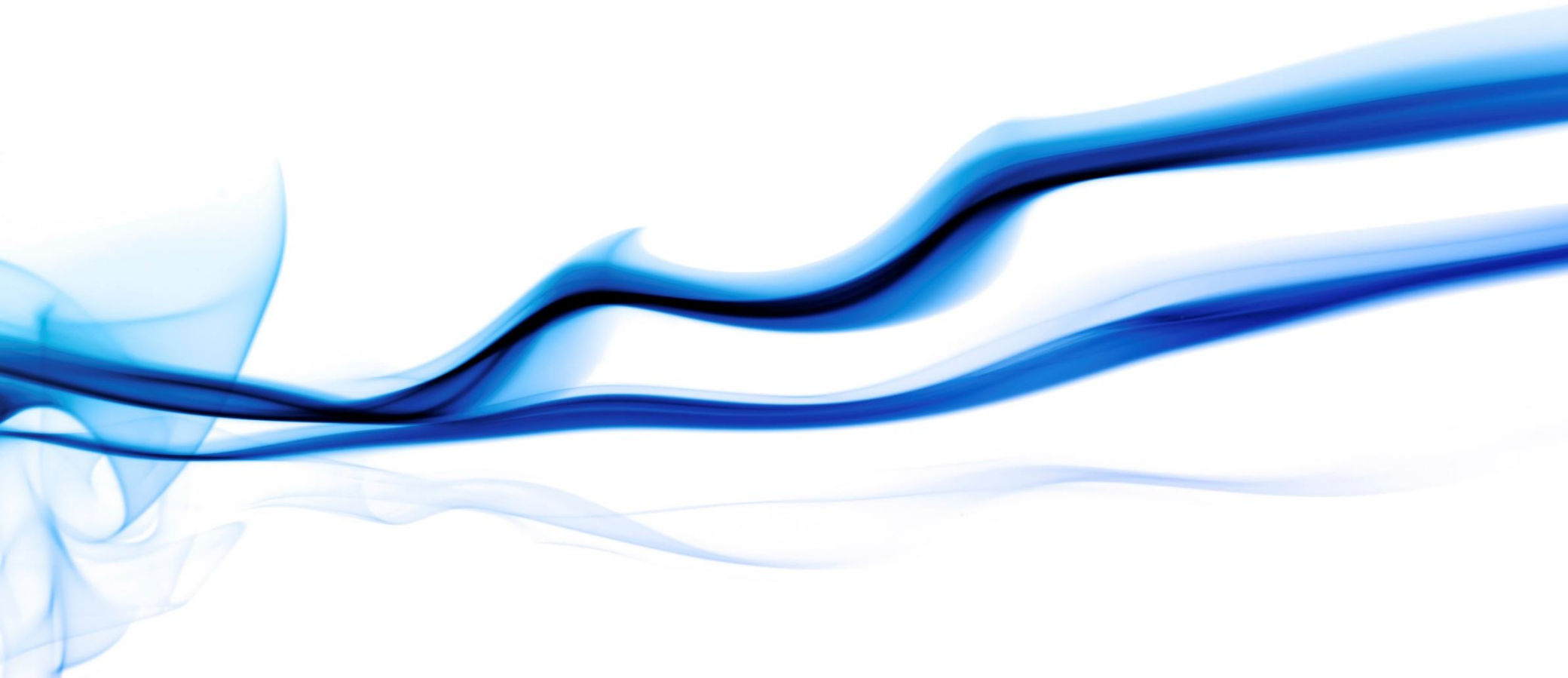
macmon
nac intelligent einfach

„macmon – Wie NAC Angreifern die Tür weist“



macmon secure GmbH

macmon
nac intelligent einfach

Deutscher Hersteller der technologieführenden NAC-Lösung macmon

- Erfahrenes Team mit Entwicklung, Support und Beratung an zentraler Stelle in Berlin
- Entwicklung von Sicherheitstechnologien und -standards
- Kooperation mit Forschungsinstituten und Hochschulen
- Erfahrung aus der Umsetzung von NAC-Projekten mit verschiedensten Branchen und unterschiedlichsten Netzwerkgrößen
- Kooperationen mit weiteren führenden Herstellern von Sicherheitstechnologien
- Mitglied der TRUSTED COMPUTING GROUP

Network Access Control – NAC

macmon
nac intelligent einfach

Sie wissen bereits, was NAC bedeutet!

„… ein alter Hut, der nie richtig passte oder ein unverzichtbarer Sicherheitsbaustein, der einem nebenbei das Leben erleichtert?“

Zielsetzung NAC:

Im Netzwerk betriebene Geräte haben Zugriff auf LAN-Ressourcen,

- ✓ wenn sie für diese zugelassen sind ➡ **NAC**
- ✓ wenn sie den gültigen Sicherheitsstandards genügen ➡ **Compliance**

➡ **Prüfen Sie die angebotene Lösung – was erhalten Sie wirklich?**

Network Access Control – NAC

macmon
nac intelligent einfach

Warum sollten Sie NAC einsetzen ?

- Bundesdatenschutzgesetz (BDSG)
- Sarbanes-Oxley Act
- EuroSox (EU Directive No. 8)
- Basel II
- KonTraG
- MaRisk
- DIN EN 80001-1

BSI IT-Grundschutz-Kataloge

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."

