Belden Industrial Network Solutions

NAC Use Cases in OT-Umgebungen

Michael Reinholz

Presales & Consulting | macmon secure GmbH

NAC Use Cases in OT-Umgebungen

Jetzt auf: → macmon.eu/ztna-factory

NAC als essentieller Baustein für die Sicherheit von Industrieanlagen




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

NAC ergänzt bestehende Cybersicherheitsrichtlinien

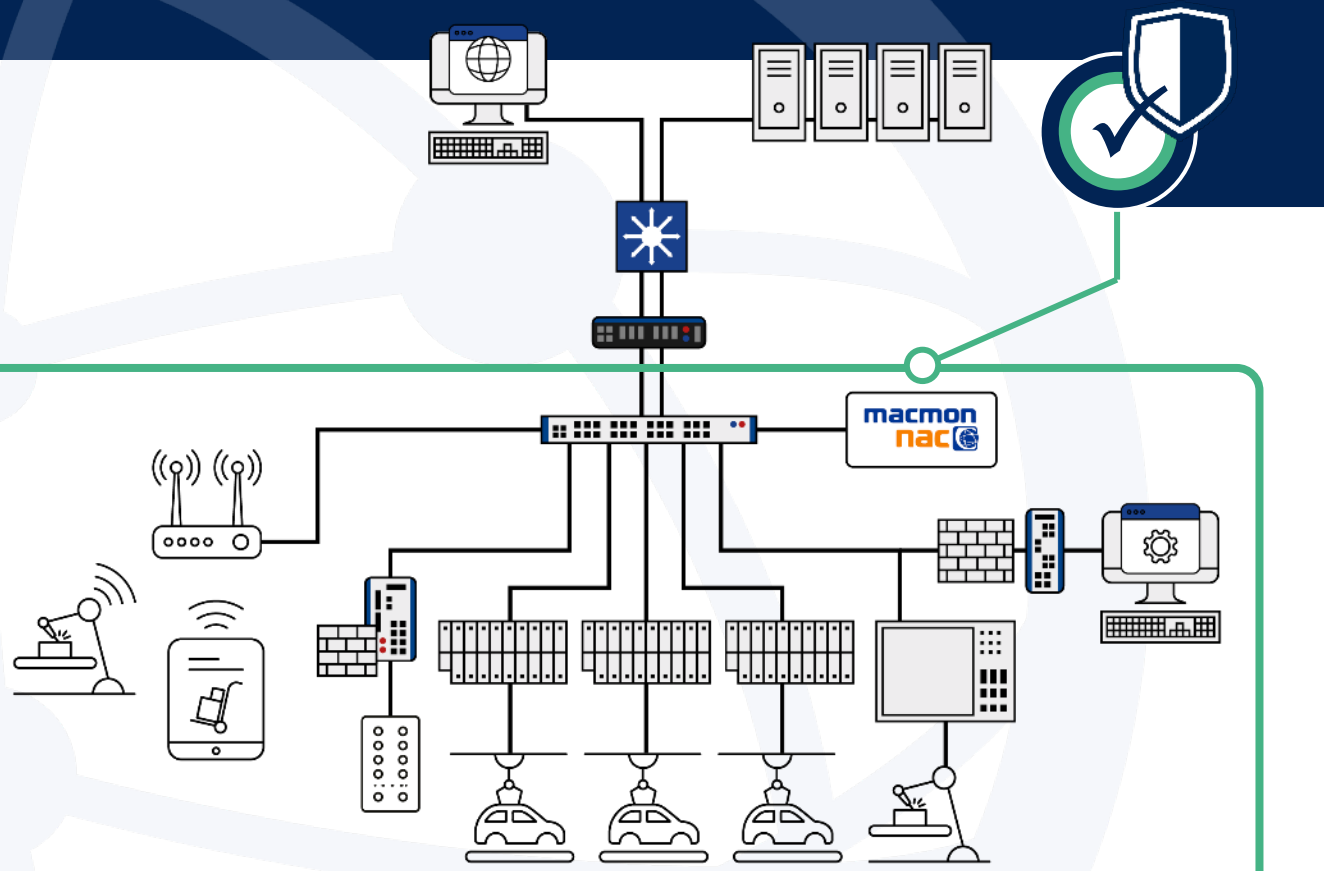
macmon nac

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:

