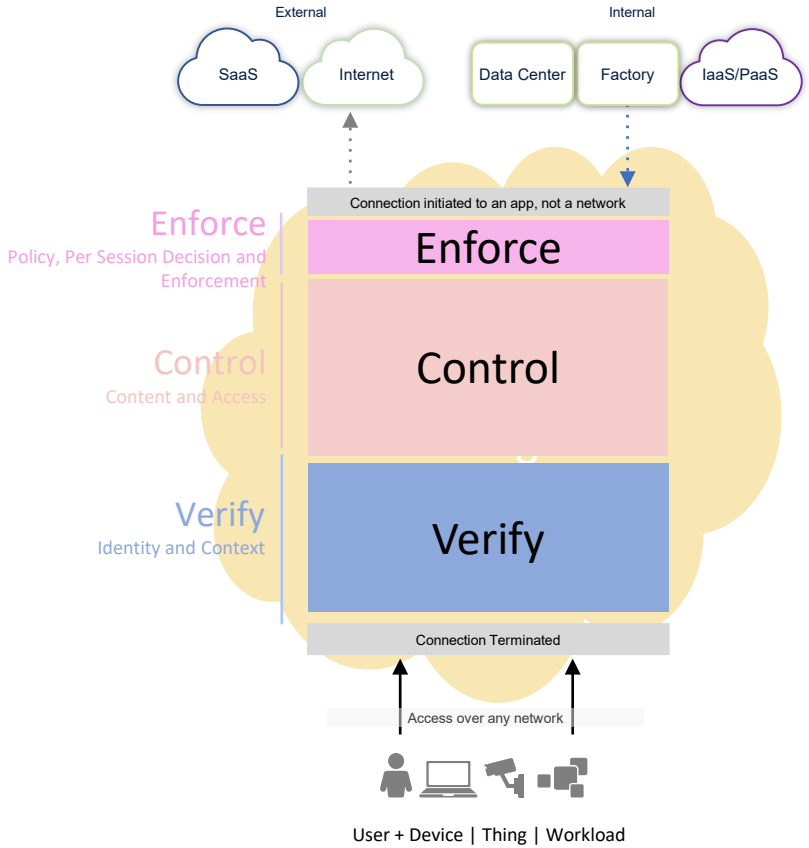
AVANTEC
Competence. Security. Trust.

Zero Trust Network Access

Architektur und Prinzipien

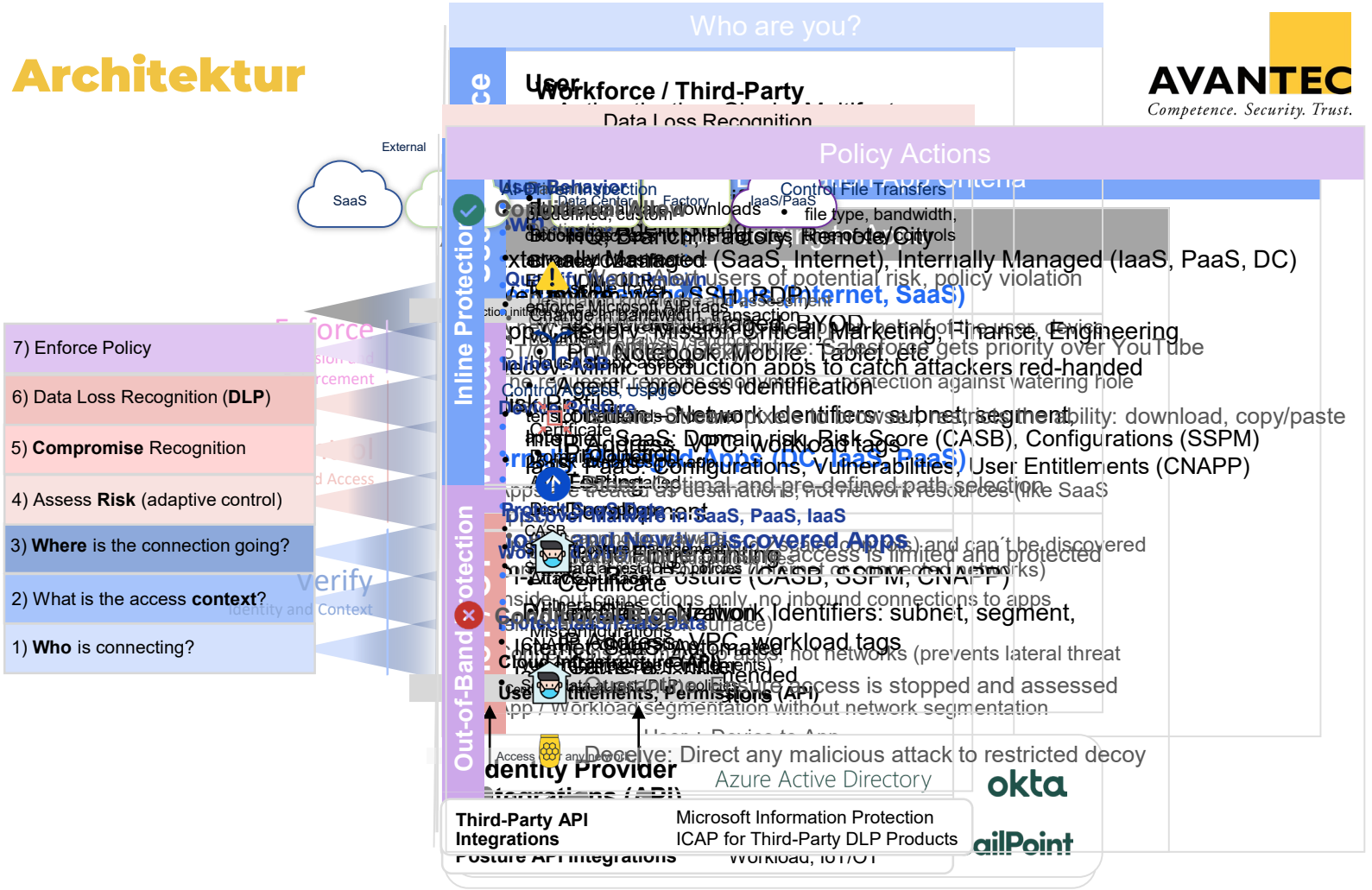
Produkt unabhängig aus Sicht von Zscaler...