ISO IT Sicherheitsstandard gemäß IEC 27001/17799

11.4.3 Equipment identification in networks „Automatic equipment identification should be considered as a means to authenticate connections from specific locations and Equipment"

ISO International Organization for Standardization

Network Access Control – NAC

macmon
nac intelligent einfach

Sie wissen bereits, warum Sie NAC einsetzen sollten!

...**welche Systeme** in Ihrem Netzwerk sind?

...dass **alle Geräte** in Ihrem Netz auch **von Ihnen** sind?

...dass niemand Ihre **VoIP-Gespräche** mithört?

...dass alle Ihre **Geräte geschützt** sind und keines davon ein Einfallstor darstellt?

Spionageaktivitäten, die so nicht passiert wären…

macmon
nac intelligent einfach

Schon fast amüsant:

WLAN in der Tupperdose

- außerhalb des Gebäudes
- nicht erkannt
- jahrelang

über macmon sofort als Device sichtbar

Getauschte Drucker

- „angeblicher“ Servicepartner
- Drucker mit Festplatte getauscht
- Abzüge von allem, was gedruckt wurde

über macmon als neue „MAC“ ersichtlich und geblockt

Kennen Sie alle Geräte in Ihrem Netz?

macmon®
nac intelligent einfach

Trend: „Bring your own Device“ (BYOD)

Jeder arbeitet doch am liebsten mit „seinem“ Gerät:

- Mitarbeiter
- Gäste, Besucher
- Dienstleister, Servicetechniker, Berater...

Traum oder **Albtraum**?

„BYOD“: zwei verschiedene Auffassungen

macmon
nac intelligent einfach

Behandlung von Smartphones und anderen Mobile Devices

- Konfigurieren des Devices
- Kontrollieren der Daten
- Admin-Zugriff
- Remote Wipe
  - Firmeneigentum
  - Vorstandsvorgabe

Mobile Device Management „MDM“

- Kein Zugriff
- Zugang gewähren
- Schutz des Netzwerks
- Anbieten bestimmter Ressourcen
  - Mitarbeitereigentum
  - Vorstandsvorgabe

Network Access Control „NAC“

+ BYOD Portal zur Registrierung

macmon
nac intelligent einfach

Die Bedeutung von NAC in der Praxis

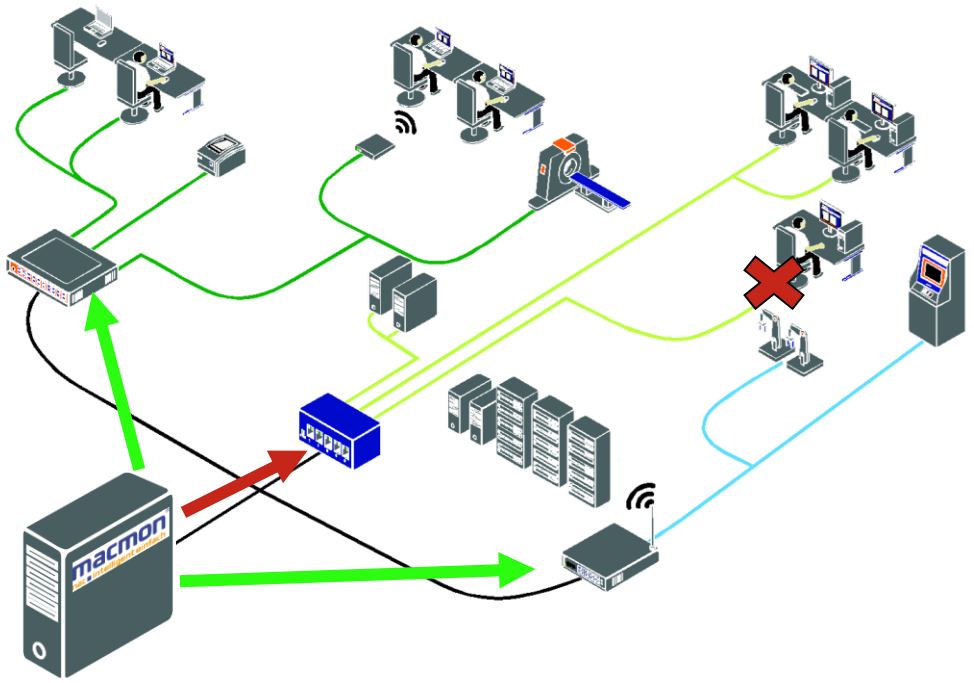
- Ein Großteil der Organisationen/Unternehmen haben **bisher keine oder nur unzureichende Schutzmaßnahmen** etabliert.
- Die Bedeutung von Netzwerkzugangs-Kontrollsystemen (NAC) **nimmt gerade durch die „Bring Your Own Device" Thematik enorm zu**.
- Die immer umfangreicher und komplexer werdenden **Netzwerke** sind **oft ohne** ein **entsprechendes Kontrollsystem nicht mehr überschaubar**.

macmon
nac intelligent einfach

Warum also wird NAC so wenig genutzt?

