



Belden Industrial Network Solutions

NAC Use Cases in OT-Umgebungen

Michael Reinholz

Presales & Consulting | macmon secure GmbH



NAC Use Cases in OT-Umgebungen

ENTDECKEN
SIE ALLE

FACTORY OF ZTNA

USE CASES

nac 

sdp 

 HALL 3

Jetzt auf:  macmon.eu/ztna-factory

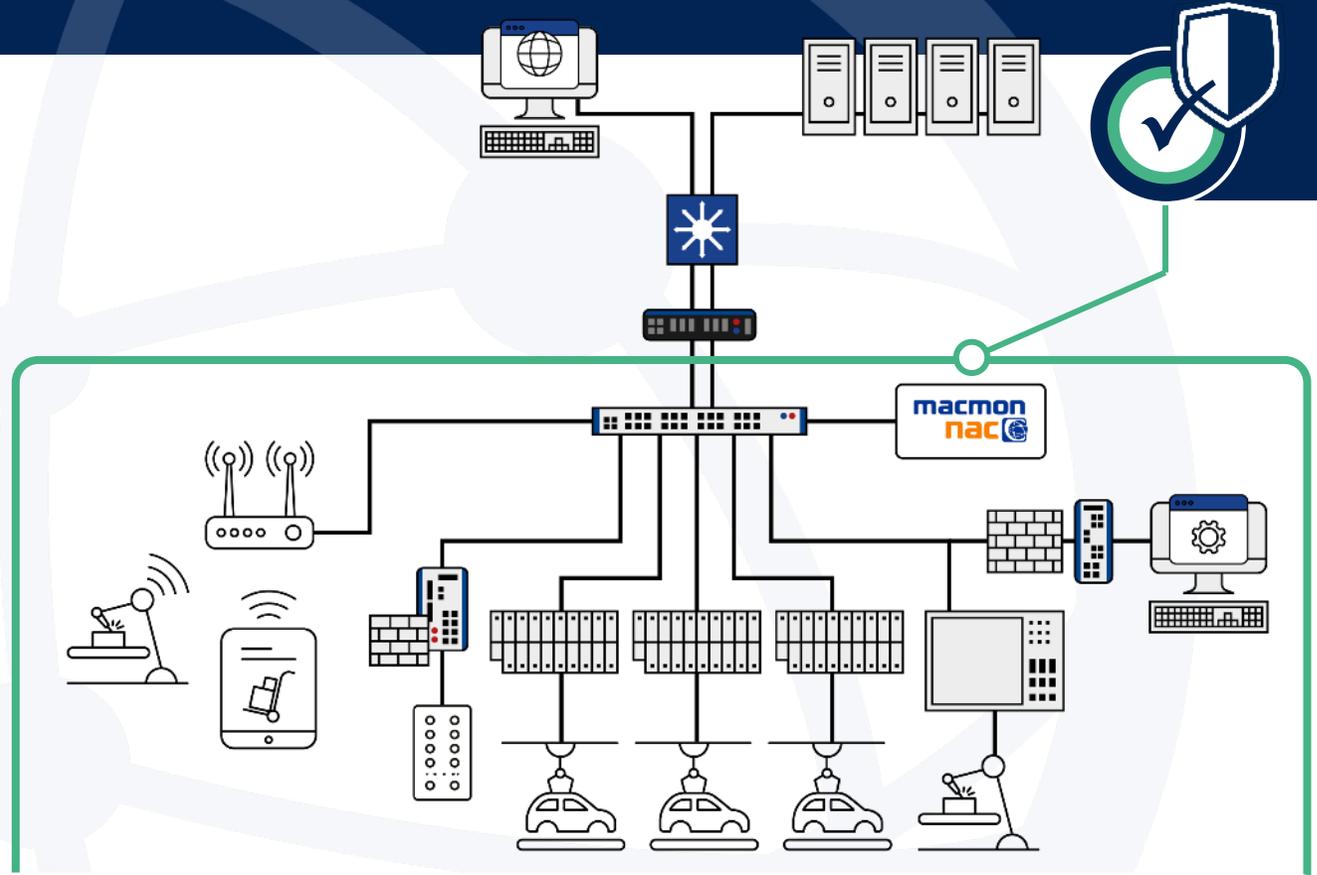


NAC als essentieller Baustein für die Sicherheit von Industrieanlagen



Eine moderne NAC-Lösung ist ein Schlüsselement bei der Umsetzung von Sicherheitskonzepten im industriellen Umfeld