ZTNA – Architektur



ZTNA – Architektur

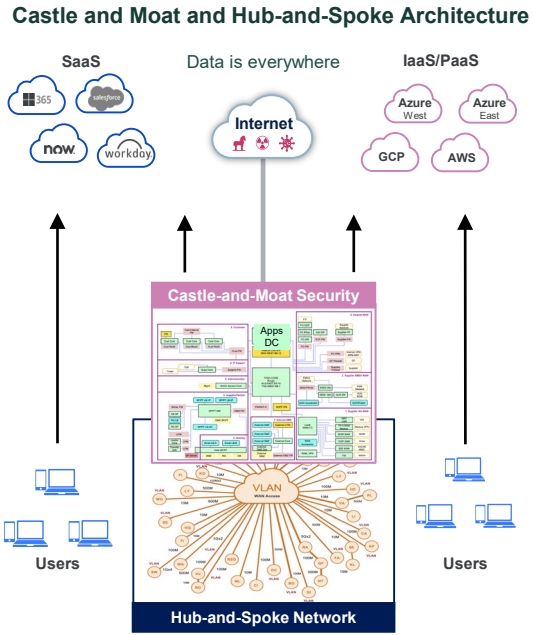
ZTNA – Architektur



AVANTEC
Competence. Security. Trust.

AVANTEC
Competence. Security. Trust.

Warum muss unsere Strategie neu gestaltet werden?



Welche Zscaler Produkte unterstützen uns ZTNA umzusetzen?

AVANTEC
Competence. Security. Trust.

Zscaler Internet Access (ZIA)

Secure Internet and SaaS access
Cyber protection
Data protection (DLP/CASB)
Local internet breakouts (O365/SD-WAN)

Cloud and Branch Connector

ZTNA Access for all devices and location
SDWAN kind Access (Box)

Zscaler Deception

For SoC and Behavior Analyses –
Threats prevention and redirection
to Honeypot Solution

Zscaler Private Access (ZPA)

Secure Private App Access
Remote app access without VPN
Zero trust from office to data center
B2B customer app access

Zscaler Workload Segmentation (ZWS)

Secure Apps and Workloads
App segmentation without network segmentation
for on-prem & cloud workloads

Zscaler Cloud Posture Control

Check your Cloud Workloads
through your Compliance
Remediate cloud misconfigurations (CSPM)

Cloud Browser Isolation

Isolation service for unmatched defense
against web-based attacks and data leakage

Zscaler Digital Experiances (ZDX)

Gain complete visibility over your environment, and
identify and resolve performance issues

AVANTEC
Competence. Security. Trust.