- aufwändige Veränderungen der Infrastruktur
- hohe Investitionskosten
- hoher Pflegeaufwand
- geringer bzw. schwer festzustellender Mehrwert
- komplexe Thematik – hoher Schulungsaufwand
- Gefahr, falsche bzw. zugelassene Systeme auszusperren

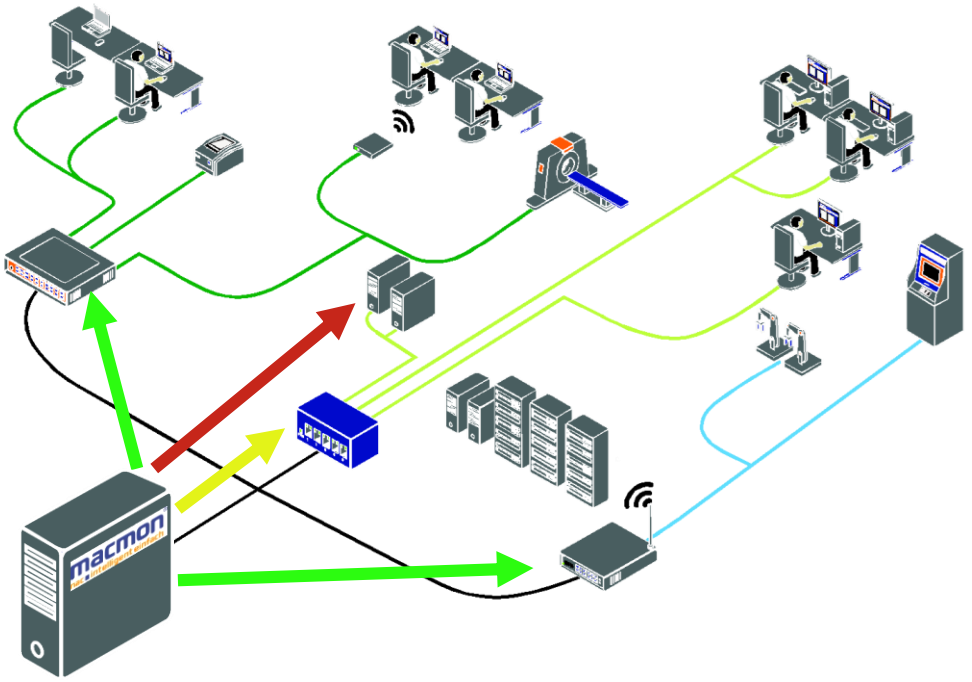
macmon Network Access Control – NAC



Gerätelokalisierung und
-steuerung am Switch-Port –
(SNMP, Telnet/SSH oder 802.1X)

- keine Agenten oder Sensoren erforderlich
- keine Veränderungen der Netzwerkstruktur
- Außenstellen werden mit überwacht
- Herstellerunabhängigkeit
- Regelbasiertes Eventmanagement
- Mischbetrieb mit & ohne 802.1X
- Zeiteinsparungen durch Automatismen
- Angriffsabwehr & Netzwerktransparenz

