



In sieben Schritten zu einer echten Zero-Trust Architektur

Michael Schumak, Partner Consulting Sales Engineer - Zscaler
Henning Dey, Security Architect – Serviceware SE
it-sa 2023

Empowering your business to be more competitive



Secure

Reduce Business Risk



Superior Threat Protection
Unmatched Data Protection
Unprecedented Risk Insights

Simplify

Eliminate Cost and Complexity



Consolidation
Standardization
Automation

Transform

Increase Business Agility



Improve Business Productivity
Accelerate Innovation
M&A Time to Value



“It’s a rare occasion in history where it got **more secure**,
provided a better experience and got cheaper all at once.”

Proof of Value

Secure

Reduce Business Risk

35x Fewer infected machines



Simplify

Eliminate Cost and Complexity

70% Infrastructure Cost reduction



Transform

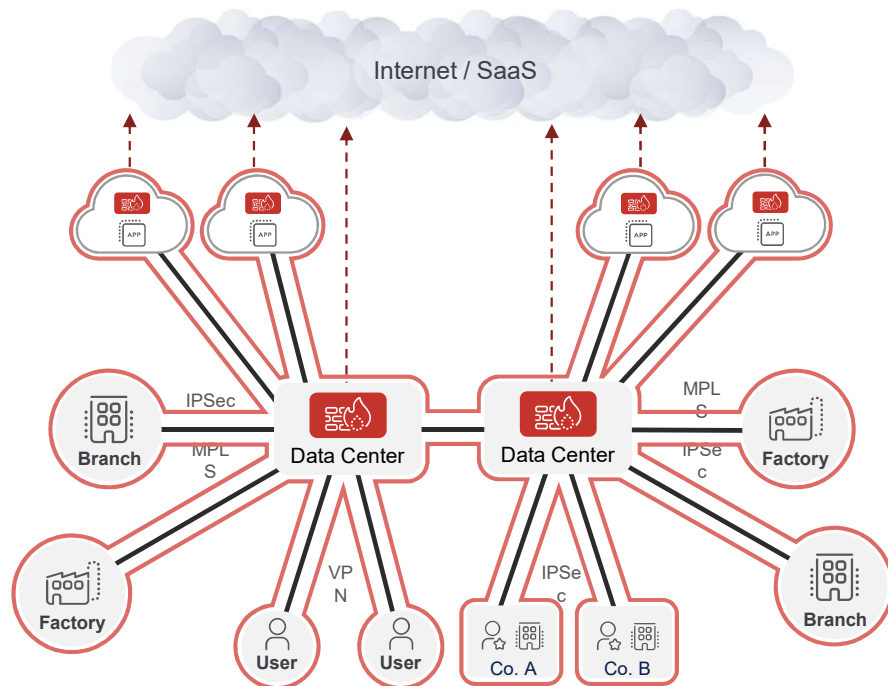
Increase Business Agility

1 Day to onboard M&A users



Digital Transformation Requires a Zero Trust Architecture

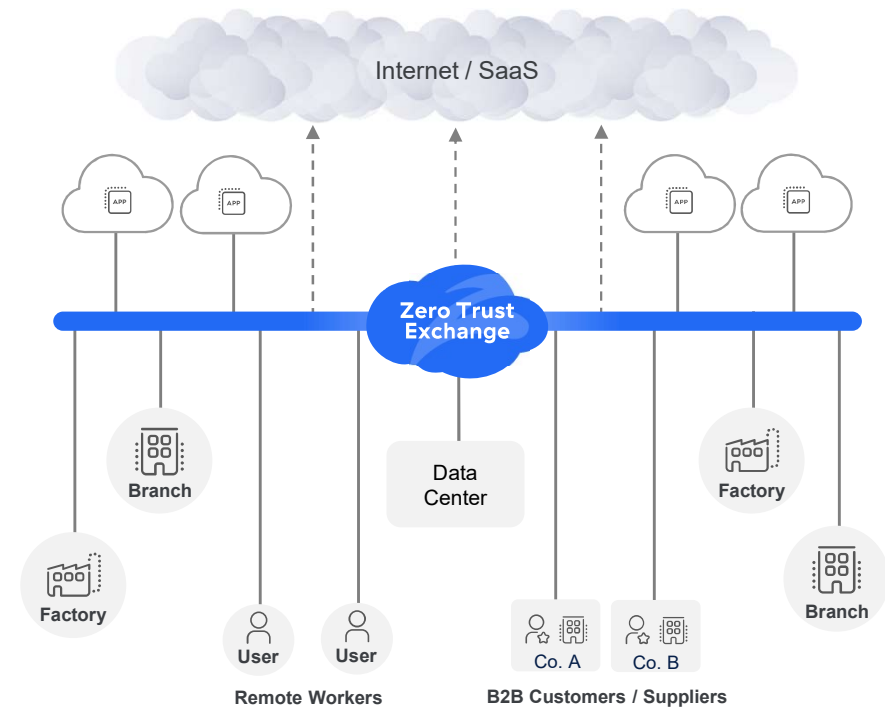
Network & Firewall-centric Architecture



A trusted network connects users, sites and apps
Secure the network for threat and data protection

Rigid, Complex and a Security Risk
Barrier to Transformation

Zero Trust Architecture



Business policies determine who can access
what over any network, the network is transport