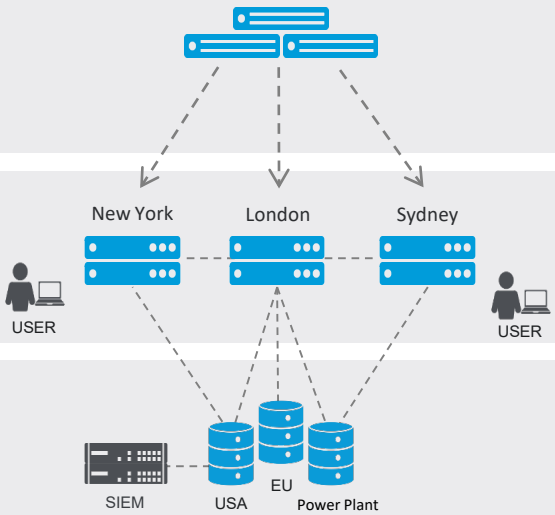
Zscaler Internet Access

Architektur & Konzept

Zscaler Zero Trust Exchange: Architektur

AVANTEC
Competence. Security. Trust.

Central Authority
Brain/nervous system, policy definition, cloud health, rapid updates



Policies by User, Location and AD Groups
Policy changes instantly cascaded through cloud with zero latency

Enforcement Nodes
Inspects traffic, enforces policy

Granular by location or device
Polices follow user location and update immediately on change

NanoLog Cluster
Logs go to a designated log cluster in real-time, never written in ZENs

Complete scalability
Policies scaled and implemented across Zscaler's 150+ Datacenters

Zscaler: Die Security Cloud

AVANTEC
Competence. Security. Trust.

150 Rechenzentren
Richtliniendurchsetzung an der Service-Edge (SASE)

Über 150 Mrd.
Anfragen verarbeitet pro Tag

über 100 Mio.
Bedrohungen blockiert pro Tag

über 175 Tsd.
Spezifische Sicherheits-Updates pro Tag

Peering in Internet-Knoten

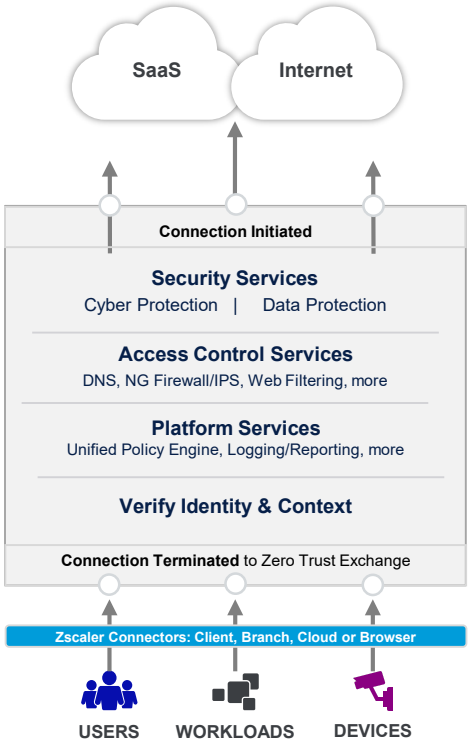
Office 365
Rechenzentrum
Peering

Peering: https://www.peeringdb.com

High Authority

Zscaler Internet Access: Secure and fast internet and SaaS access

AVANTEC
Competence. Security. Trust.



Use Cases

Security Driven

Security Gateway Replacement
- SWG, Firewall, Proxy replacement

Superior Cyber Protection
- Defense in depth: Reputation, signatures, AI/ML, Sandbox, Isolation, more
- SSL/TLS Inspection at Scale

Superior Data Protection
- Secure SaaS (CASB, SSPM)
- Advanced data classification and controls

Zero Trust Connectivity

Local Breakouts (Microsoft 365)
- Performance optimizations and integrations

Zero Trust SD-WAN
- Non-routable branches (like Starbucks)

Secure Workload to Internet
Eliminate virtual firewalls, proxies

Secure IoT / OT to Internet
- Zero Trust Connectivity

Business Value

Reduce Risk	Superior protection in all locations
Improve Productivity	Better collaboration and internet experience
Reduce Costs	Eliminates appliances, reduces MPLS costs

- Firewall / IPS
- URL filter
- Anti-virus
- Data loss prevention
- SSL inspection
- Sandbox