NAC – erweiterte Sicherheitsfunktionen



SNMP

IP-Adress-auflösung über ARP

Netzwerk-dienste DNS und DHCP

Erweiterte Endgeräte-Identifizierung

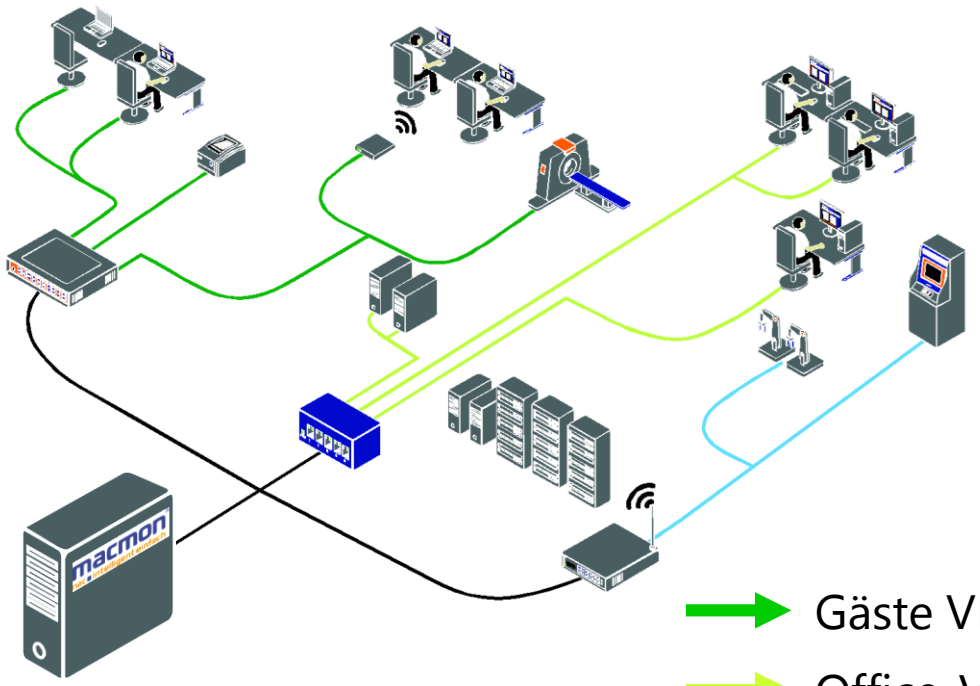
- Footprinting

Schutz vor Angriffen

- Adressfälschung
- Angriffe auf Switches
- ARP-Spoofing/MAC-Spoofing

macmon vlan manager

„Dynamische VLANs“

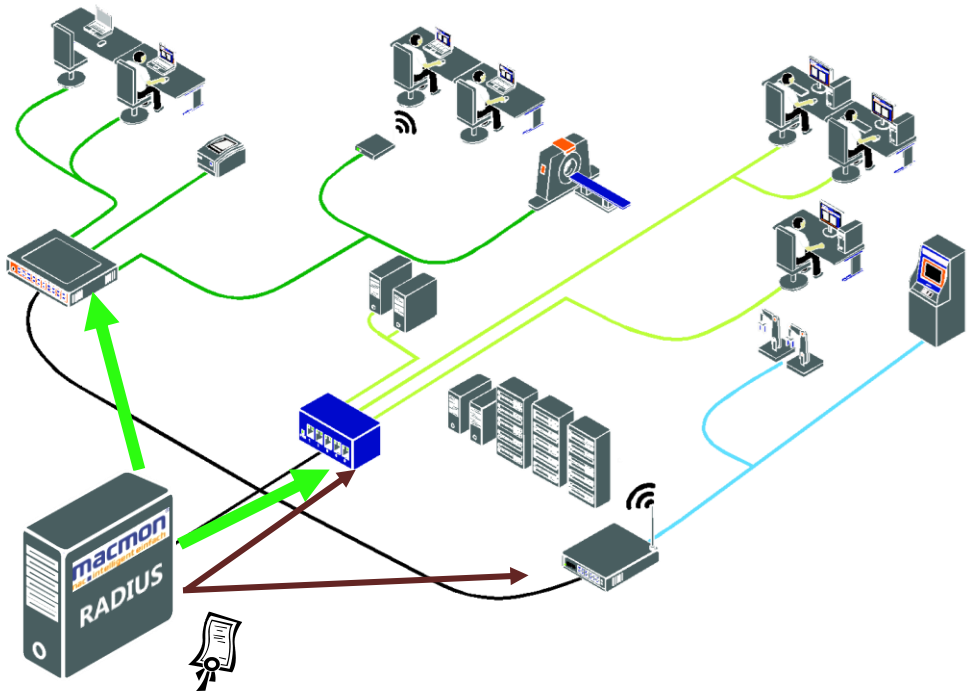


Das VLAN wird durch das Endgerät bestimmt (MAC-Adresse ➡ VLAN-ID).

Die Anwender haben immer den richtigen Zugang zum Netz, unabhängig vom physischen Anschluss.

- Einfache Pflege, keine Nachkonfigurationen bei Umzügen oder mobilen Nutzern.
- Kein Switch-Knowhow bei den für die Pflege eingesetzten Mitarbeitern notwendig.

macmon IEEE 802.1X



SNMP

EAP/802.1X

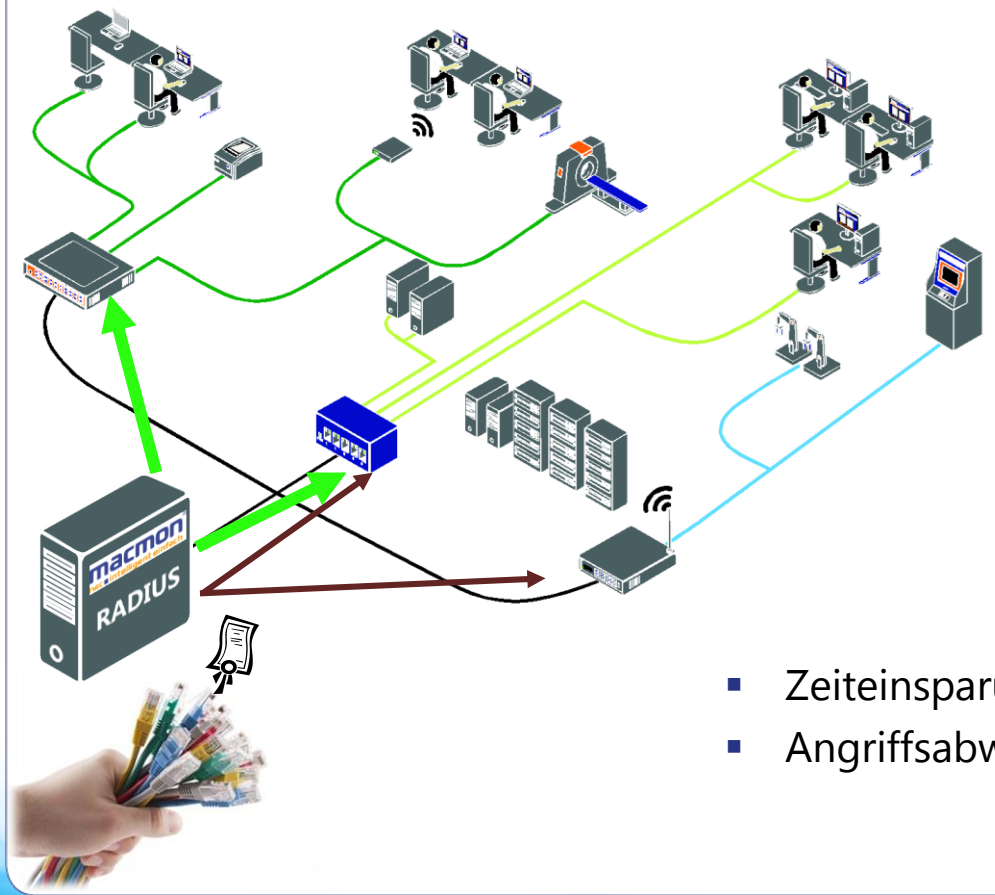
- Switch führt Autorisierung über Radius-Protokoll durch.
  - MAB (MAC Authentication Bypass)
  - Identität & Passwort auch AD-Konten
  - Zertifikat
- Etablieren von Sicherheitszonen
- Die VLAN-Steuerung erfolgt über macmon
- Fehlversuche erzeugen ein Ereignis!