Agile, Simple and Secure
Enables Transformation

Two Opposing
Architectures

Zscaler: The Industry's Largest Inline Security Cloud

150 Zero Trust Exchanges
Worldwide

300B+ Requests
processed/day

500T Daily Signals

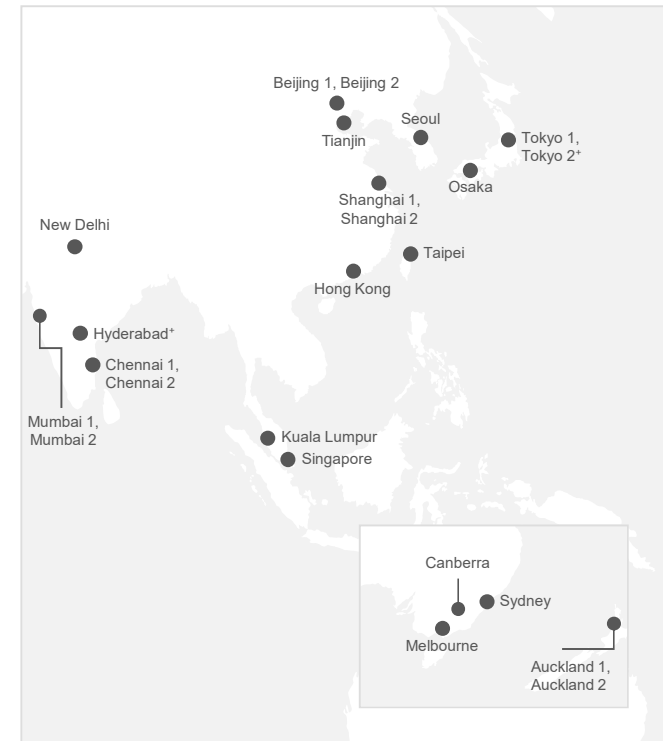
AMERICAS



EUROPE, MIDDLE EAST and AFRICA



ASIA-PACIFIC



*Coming soon.