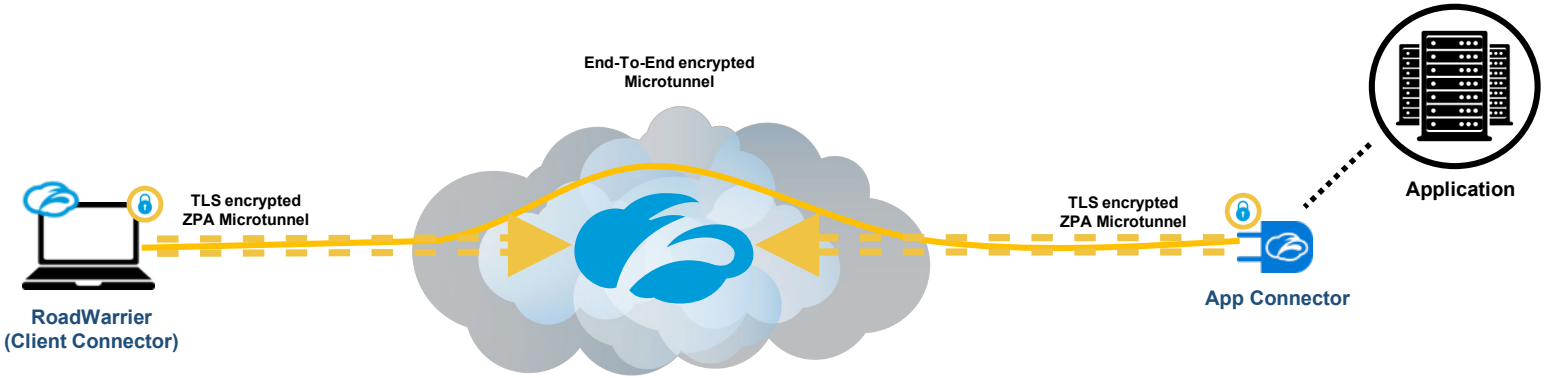
AVANTEC
Competence. Security. Trust.

Zscaler Private Access

was uns dabei wichtig ist.

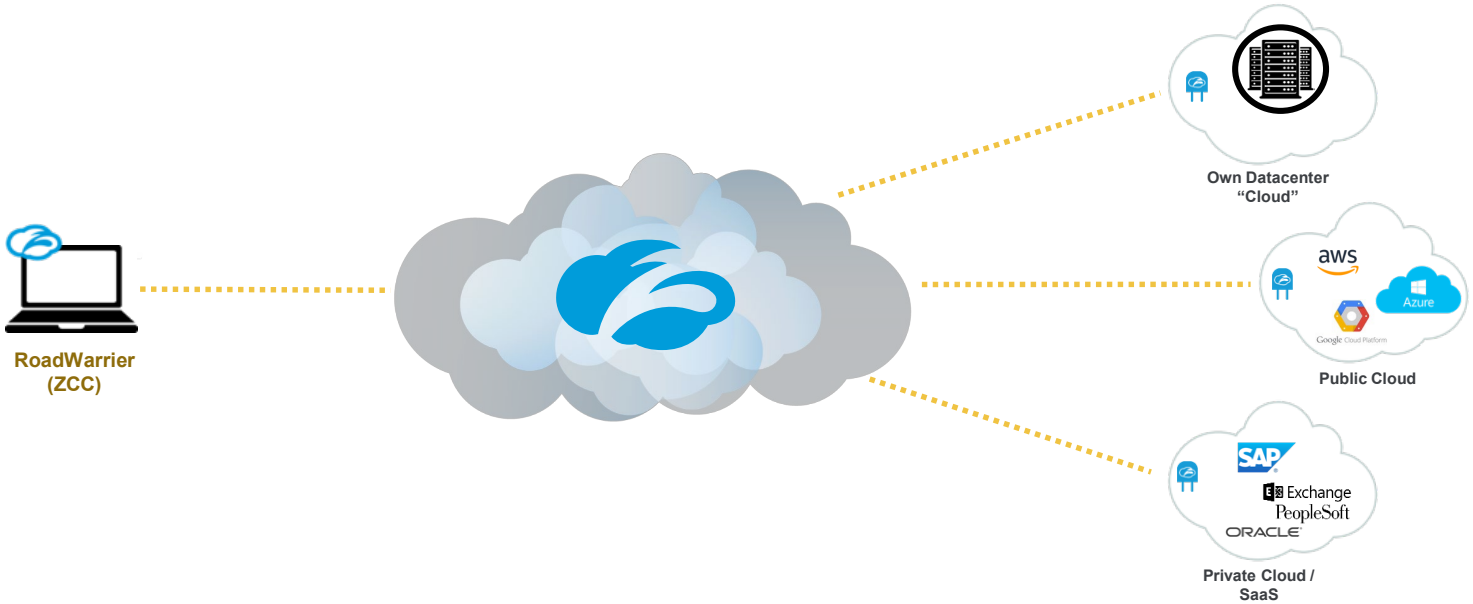
Microtunnel pro Verbindung

AVANTEC
Competence. Security. Trust.



ZPA – Path Selection

AVANTEC
Competence. Security. Trust.



