Zscaler Technical Update
25. Januar 2023

Round Table: Zero Trust Network (Architecture)

Christian Burgert
Senior Security Engineer
burgert@avantec.ch

Ziele dieses Roundtables

- Mein Ziel dieses Roundtable ist es, in einer Diskussionsrunde …
  - festzustellen, wer ist in der Runde (5 min)
  - Zu definieren was ZTNA ist (20 min)
  - was der Mehrwert sein kann (5 min)
  - welche Produkte von Zscaler uns dabei unterstützen (5 min)
  - Offene Runde (10 min)

Zscaler Technical Update
25. Januar 2023

Who is in this round?

- Who – are you?
  - What is you doing?
- What – are you expecting?

What is your experience?

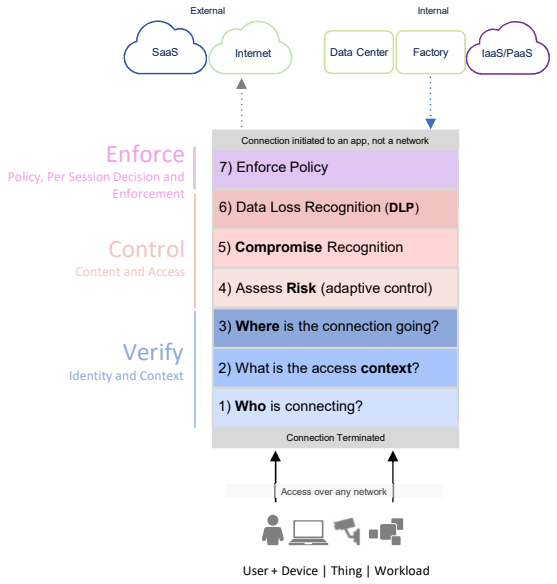
- Who is sure what ZTNA is?
- Who already uses ZTNA?

Wir sorgen für höchste IT-Sicherheit –
was uns dabei wichtig ist.

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

What is ZTNA?



What is ZTNA?

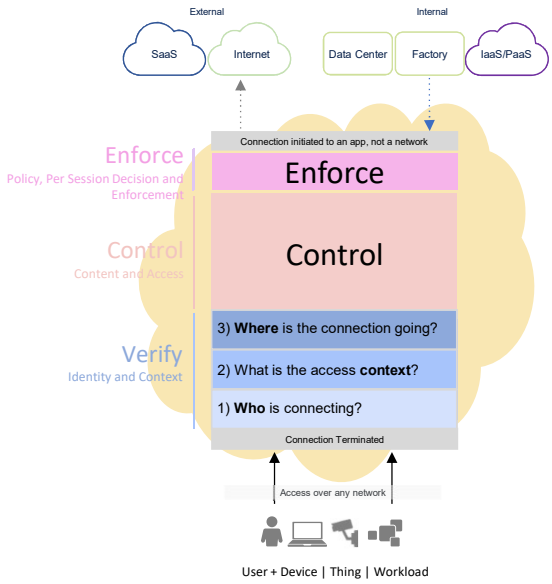
- Open discussion…

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

ZTNA – the architecture

AVANTEC
Competence. Security. Trust.



Verify – in details

AVANTEC
Competence. Security. Trust.

	Who are you?	What are your responsibilities and context?
User + Device	**User** • Authentication: Single, Multifactor **Device** • Fingerprint, Certificate • User Agent String	**Workforce / Third-Party** • Sales, Engineering, Support • Contractor, Supplier, B2B customer **Location** • HQ, Branch, Factory, Remote/City **Device** • Corporate Managed, BYOD • PC, Notebook, Mobile, Tablet, etc.
Workload	• Agent – process identification • Location – Network Identifiers: subnet, segment, IP Address, VPC, workload tags	• Production • Testing • Development
IoT / OT	• Traffic Fingerprinting • Certificate • Location – Network Identifiers: subnet, segment, IP Address, VPC, workload tags	• Camera, Printer • Sensors, Actuators

Destination App Criteria

Known Apps
- Externally Managed (SaaS, Internet), Internally Managed (IaaS, PaaS, DC)
- Web or Non-web (SSH, RDP)
- App Category: Mission Critical, Marketing, Finance, Engineering
- Decoy: Mimic production apps to catch attackers red-handed
- Risk Profile
  - Internet, SaaS: Domain risk, Risk Score (CASB), Configurations (SSPM)
  - IaaS, PaaS: Configurations, Vulnerabilities, User Entitlements (CNAPP)

Unknown and Newly Discovered Apps
- API-Driven Risk Posture (CASB, SSPM, CNAPP)
- ML-Driven Categorization
  - Internet, SaaS: Automated
  - IaaS, PaaS: Recommended

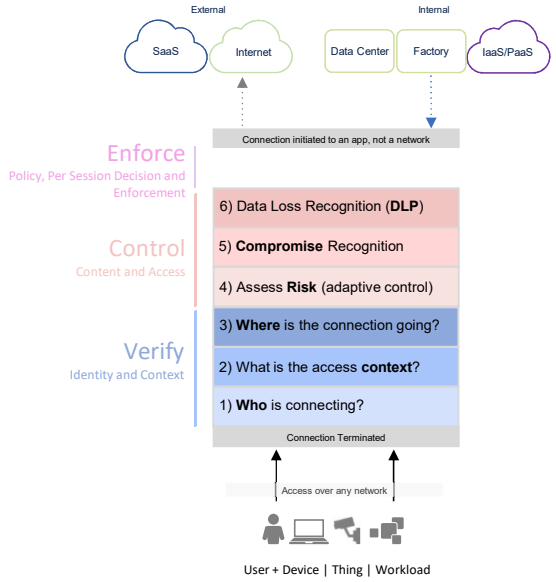
Identity Provider Integrations (API) Azure Active Directory okta Ping ADFS SailPoint

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

ZTNA – the architecture

AVANTEC
Competence. Security. Trust.