Delivers exceptional user experience, reliability, and security

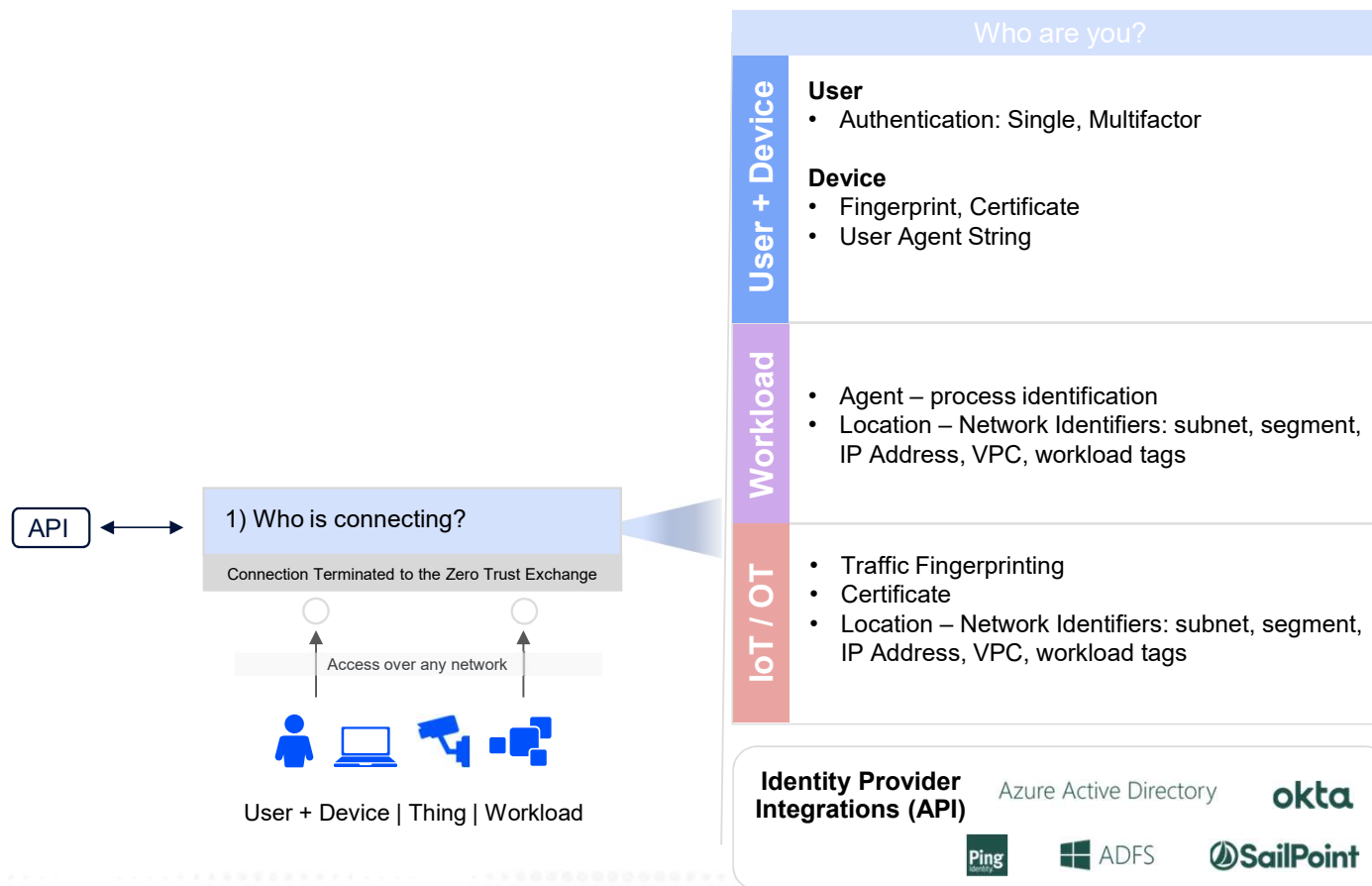


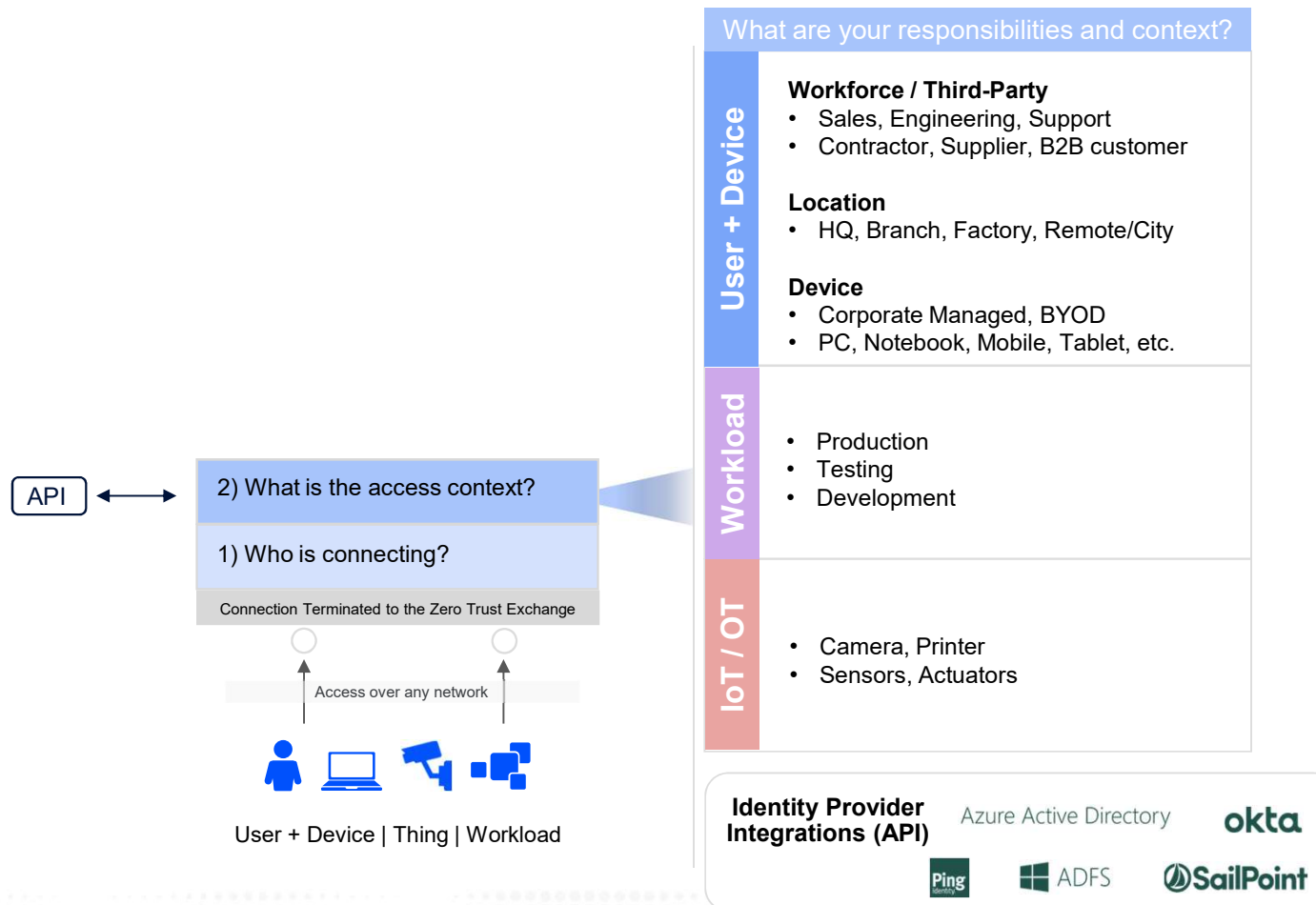
7 Elements Of Zero Trust Policy Application