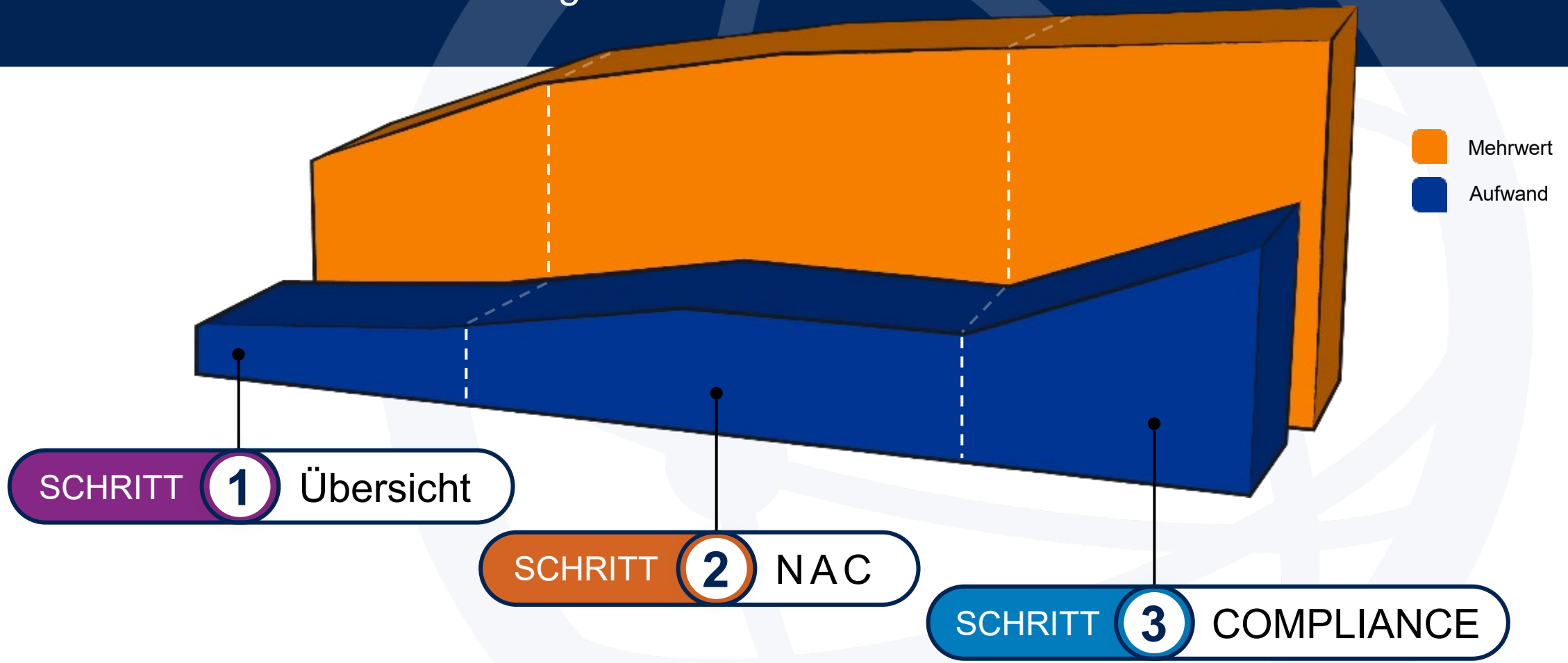
Maßnahme 2.216

„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

Individuell anpassbares Dashboard für jeden Benutzer

Anzeige aller Aktivitäten und Bewegungen im Netzwerk

Direkter Zugriff auf alle Funktionen und Menüs

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

1. ÜBERSICHT → Topologie
2. NAC → Network Access Control
3. COMPLIANCE → 3rd Party Solutions