Zscaler Private Access – how it works

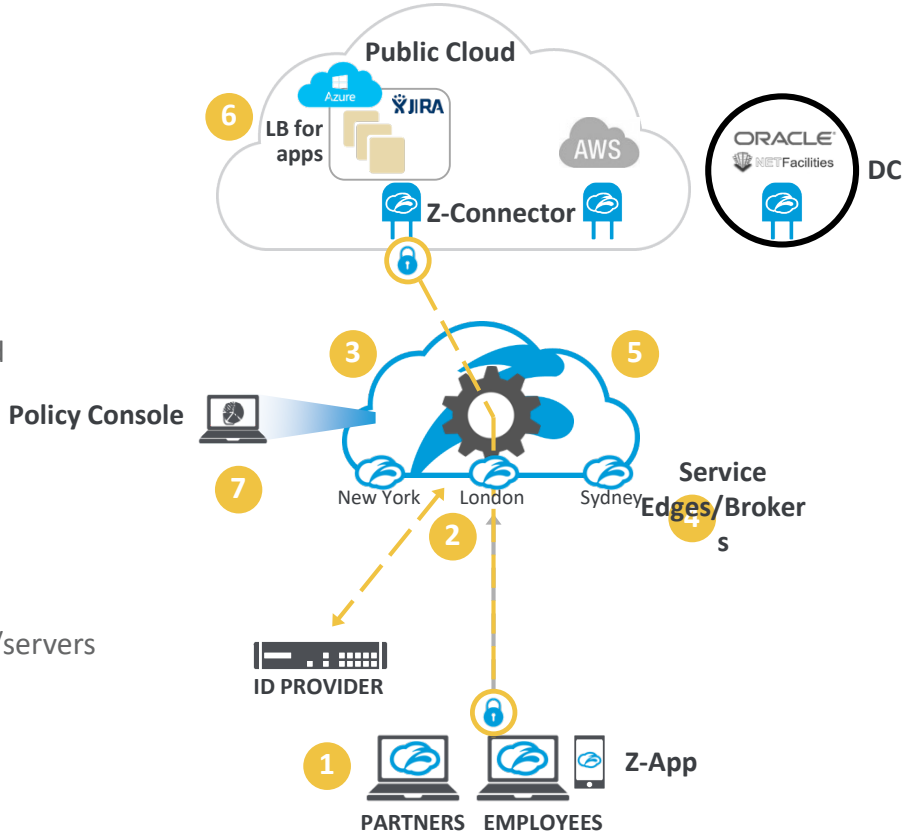
AVANTEC
Competence. Security. Trust.

GETTING STARTED

- Deploy ZCC on endpoints
- Deploy Z-Connectors in front of your apps
- Define user and app access policies

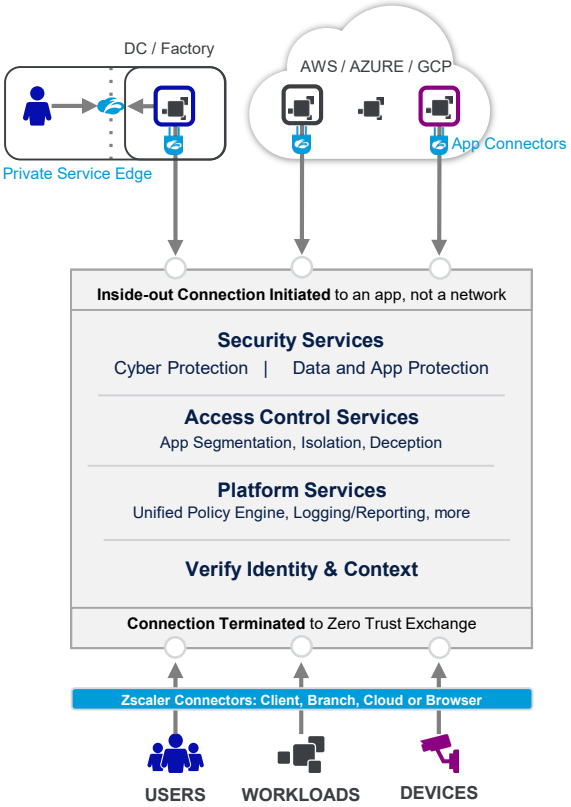
HOW IT WORKS

1. User attempts to access an app
2. User identity/role is verified (before DNS)
3. Policy is checked to determine if access is permitted
4. Optimal path to app is determined
5. If allowed:
   - Z-Connector initiates outbound connection
   - ZCC initiates a connection (per app)
   - Zscaler cloud broker stitches connection together
6. Z-Connector provides app load balance across VMs/servers
7. Monitor app usage – anomaly detection



Zscaler Private Access: Secure and fast private app access

AVANTEC
Competence. Security. Trust.