NAC ergänzt bestehende Cybersicherheitsrichtlinien



NAC bietet mehr Granularität

als herkömmliche Firewall-Ansätze



NAC ist Mikro

während Firewall / ACL Macro ist



NAC schützt auf der Ebene der physischen Port-Verbindungen



Network Access Control – NAC

Die Erfüllung diverser Vorgaben und Anforderungen

Datenschutz-Grundverordnung (DSGVO)

DIN EN 80001-1

Payment Card Industry Compliance (PCI)

ISO IT Sicherheitsstandard gemäß IEC 27001/27002

Audits (z. B. TISAX®)

Genehmigungsverfahren für IT-Komponenten:

Maßnahme 2.216

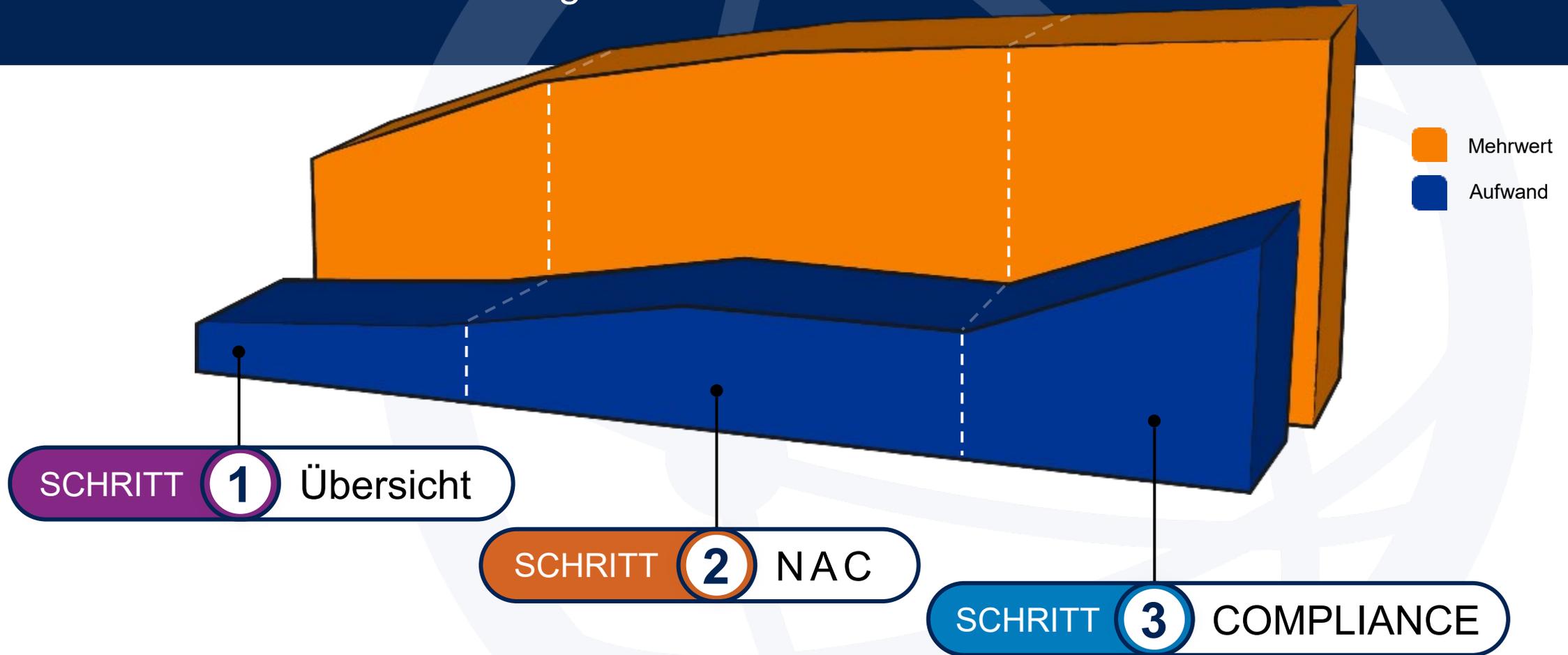
„Die Installation und Benutzung nicht freigegebener IT-Komponenten muss verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.“