TOPOLOGIE

Finden Sie heraus, was in Ihrem Netzwerk los ist …

1 ÜBERSICHT → Topologie

2 NAC → Network Access Control

3 COMPLIANCE → 3rd Party Solutions

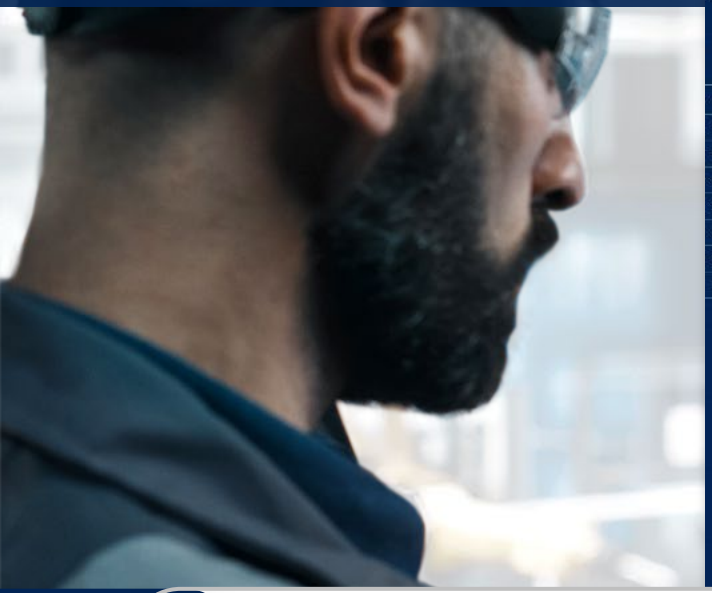
! EIN UFO WURDE ENTDECKT

Hirschmann-SPIDER-PL

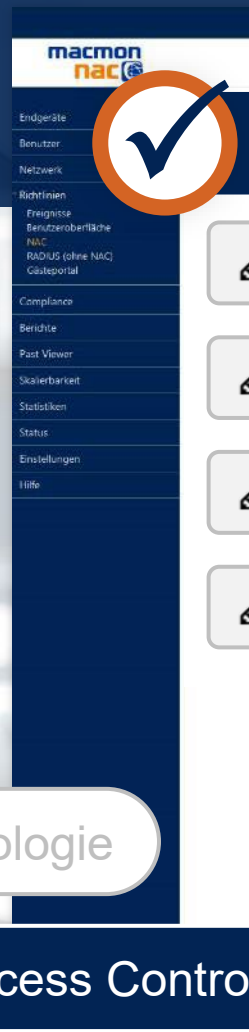
40-04T1O69999TY9HHHH Industrial-Ethernet-Switch

… und entdecken Sie **U**nbekannte, **F**remde **O**bjekte

NAC RICHTLINIE



1. ÜBERSICHT → Topologie
2. NAC → Network Access Control
3. COMPLIANCE → 3rd Party Solutions



Automatische Regel-Engine mit integrierten NAC-Richtlinien

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

- 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

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**

macmon nac

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.