Use Cases

Zero Trust App Access

VPN Alternative
- Workforce, contractors
- Remote access to OT Systems

VDI Alternative
- Secure BYOD (Web, SSH, RDP)

Zero Trust On-Premises
- Users and apps not on the same network

B2B Customers / Suppliers
- Secure app access (clientless, isolation)

Zero Trust Connectivity

Direct Access to Cloud Apps
- Eliminate Virtual DMZs, No Firewalls or VPNs

Segmentation
- User to App, App to App (mit Branch / Cloud Connector)
- Microsegmentation

Multi-Cloud Connectivity
- Cloud to Cloud, Cloud to DC

Accelerate M&A IT Integration
- App access without integrating networks

Business Value

Reduce Risk
Minimizes the attack surface
Prevents lateral movement

Improve Productivity
Access private apps like SaaS apps – no backhaul

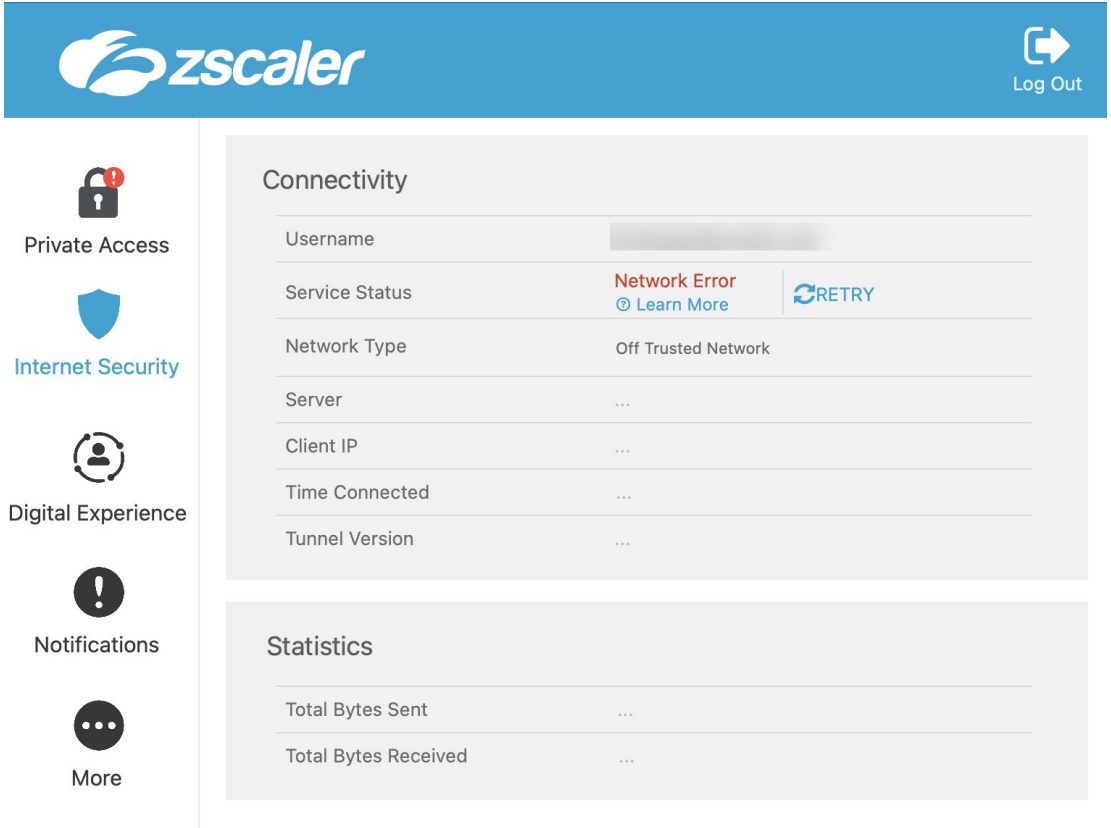
Reduce Costs
Eliminates VPN infrastructure
Physical and Virtual DMZs

- Global load balancing
- DDOS protection
- External firewall / IPS
- Internal load balancer
- VPN concentrator
- Internal firewall

Zscaler Client Connector / Cloud & Branch Connector

Forwarding des Traffics zum Zero Trust Exchange...
Client Forwarding & ZTNA Gateway