BSI IT-Grundschutz-Kompendium

Network Access Control – NAC

Drei Schritte der Umsetzung



DASHBOARD



macmon nac Dashboard (sales demo)

Individuell anpassbares Dashboard für jeden Benutzer

Anzeige aller Aktivitäten und Bewegungen im Netzwerk

Direkter Zugriff auf alle Funktionen und Menüs

Dashboard (sales demo)

Unautorisierte Endgeräte 11 / 13 11 online/13 insgesamt Netzwerkgeräte-Vorschläge 16 Nicht konfigurierte Nachbar-Netzwerkgerä...

Gesperrte Interfaces (auto) 0 Automatisch gesperrte Interfaces (letzte 7... Lizenz 479/1000 Lizenznehmer: macmon secure GmbH

Dauerhaft gesperrte Interfaces 0 Automatisch dauerhaft gesperrte Interface... DNS-ZoneLoad 1 Fehlgeschlagene Zonenübertragungen: 1

Systemstatus Performance

Status	Objekt	Wert	Details
OK	macmon-Engine	9	
OK	Speicherverbrauch der Engine		
OK	Festplatte (frei)		
OK	Speicher		

Status	Objekt	Wert	Details
OK	Scangeschwindigkeit	27/m	Anzahl der gesendeten Netzwerkpakete...
OK	Scannvorgang	242us (34ms)	Durchschnittliche Netz...
OK		0	Anzahl der aktuell gesch...
OK	angröße	0	Warteschlangenlänge der macmon-Engine

1 ÜBERSICHT → Topologie

2 NAC → Network Access Control

3 COMPLIANCE → 3rd Party Solutions

ENDGERÄTE

BENUTZER

NETZWERK

RICHTLINIEN

BERICHTE

PAST VIEWER

SKALIERBARKEIT

STATISTIKEN

STATUS

EINSTELLUNGEN

TOPOLOGIE

macmon nac Topologie anzeigen (sales demo)

Suche

Netzwerkgerät
IP-Adresse
Gruppe
Status
Standort

- Netzwerkgerät
- Netzwerkgerät-IP
- Netzwerkgerätegruppe
- Beschreibung
- Standort
- VLANS
- Alle



Grafische Übersicht aller Netzwerkgeräte

1 ÜBERSICHT → Topologie

2 NAC → Network Access Control

3 COMPLIANCE → 3rd Party Solutions



Live-Bestandsmanagement aller Endgeräte



Umfassende Berichterstattung über die Überwachungsdaten



Umfangreiche Analysemöglichkeiten

TOPOLOGIE



Finden Sie heraus, was in Ihrem Netzwerk los ist ...