macmon 802.1X

macmon macht es anders:

- ✓ Intelligent einfache Anbindung von AD/LDAP und anderen Identitätsquellen mit „Mapping“
- ✓ Möglichkeit des gemischten Betriebes – mit und ohne 802.1X
- ✓ Kombination von MAB mit macmon „Footprinting“
- ✓ Konfiguration von Gruppen ergibt automatische Regeln
- ✓ Intuitives und dynamisches Regelwerk
- ✓ Gerätefokus erleichtert die Administration
- ✓ Automatisiertes „Lernen“ von Geräten

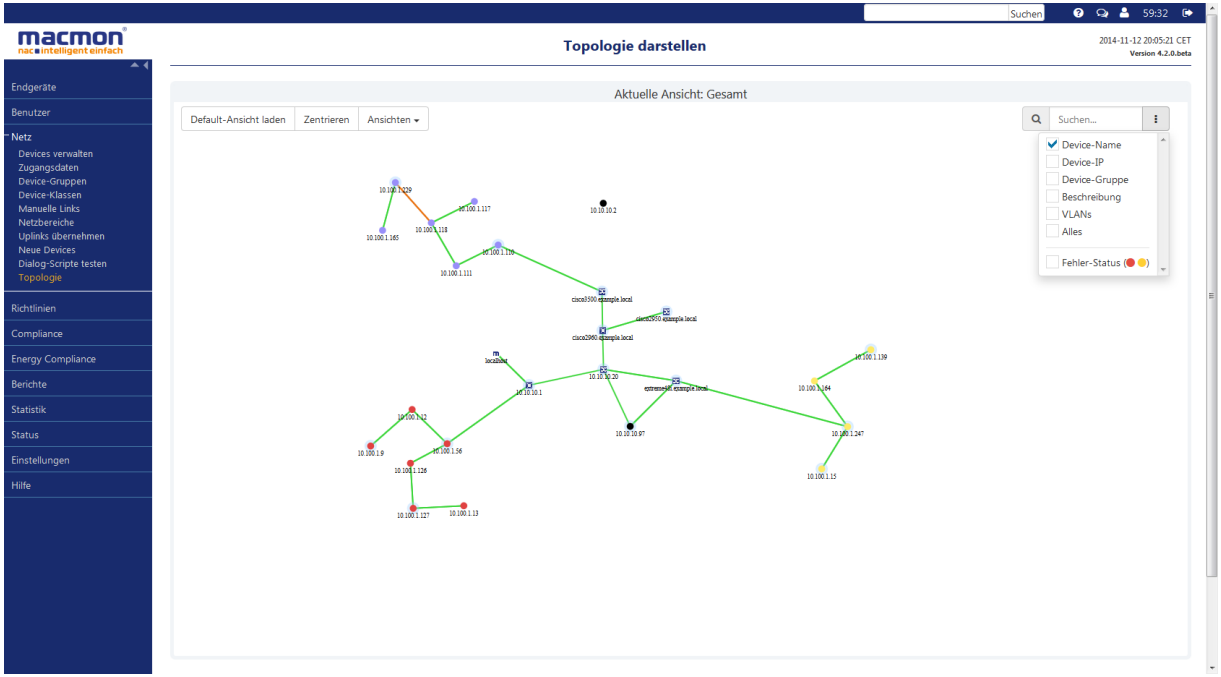
Übersicht, Kontrolle & Komfort



- Erstellen einer Referenzliste
- Anbinden des Active Directorys und Lernen der Geräte (802.1X)
- Kommunikation mit allen Switchen
- nur noch bekannte Geräte im LAN
- Unbekannte Geräte sperren/Gäste-LAN
- eigene Geräte ins hinterlegte VLAN
- einfache GUI – Intelligenz im Hintergrund
- Zeiteinsparungen durch Automatismen
- Angriffsabwehr & Netzwerktransparenz

macmon grafische Topologie

„effektive grafische Übersicht“



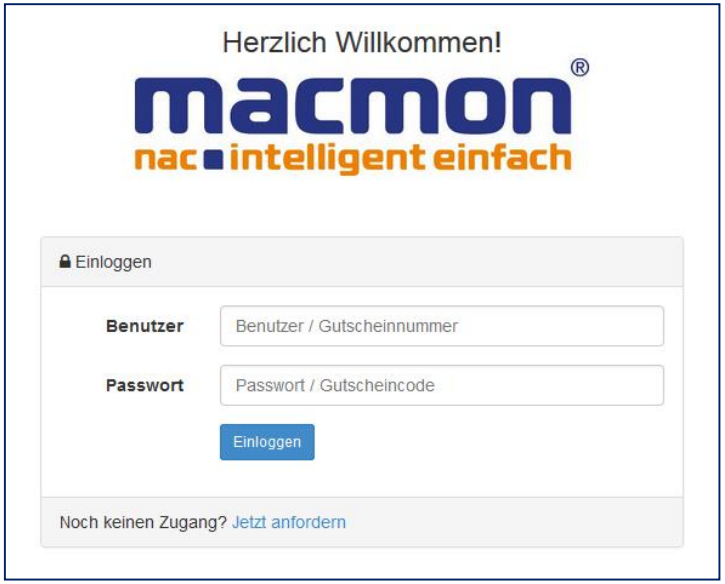
macmon hat im Betrieb automatisch alle Informationen:

- Automatisches Anordnen und Ergänzen von neuen Devices.
- Filtern anhand von Eigenschaften wie IP-Adresse, Name, VLAN, etc.
- Speichern, Laden und Exportieren als .SVG
- Fehlkonfigurationen finden und manuell Uplinks pflegen

macmon guest service

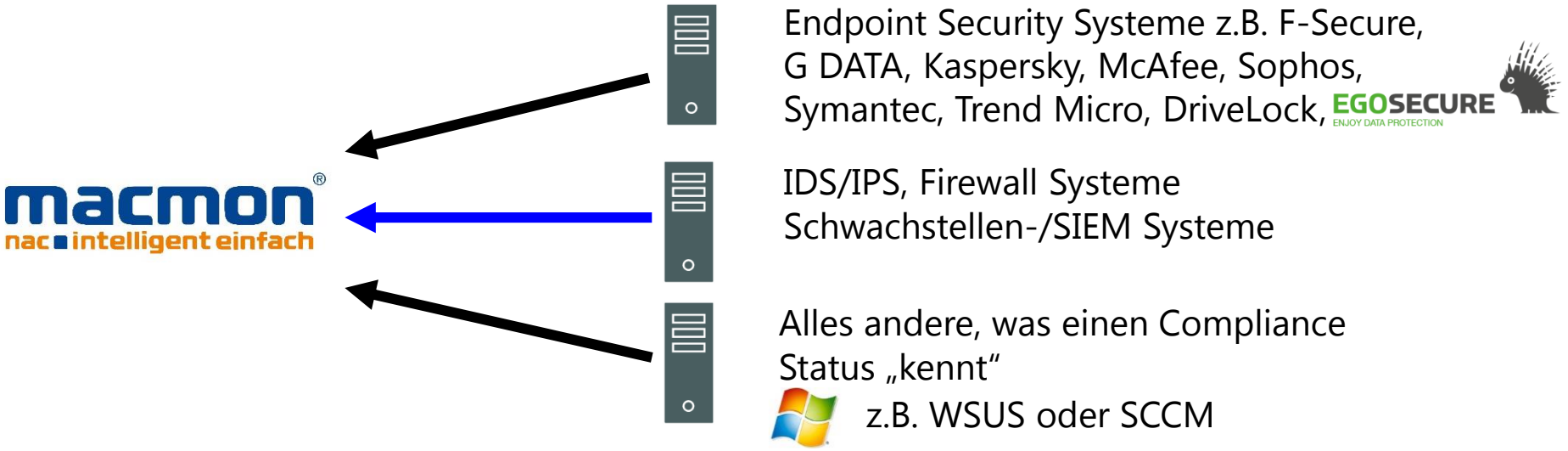
Korrekt wäre „Zugangs-Portal“

- ✓ Individuelle Gestaltung des Captive-Portals
- ✓ Nutzung verteilter Instanzen mit unterschiedlichem Layout
- ✓ Unabhängig vom Hersteller der LAN/WLAN-Infrastruktur
- ✓ Ortung der Geräte (an welchem Access-Point)
- ✓ Reaktives Aussperren der Geräte
- ✓ Selbstregistrierung mit Handy-Nr. und User-Namen
- ✓ Erstellung von Voucher-Listen zur Vereinfachung des Ablaufs am Empfang
- ✓ Sponsor Portal & BYOD-Portal
- ✓ AD/LDAP Integration