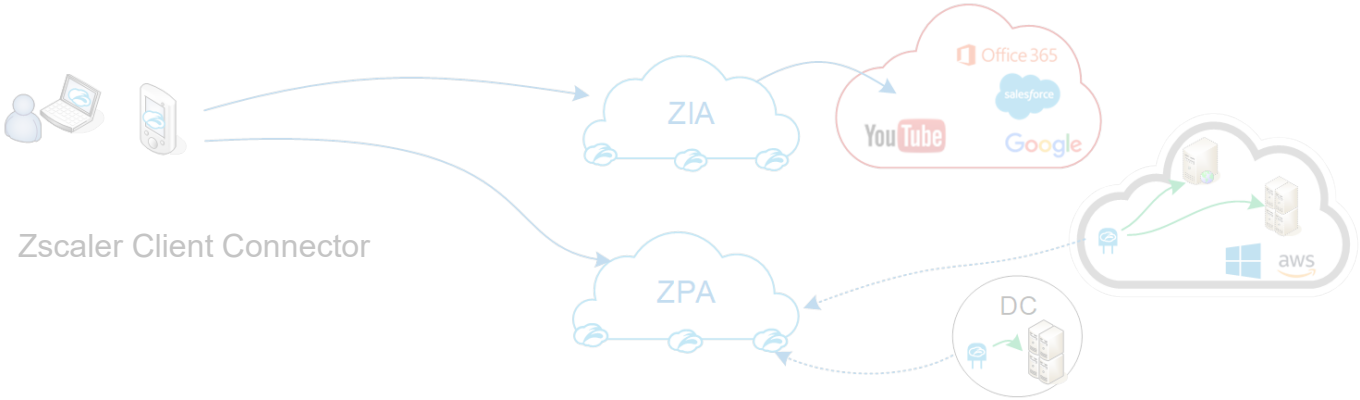
Zscaler Client Connector

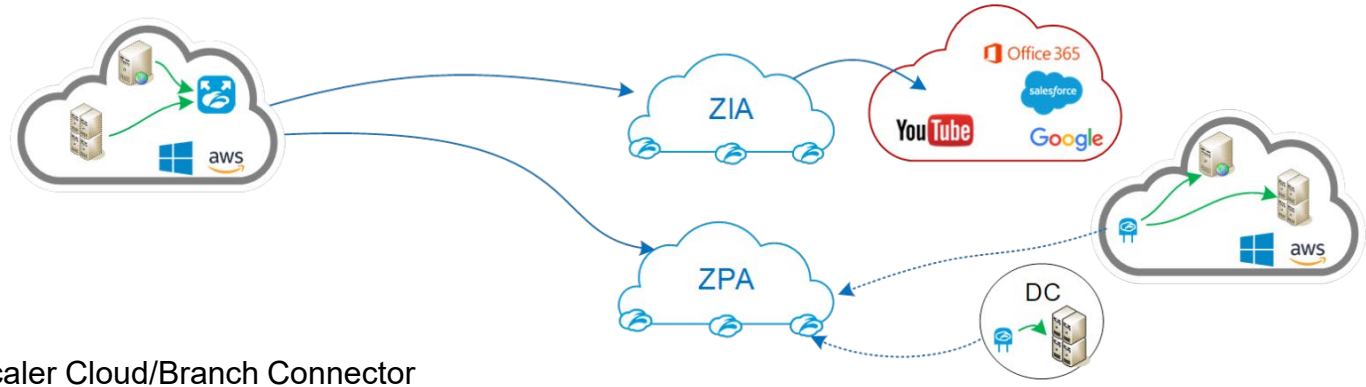


Unterstützung für:

- iOS 9 oder höher
- Android 5 oder höher
- Windows 7 oder höher
- Mac OSX 10.10 oder höher
- CentOS 8
- Ubuntu 20.04

Client- und Branch/Cloud-Connectors





Zscaler Cloud/Branch Connector

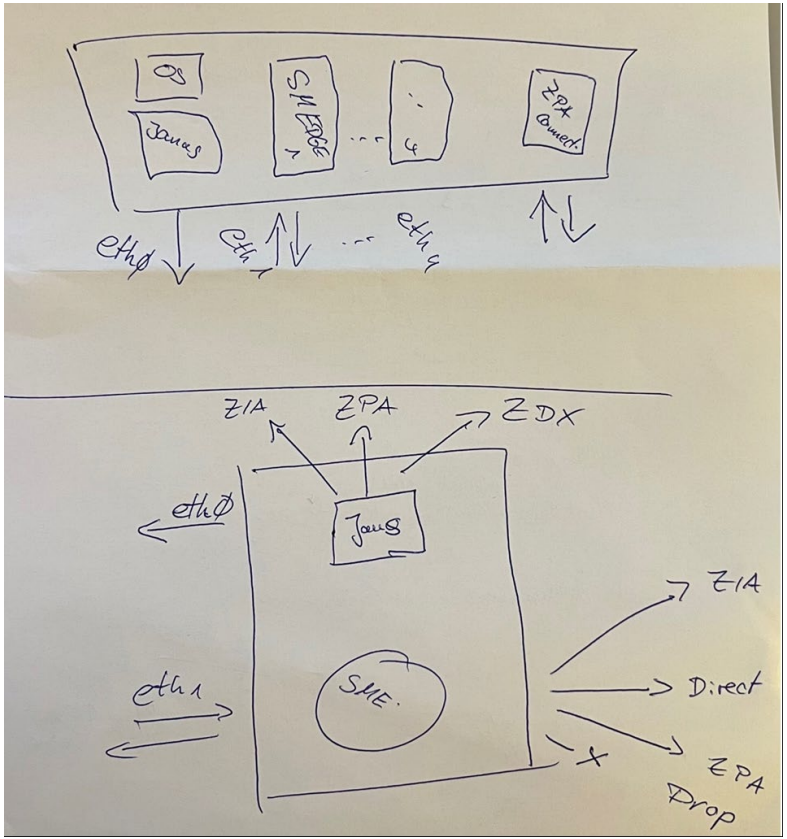
Branch & Cloud-Connectors

AVANTEC
Competence. Security. Trust.