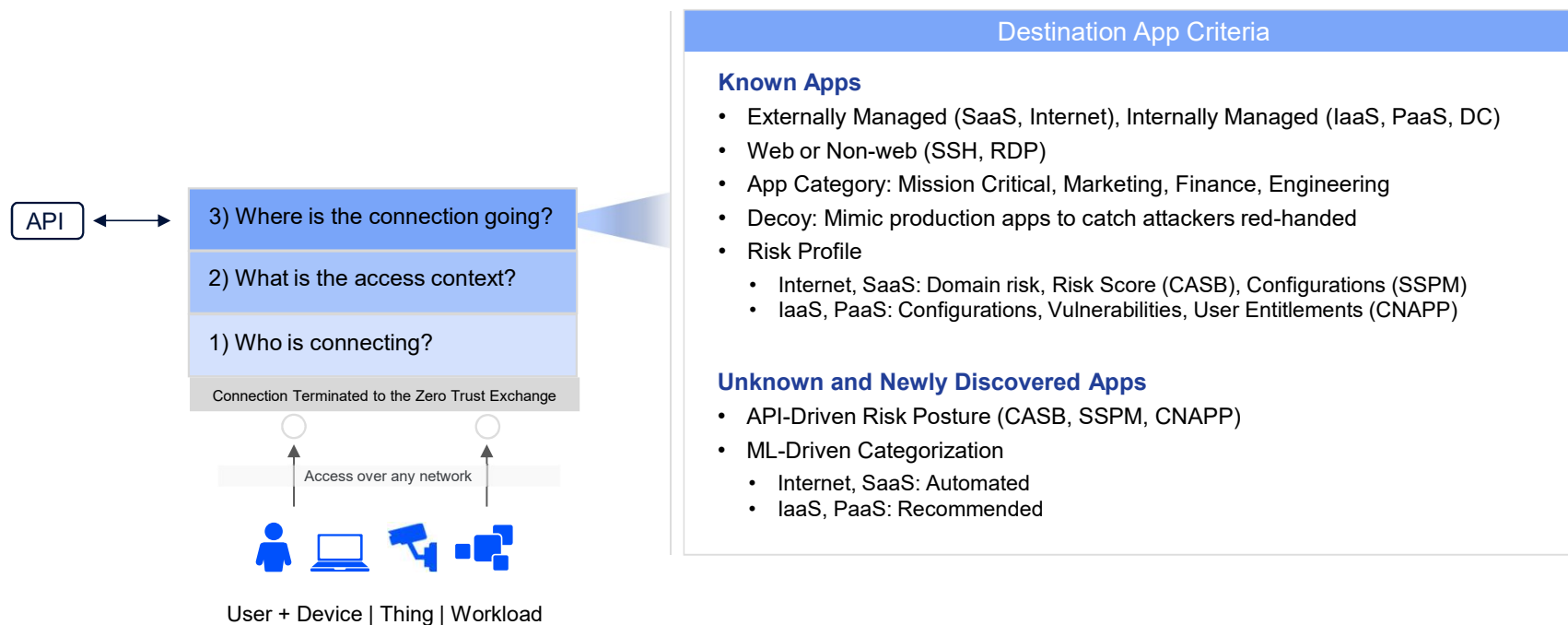


Verify

Verify Identity and Context



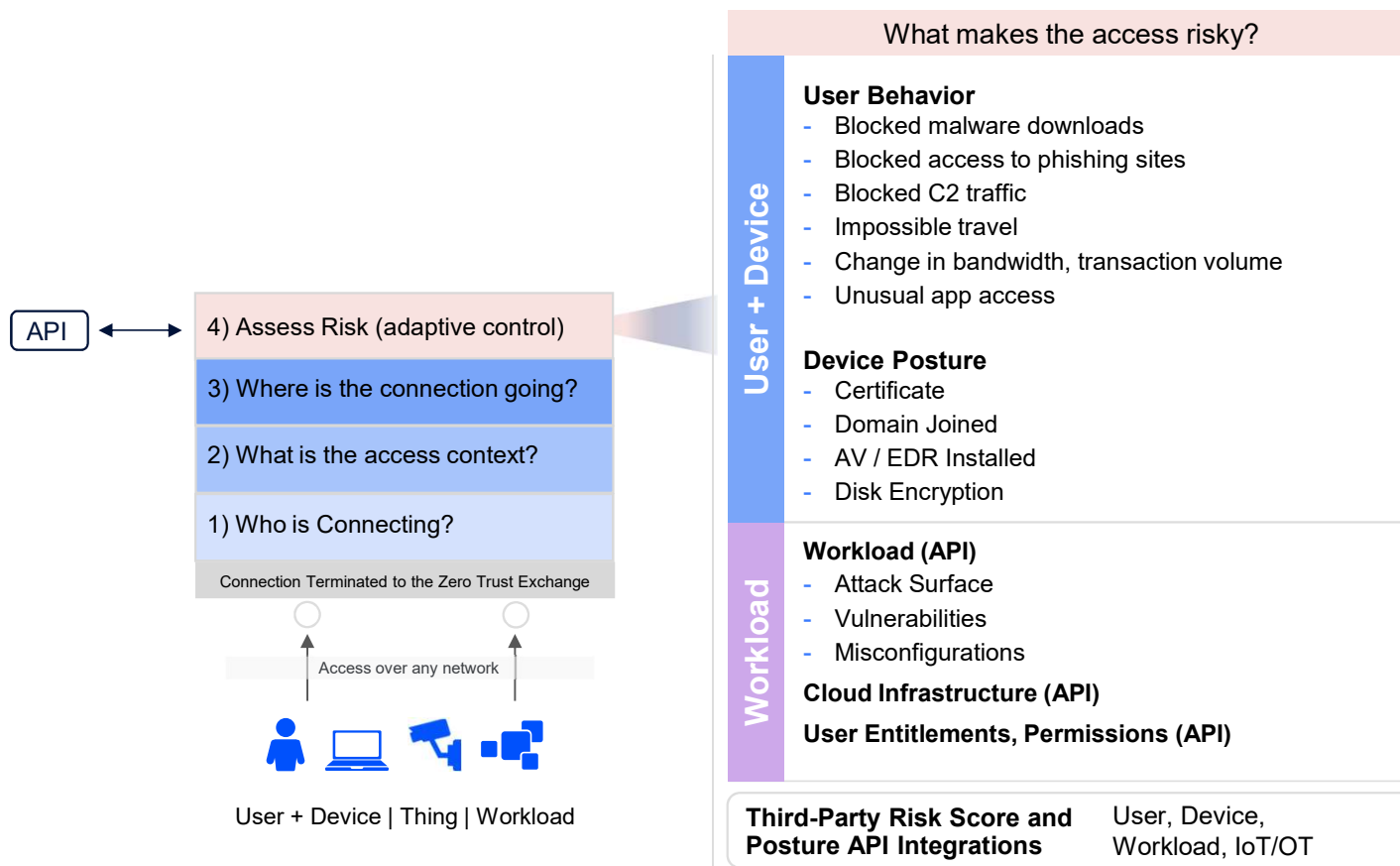


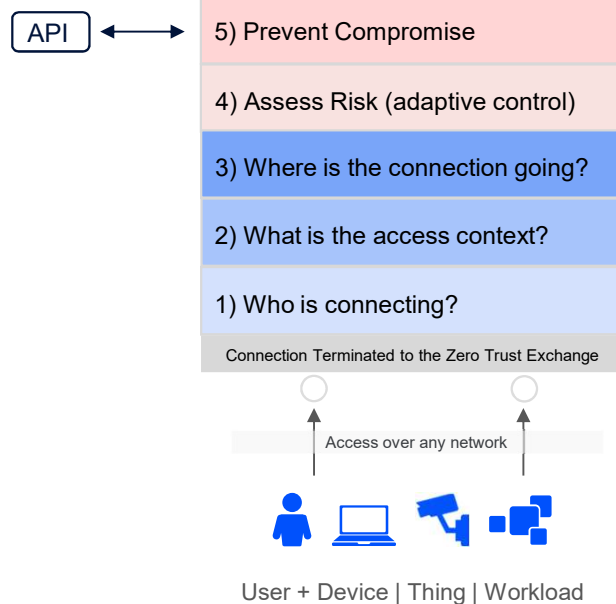




Control

Risk, Control and Access





Are you carrying anything bad?

Inline Threat Protection

Block the Known Bad

- Pattern
- Signature
- Destination

Quantify the Unknown

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

Continuous Updates

250,000 unique security updates every day

Cloud Effect

Once a new threat is identified, it's blocked for all

Out-of-Band Threat Protection (API Scanning)

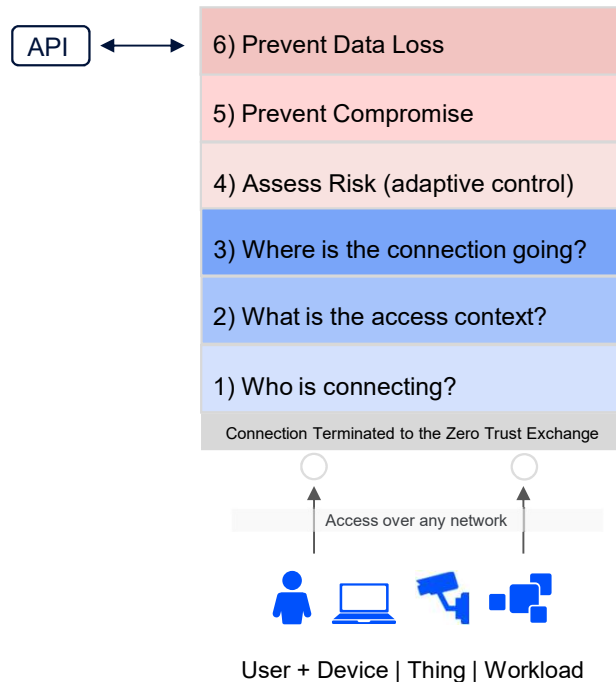
Discover Malware in SaaS, PaaS, IaaS

- API scanning for malware
- Sandbox unknown, suspicious files

Common Platform Services

Third-Party API Integrations
Threat Intelligence

40+ threat feeds
Endpoints: CrowdStrike, Microsoft, etc.



Are you carrying stolen goods?

Inline Data Protection

Data Loss Prevention

AI-Driven Inspection

- predefined, custom dictionaries
- advanced classification: EDM, IDM, OCR
- enforce Microsoft AIP tags

Inline CASB

Control Access, Usage

- tens of thousands of defined apps
- 25 risk attributes per app

File Type Controls

Control File Transfers

- file type, bandwidth, time-of-day controls

Inspect all destinations, except Healthcare and Finance

Block risky/unsanctioned apps
Allow IM chat, block file transfers

Block personally encrypted files

Out-of-Band Data Protection (API Scanning)