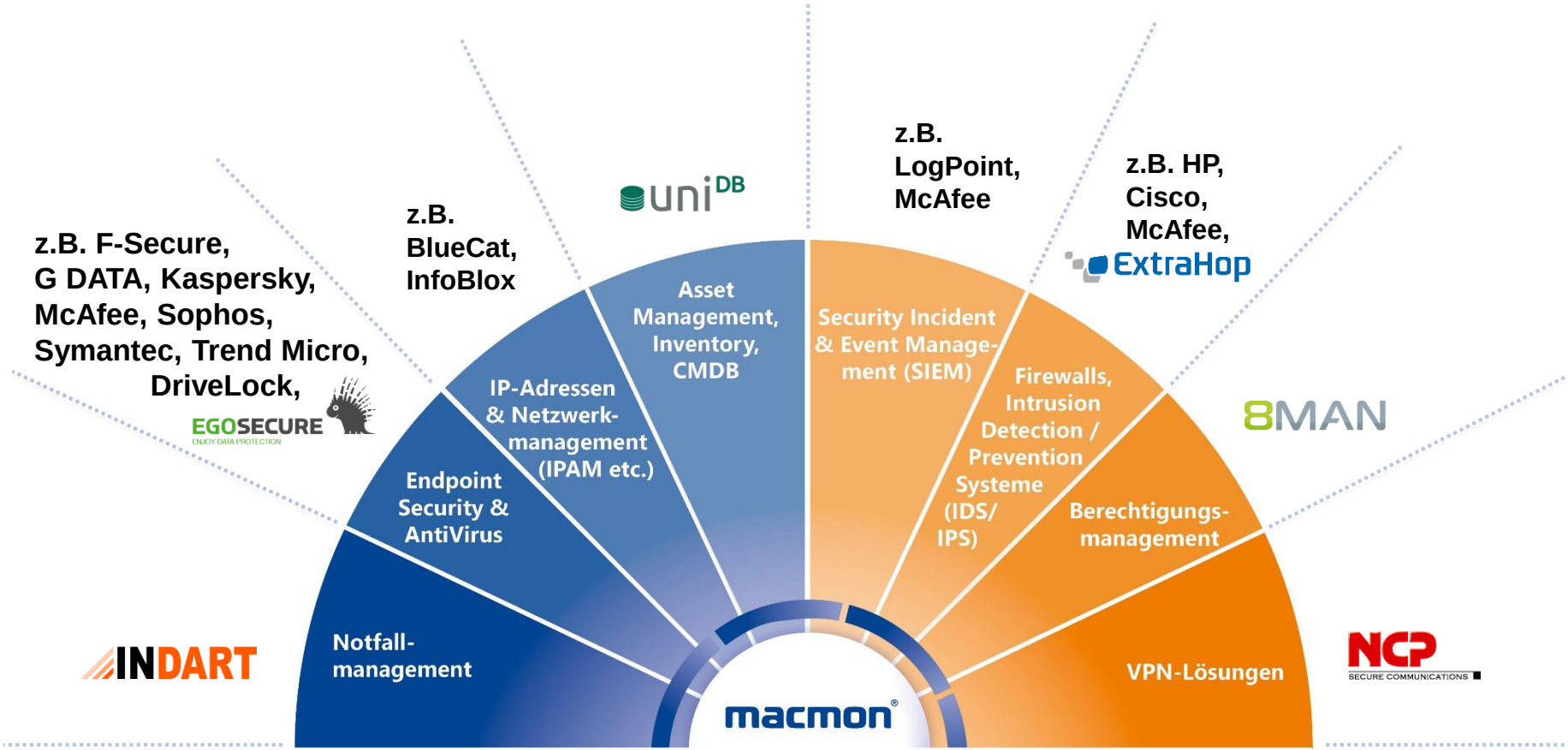
macmon „agentenlose multiple“ compliance

- **Offene Schnittstelle** zu beliebigen, **herstellerunabhängigen** Datenquellen
- **antivirus connector** – Anbindung führender Anti-Virus-Systeme
- Aktive Statusänderung durch den **macmon-eigenen Compliance Agenten**
- Integrierte **IF-MAP Technologie**
- Sofortige Erhöhung des ROI durch das Nutzen aller vorhandenen Systeme