- Generell
  - Forwarding zu ZIA / ZPA / Direct oder Drop
  - Quasi: ZTNA “SDWAN” Gateway
  - Per SME-Process: 500Mbits

- Branch Connector
  - Hardware (derweil auch als VM)
  - ZPA Connnector

- Cloud Connector
  - Ready to deploy Templates
  - Kein ZPA Connnector

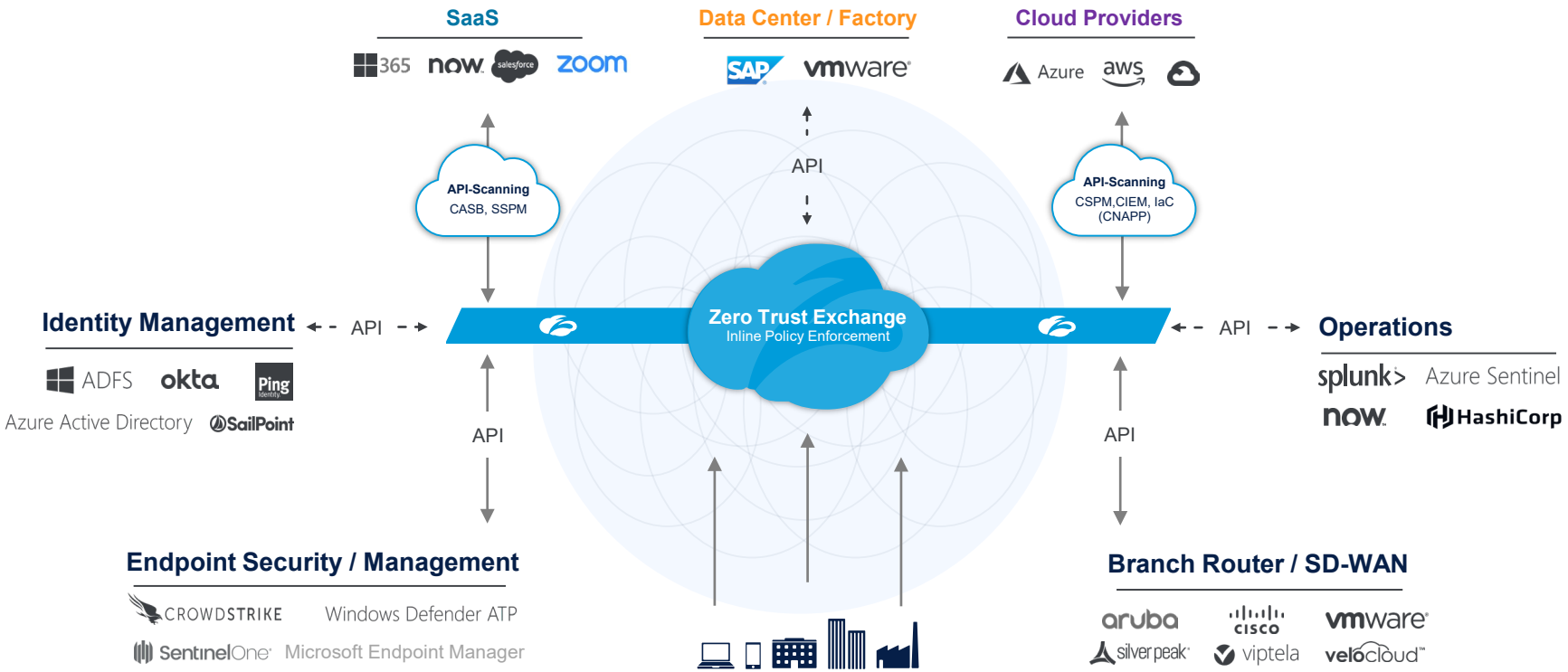


Zusammenspiel Best-of-Breed

Es kann nicht nur einen geben...!?

Zusammenspiel der best-of-breed Plattformen

AVANTEC
Competence. Security. Trust.



Microsoft Integrations

AVANTEC
Competence. Security. Trust.

Gefährliches maximal minimieren –
wie wir Sie dabei unterstützen können.