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

Common Platform Services

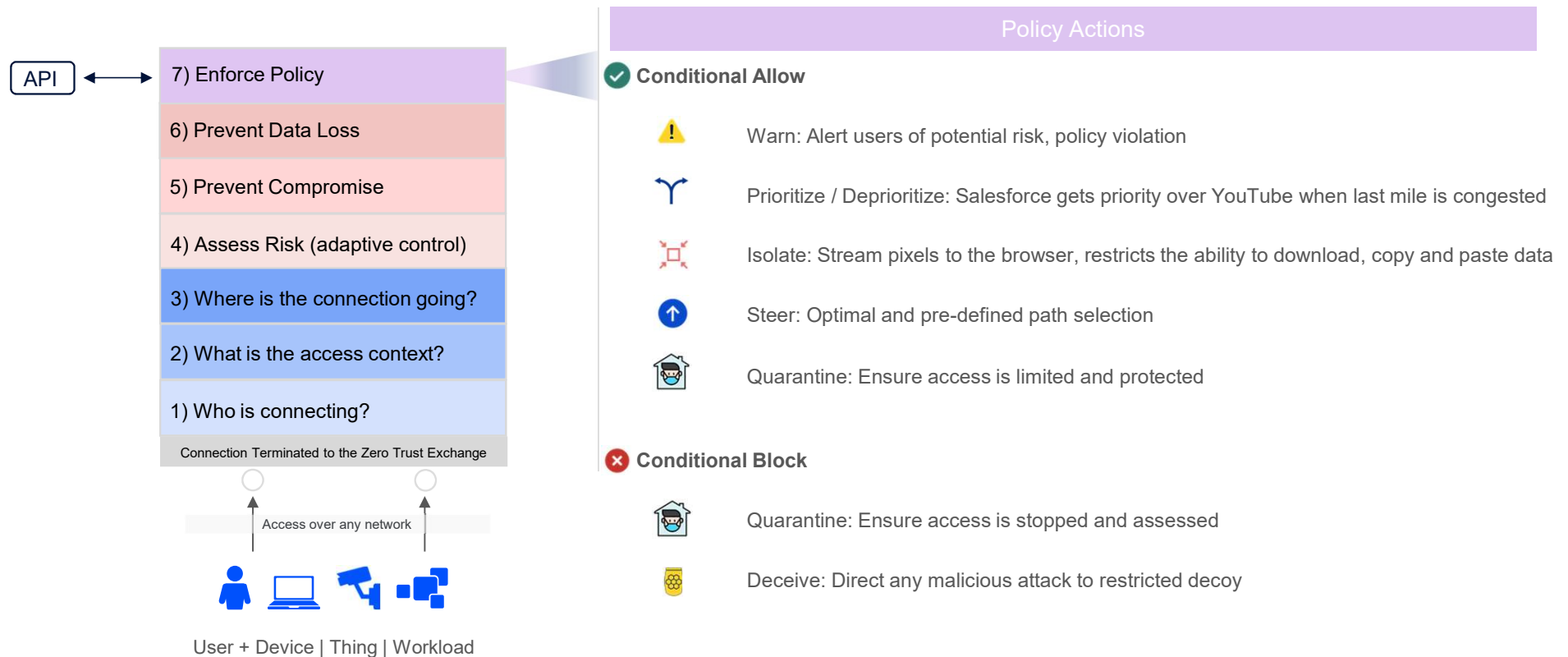
Third-Party API Integrations
Data Protection

Microsoft Information Protection
ICAP for Third-Party DLP Products



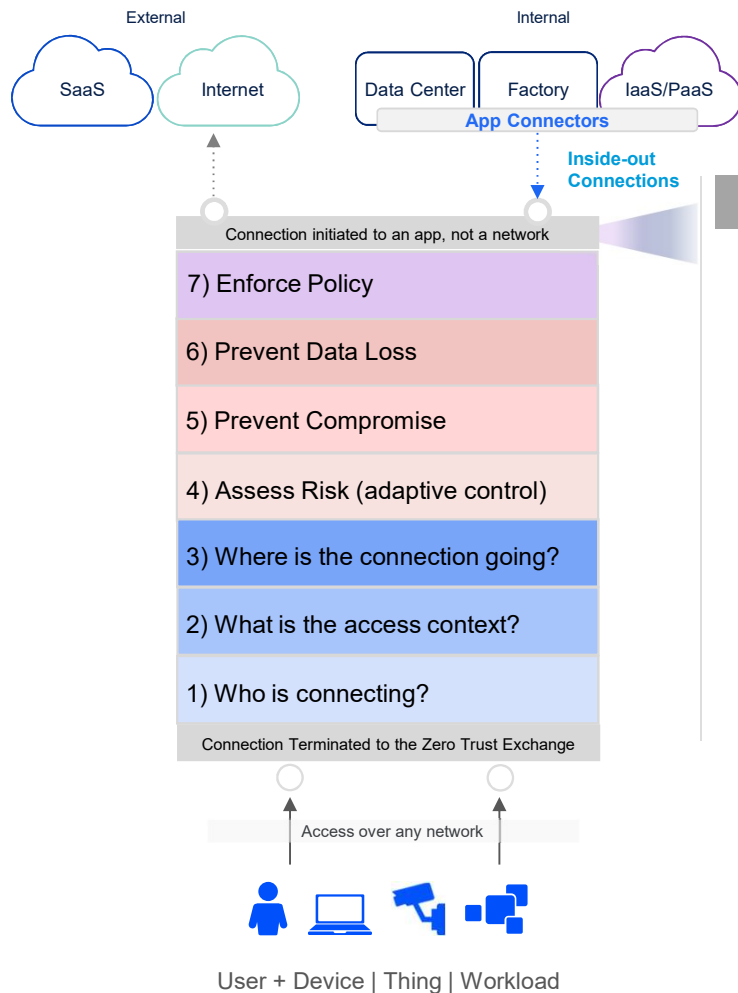
Enforce

Policy





Connect



Connecting to Apps

Externally Managed Apps (Internet, SaaS)

- A new session established to the app on behalf of the user, device, IoT/OT or Workload (proxy)
- The requester remains anonymous – protection against watering hole attacks