Control – in detail

AVANTEC
Competence. Security. Trust.

Access Risk

User + Device

User Behavior
- Blocked malware downloads
- Blocked access to phishing sites
- Blocked C2 traffic
- Impossible travel
- Change in bandwidth, transaction volume
- Unusual app access

Device Posture
- Certificate
- Domain Joined
- AV / EDR Installed
- Disk Encryption

Workload

Workload (API)
- Attack Surface
- Vulnerabilities
- Misconfigurations

Cloud Infrastructure (API)

User Entitlements, Permissions (API)

Third-Party Risk Score and Posture API Integrations — User, Device, Workload, IoT/OT

Compromise Recognition

Inline Protection

Block the Known Bad
- Pattern
- Signature
- Destination

Quantify the Unknown
- Destination knowledge and assessment
- Content knowledge and analysis
- Behavioral Analysis (sandbox)

Out-of-Band Protection

Discover Malware in SaaS, PaaS, IaaS
- API scanning for malware
- Sandbox unknown, suspicious files

Third-Party API Integrations — Threat Intelligence, Cloud effect

Data Loss Recognition

Inline Protection

Data Loss Prevention
AI-Driven Inspection
- predefined, custom dictionaries
- advanced classification: EDM, IDM, OCR
- enforce Microsoft AIP tags

File Type Controls
Control File Transfers
- file type, bandwidth, time-of-day controls

Inline CASB
Control Access, Usage
- tens of thousands of defined apps
- 25 risk attributes per app

Out-of-Band Protection

Protect SaaS Data
- CASB
- SSPM (posture management)
- Scan data at rest (DLP) policies

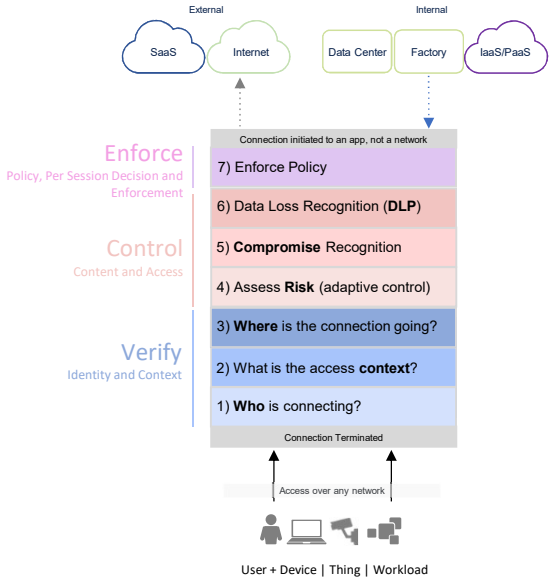
Protect IaaS/PaaS Data
- CNAPP (configurations, vulnerabilities, user entitlements)
- Scan data at rest (DLP) policies

Third-Party API Integrations — Microsoft Information Protection, ICAP for Third-Party DLP Products

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

ZTNA – the architecture



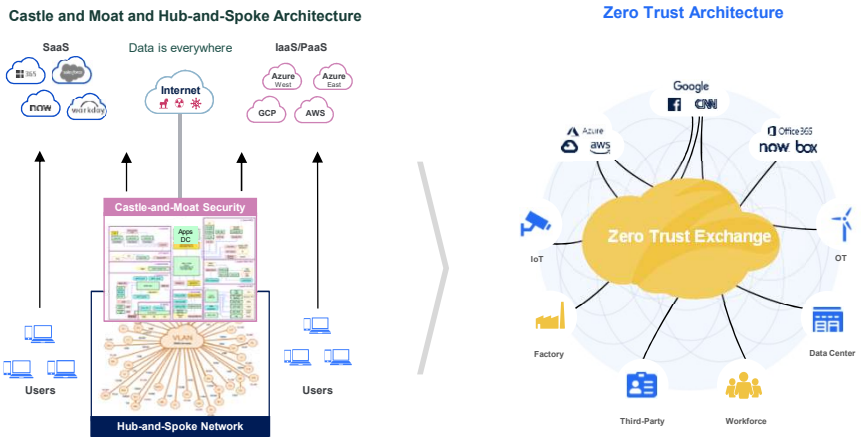
Enforce – in detail

Policy Actions
Conditional Allow
Warn: Alert users of potential risk, policy violation
Prioritize / Deprioritize: Salesforce gets priority over YouTube when last mile is congested
Isolate: Stream pixels to the browser, restricts the ability to download, copy and paste data
Steer: Optimal and pre-defined path selection
Quarantine: Ensure access is limited and protected
Conditional Block
Quarantine: Ensure access is stopped and assessed
Deceive: Direct any malicious attack to restricted decoy

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

Why the control plane needed a redesign



What is the added value?

- Open discussion…

Zscaler Technical Update
25. Januar 2023

What Zscaler Products exists for?

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)

Zscaler Private Access (ZPA)

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

Cloud and Branch Connector

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

Zscaler Workload Segmentation (ZWS)

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

Zscaler Deception

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

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

Open round

AVANTEC
Competence. Security. Trust.

- Open discussion…

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

AVANTEC
Competence. Security. Trust.