EIN UFO WURDE ENTDECKT

Hirschmann-SPIDER-PL

40-04T1069999TY9HHHH Industrial-Ethernet-Switch



1 ÜBERSICHT → Topologie

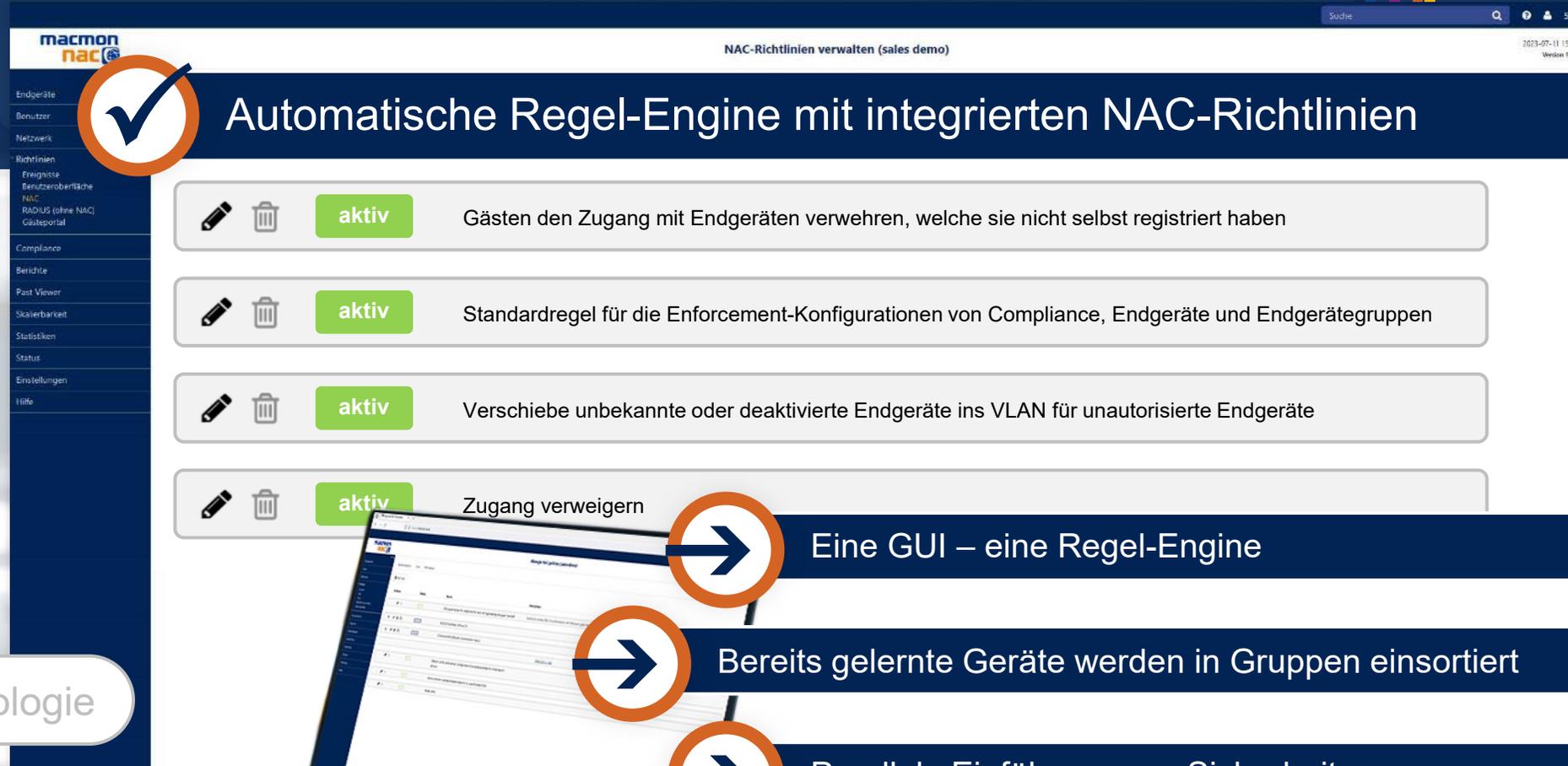
2 NAC → Network Access Control

3 COMPLIANCE → 3rd Party Solutions



... und entdecken Sie Unbekannte, Fremde Objekte

NAC RICHTLINIE



macmon nac

NAC-Richtlinien verwalten (sales demo)

2023-07-11 15:...

Endgeräte
Benutzer
Netzwerk
Richtlinien
Ereignisse
Benutzeroberfläche
NAC
RADIUS (ohne NAC)
Guestportal
Compliance
Berichte
Post Viewer
Skalierbarkeit
Statistiken
Status
Einstellungen
Hilfe

aktiv Gästen den Zugang mit Endgeräten verwehren, welche sie nicht selbst registriert haben

aktiv Standardregel für die Enforcement-Konfigurationen von Compliance, Endgeräte und Endgerätegruppen

aktiv Verschiebe unbekannte oder deaktivierte Endgeräte ins VLAN für unautorisierte Endgeräte