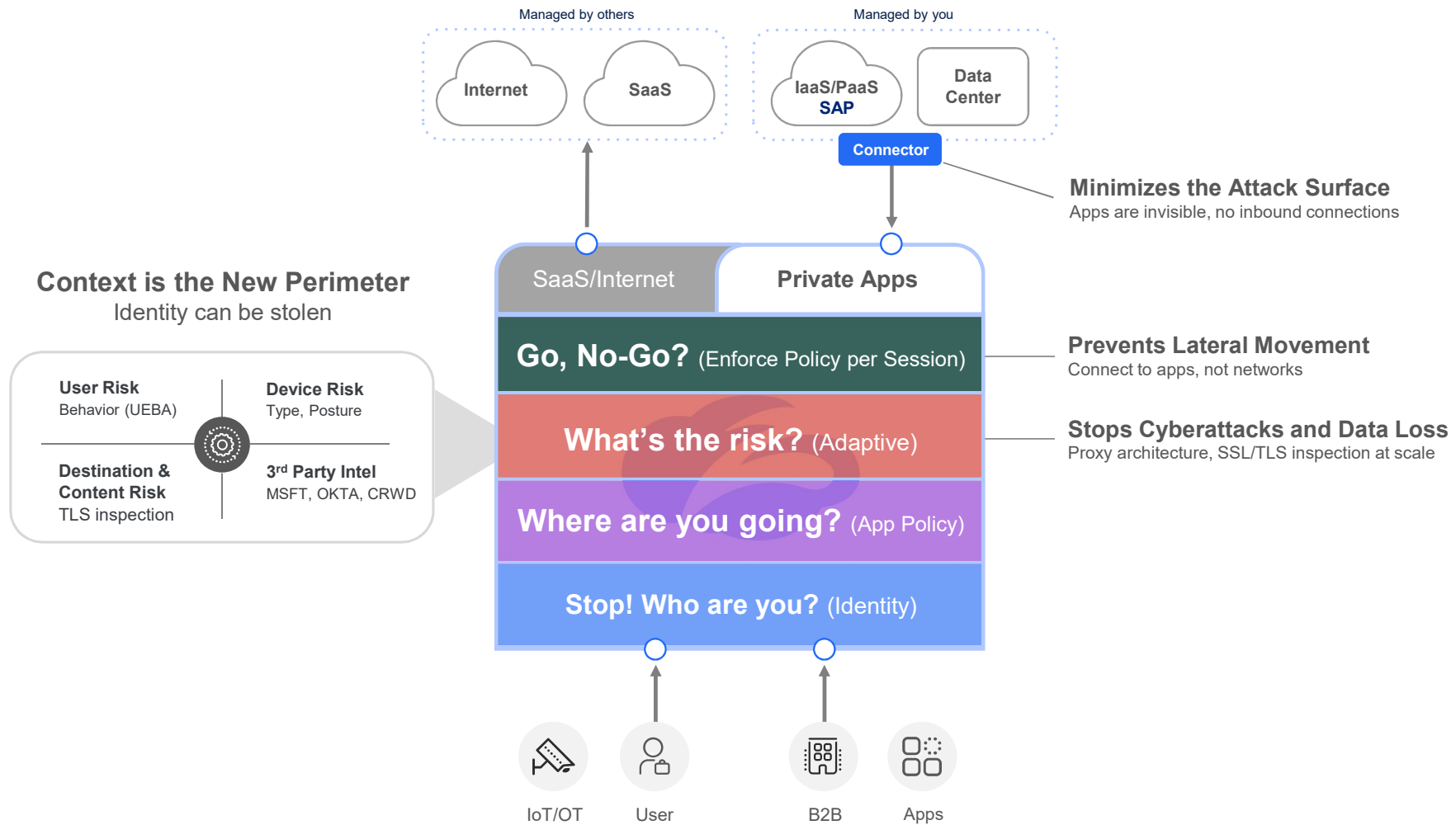
Internally Managed Apps (DC, IaaS, PaaS)

- Apps are treated as destinations, not network resources (like SaaS apps)
- Apps are invisible (sit behind Zscaler controls) and can't be discovered from unauthorized sources (Internet or connected networks)
- Inside-out connections only, no inbound connections to apps (eliminates the attack surface)
- Connections are made to apps, not networks (prevents lateral threat movement)
- App / Workload segmentation without network segmentation
 - User + Device to App
 - IoT / OT to App
 - Workload to Workload
 - Identity based microsegmentation (process-level)