macmon nac

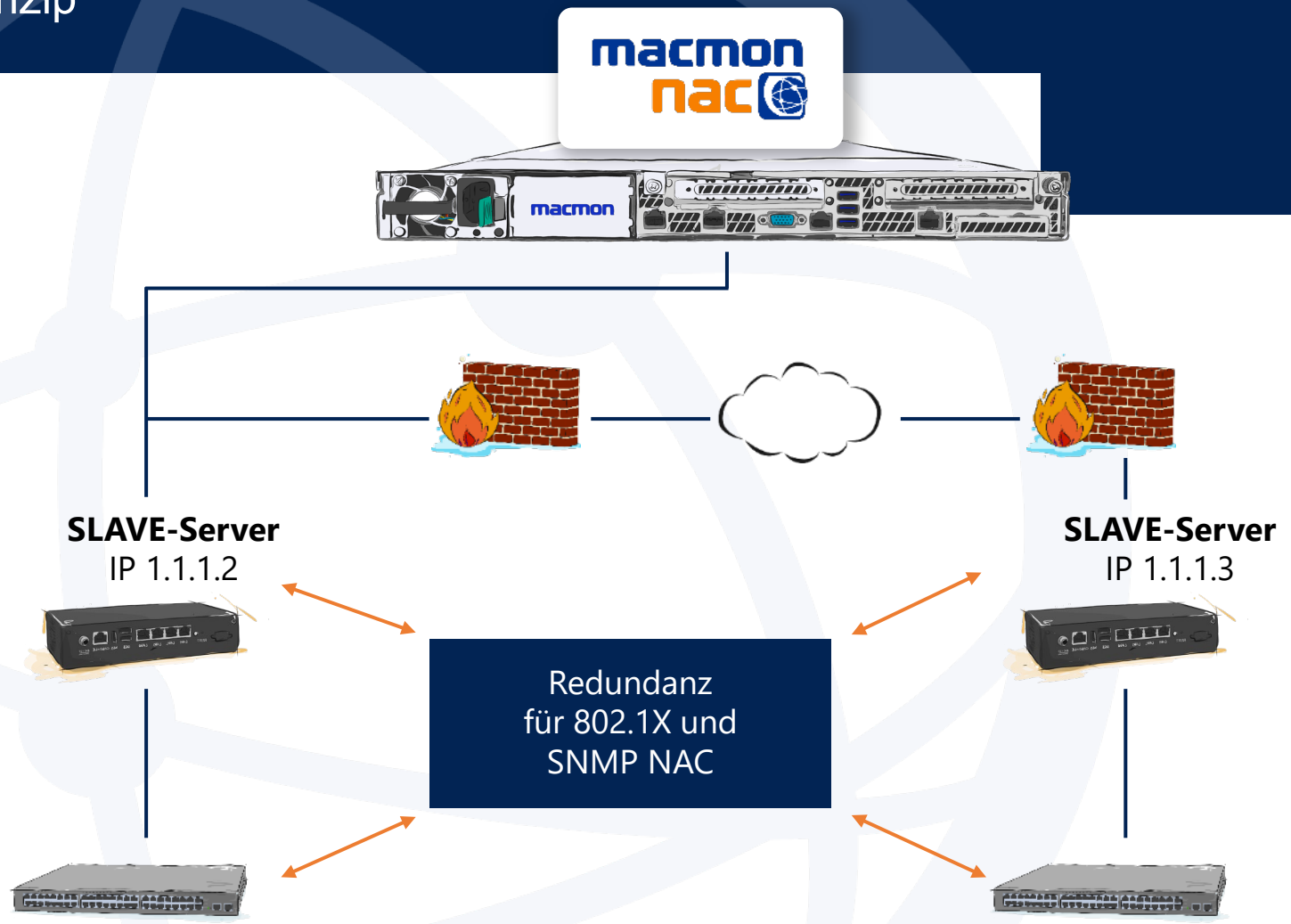
NETZWERK SEGMENTIERUNG

- ○ CORE
- ● BORDER
- ○ VPN

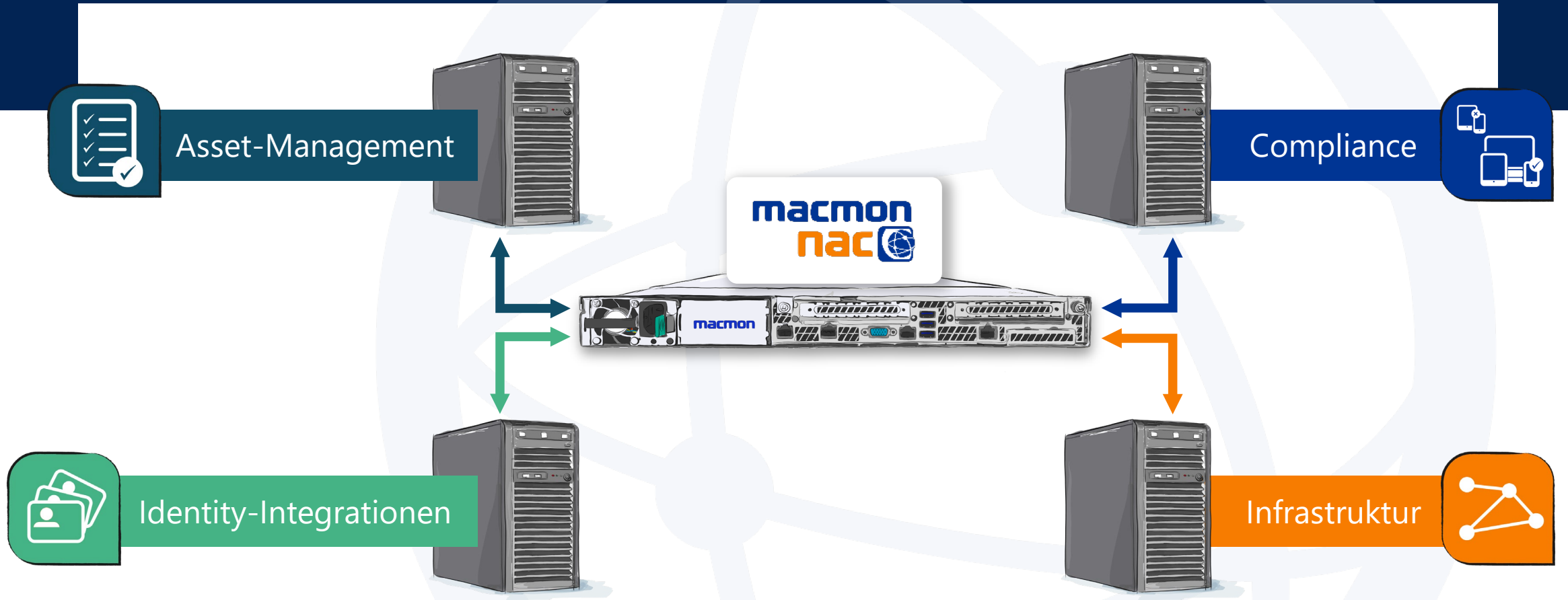
Scalability Redundanz-Prinzip

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