aktiv Zugang verweigern



Automatische Regel-Engine mit integrierten NAC-Richtlinien

1 ÜBERSICHT → Topologie

2 NAC → Network Access Control

3 COMPLIANCE → 3rd Party Solutions



Eine GUI – eine Regel-Engine



Bereits gelernte Geräte werden in Gruppen einsortiert



Parallele Einführung von Sicherheitszonen



Die integrierten NAC-Regeln decken fast 95% der Anwendungsfälle ab



Zusätzliche Regeln sind nur für Sonderfälle erforderlich



ACCESS CONTROL



VLAN-Konzepte und Sicherheitszonen können einfach umgesetzt werden



1 ÜBERSICHT → Topologie

2 NAC → Network Access Control

3 COMPLIANCE → 3rd Party Solutions



Verschiedene Identitätsquellen

COMPLIANCE



Nicht konforme Geräte können verschoben werden, z. B. In ein Quarantäne-VLAN



Quarantäne VLAN



NONCOMPLIANT



COMPLIANT



COMPLIANT

1 ÜBERSICHT → Topologie

2 NAC → Network Access Control

3 COMPLIANCE → 3rd Party Solutions



Dynamisch



Automatisch



In jeder Umgebung



COMPLIANCE Quellen



Zwei typische OT-Use Cases



Use Case „Wartungsmodus“



Use Case „Flache Netzwerksegmentierung“





Use Case: „Wartungsmodus“



Ein Wechsel zwischen statischem und veränderbarem Betrieb soll möglich sein



Industrielle Netzwerke benötigen **im Normalfall keine Dynamik.**



Veränderungen müssen im Betrieb verhindert werden, sollen aber **im Wartungsfenster** oder **beim Umbau** einfach möglich sein.



Unbetreute Anlagen sollen **nicht verändert** werden können.





Use Case: „Wartungsmodus“



LÖSUNG: Wechsel vom Produktions- in den Wartungsmodus

macmon NAC blockiert neue Endgeräte nur im **Produktionsmodus**, aber akzeptiert sie im **Wartungsmodus**



**NEUE ENDGERÄTE
WERDEN AKZEPTIERT**

Produktions
MODUS



Wartungs
MODUS





Use Case: “Flache Netzwerksegmentierung”



Die Netzwerksegmentierung durch Firewalls ist nicht praktikabel in OT-Netzen



Die Netzwerksegmentierung durch Firewalls ist **komplex** und kann **nicht ohne Unterbrechung** durchgeführt werden.



Viele OT-Netze haben sich **praxisbezogen entwickelt**.



Eine nachträgliche Segmentierung eines gewachsenen, flachen Netzes ist **ohne eine grundlegende Neugestaltung kaum möglich**.





Use Case: “Flache Netzwerksegmentierung”



LÖSUNG: Segmentierung durch NAC an der Netzwerkgrenze

macmon NAC erlaubt die Segmentierung flacher, historisch gewachsener Netzwerkstrukturen auch an der Netzwerkgrenze.