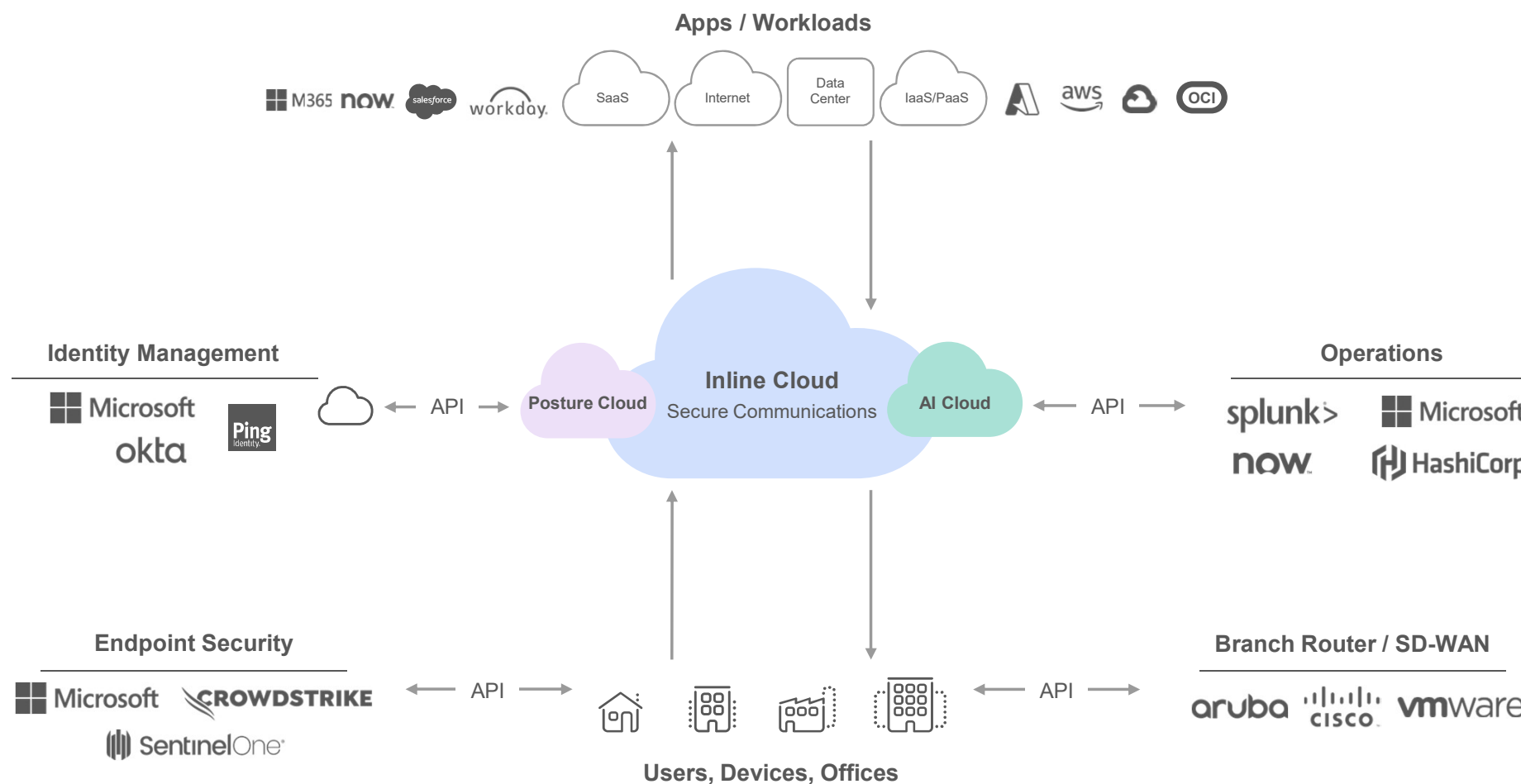
Connecting the Dots

Zscaler Zero Trust Exchange Architecture



You can't do Zero Trust with Firewalls/VPN

Best of Breed Platforms to Implement Zero Trust



Validated integrations accelerate deployment, reduce risk and operational overhead

Customer Zero Trust Journey

Example of a Common Phased Journey

Varies based on customer requirements

Phase 1

Secure the Workforce, all Locations

- Secure Internet & SaaS Access
- Secure Private App Access
- Zero Trust Branch Connectivity
- Digital User Experience
- Deception

Phase 2

Prevent Data Loss

- Secure SaaS Data (SSPM/CASB)
- Internet DLP
- Email DLP
- Endpoint DLP

Phase 3

Secure Cloud Workloads

- Posture Control (CNAPP)
- ZIA for Workloads
- ZPA for Workloads
- Zero Trust Cloud Connectivity

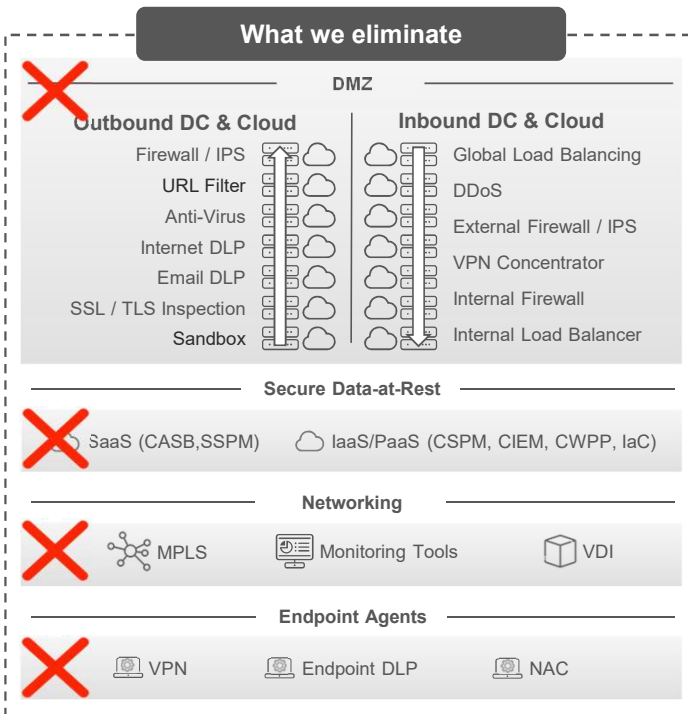
Phase 4

Secure B2B Customers and Suppliers

- Secure App Portal Access; no legacy DDoS, Firewalls
- Site-to-Site Connectivity, without site-to-site VPN

The sequence of journey phases varies from customer to customer

Zscaler Delivers a Strong ROI



ROI for a 10K User Company

Product Savings

Eliminate point products

Data Center DMZ: Inbound & Outbound
Cloud Gateway: Virtual DMZ / VPN
Secure Data-at-Rest

\$1.14M

Operational Savings

DMZ Management
Network Simplification
Automation

\$1.3M

Network Savings

MPLS Savings
Networking Products
Monitoring Tools

1.2M

Risk Reduction

Business Disruption
Data Protection
Brand Reputation

\$2.6M

Improved Agility and Productivity

Innovation
User Experience
M&A/ Divestitures

\$550K

Subtotal - Benefits

\$6.8M



Next Steps

Besuchen Sie uns am Stand der Serveware
Halle 7 / Stand 436
für weitere Informationen oder Demo