NETZWERK SEGMENTIERUNG



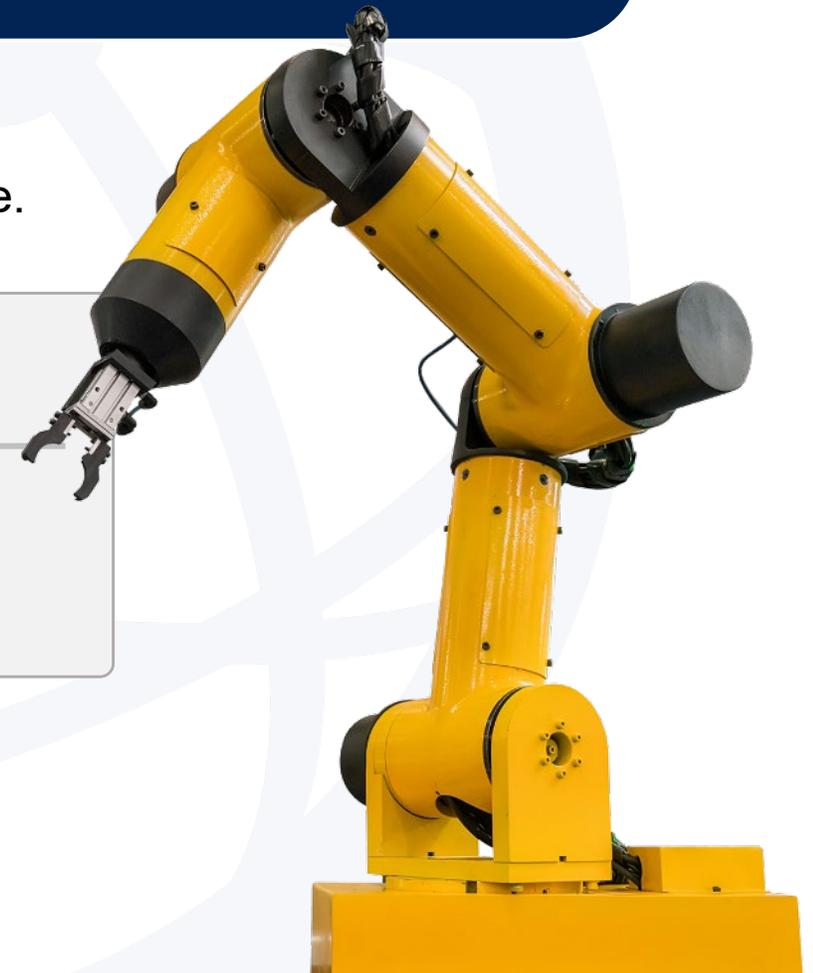
CORE



BORDER



VPN



Scalability



Redundanz-Prinzip

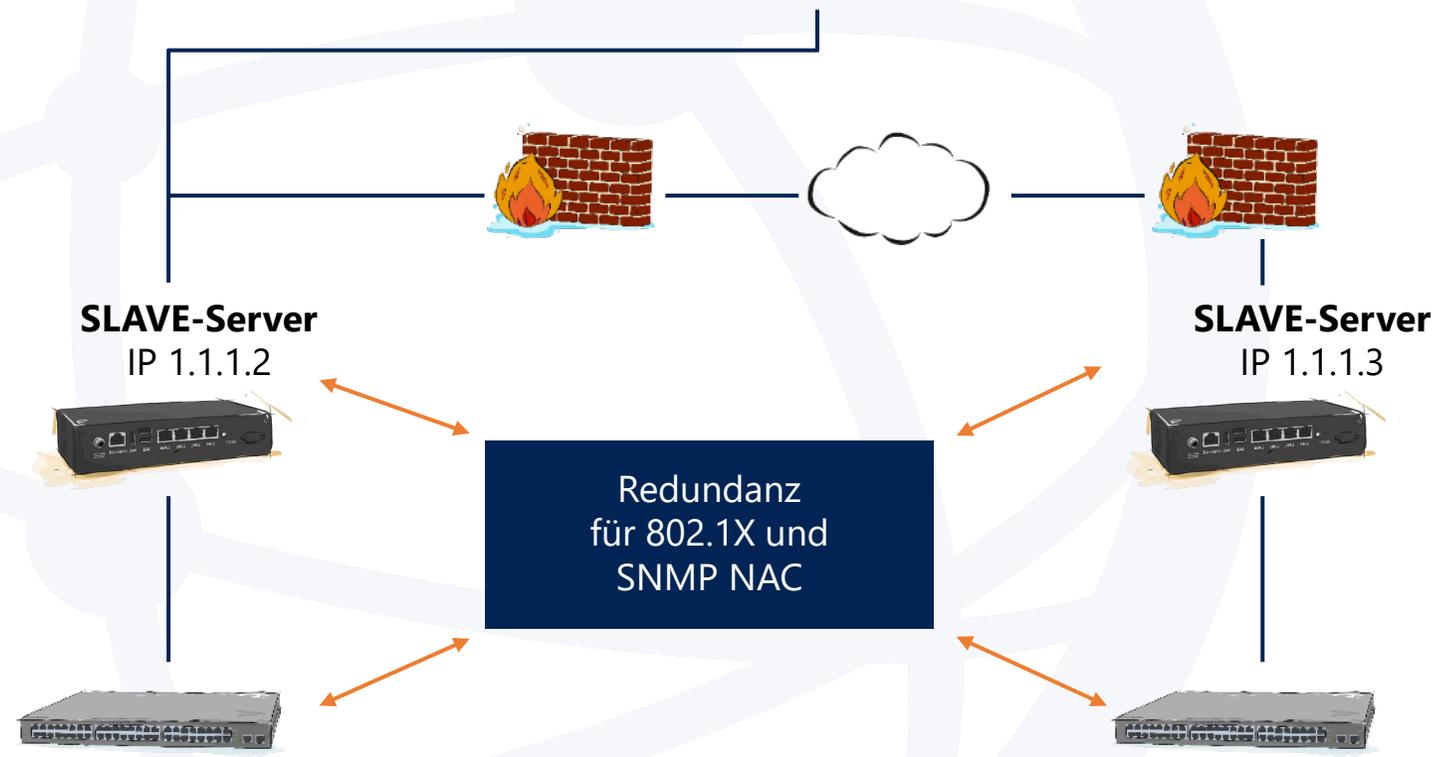


Allgemeine Eigenschaften

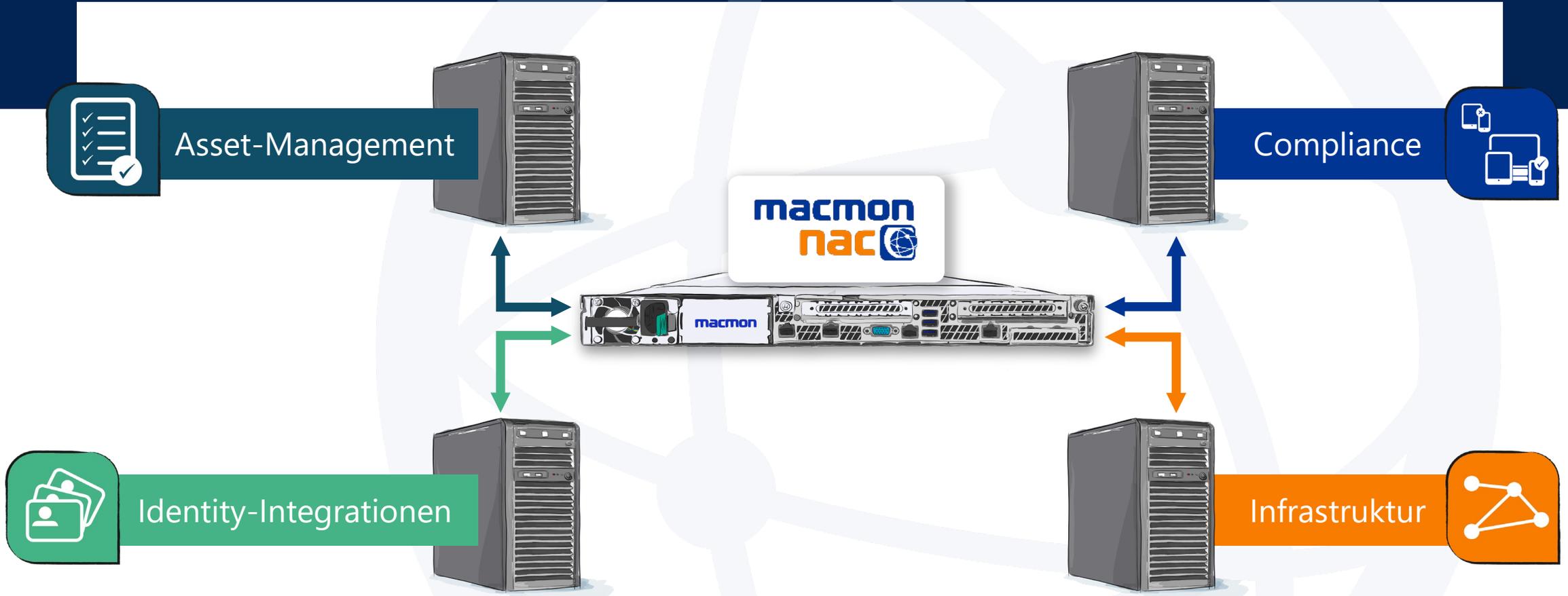
Name	Switch
Elterngruppe	Keine Elterngruppe
Beschreibung	(Layer 2 Switch) MACs
Verwaltender Skalierbarkeitsknoten	salesdemoMASTER
Sekundärer Skalierbarkeitsknoten	salesdemoSATELITE1

Bitte wählen Sie für einen verwaltenden Skalierbarkeitsknoten immer nur den selben sekundären Skalierbarkeitsknoten, damit sichergestellt werden kann, dass die Knoten alle Topologiedaten haben, um das Switch-Link-Verhalten korrekt zu entscheiden.

admin team address: standardadmins@example.local



macmon Technologiepartner & Integrationen





Treffen Sie unsere Security-Experten, hier auf der it-sa



ZERO TRUST NETWORK ACCESS
MAXIMALE IT- UND OT-SECURITY



HALLE 7 | STAND 223