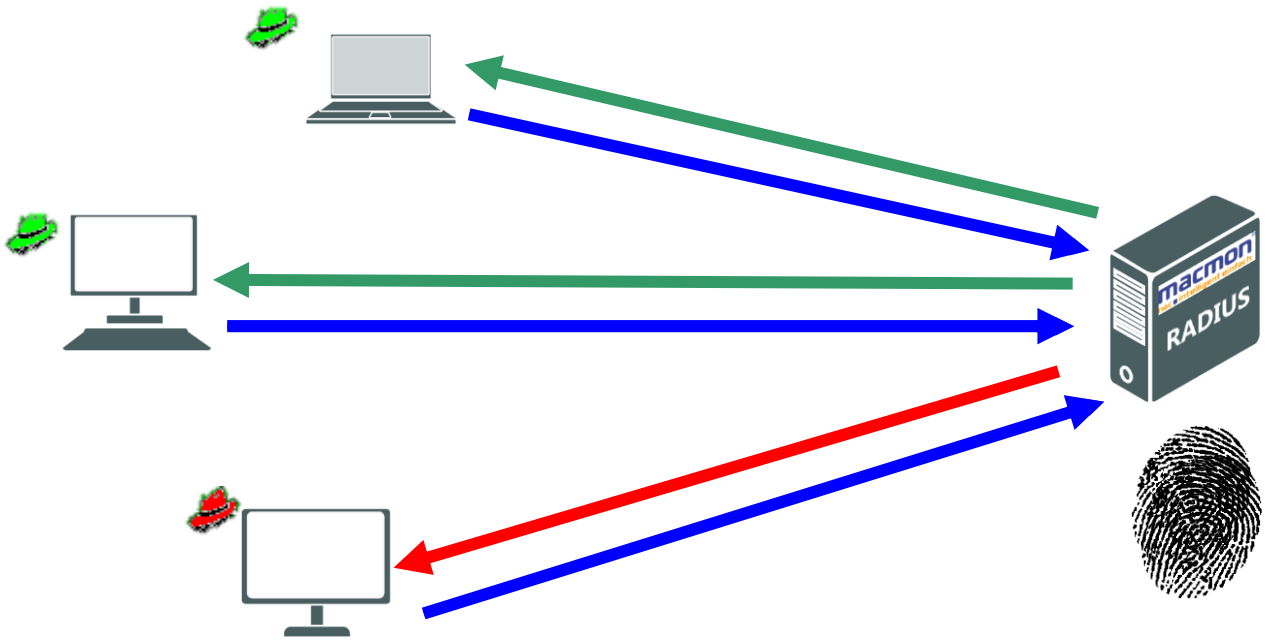


macmon NAC – Technologiepartner/Kopplungen

macmon
nac intelligent einfach



macmon client compliance



macmon client compliance Agent

Compliance Agent

Scan Daten

compliant

non-compliant

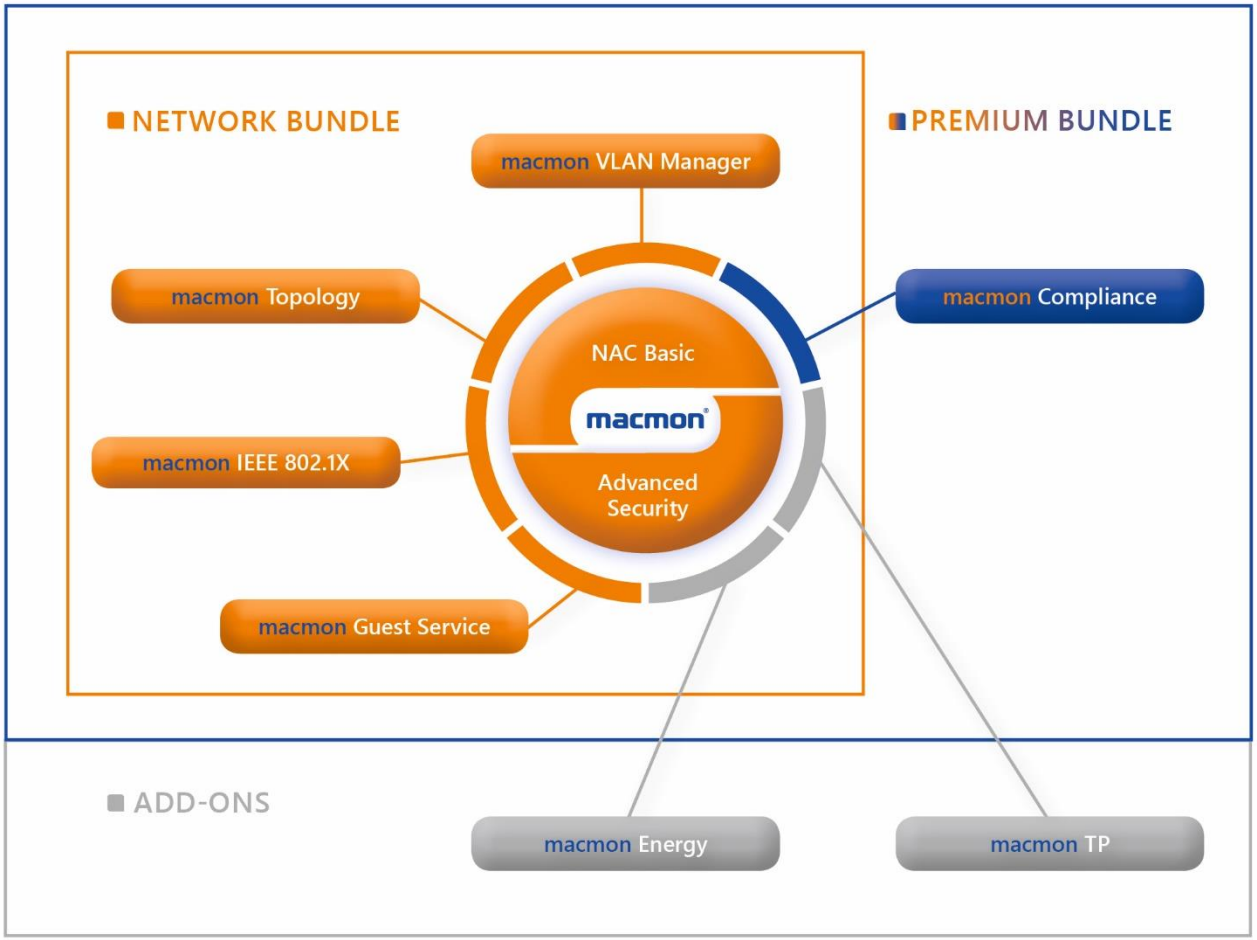
macmon energy

Energieverbrauch reduzieren & Produktivität verbessern

macmon tauscht die Energieprofile & weckt die PC's über WakeOnLan

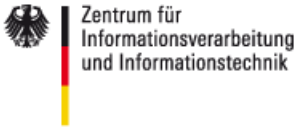
- **zeitgesteuert:** z. B. werktags um 18:00 Uhr/8:00 Uhr
- **ereignisgesteuert** durch die Zutrittskontrolle
- **geplant durch den Anwender** mit dem macmon energy-Kalender
  - Urlaube, Abwesenheit etc. können hinterlegt werden
- **zur Vermeidung von Risikosituation wie:**
  - » Angriffe, Verbreitung von Viren, Ausnutzen als Bot
- **zur Ausführung von automatisierten Wartungs- und Supportarbeiten wie:**
  - Software-Updates, vollständige Virenscans, Backups

macmon Produktfamilie



Kundenbeispiele

macmon®
nac intelligent einfach



Landratsamt Sigmaringen

Landratsamt Augsburg

Landesamt für Steuern und Finanzen

Kunden über die…

macmon
nac intelligent einfach

…Vorteile von macmon NAC:

- ✓ Sofortige Netzwerkübersicht mit grafischen Reports & Topologie
- ✓ Einführung innerhalb eines Tages & intuitives tägliches Handling
- ✓ Mischbetrieb mit und ohne 802.1X
- ✓ Intelligente AD Integration mit dynamischem Regelwerk
- ✓ Hoch flexibles „Gäste“-Portal
- ✓ Sinnvolle Integrationen mit anderen Security-Produkten
- ✓ Herstellerunabhängigkeit
- ✓ Deutscher Hersteller-Support

Kundenbeispiele – Industrie

macmon
nac intelligent einfach

Wichtige Faktoren

- Produktionsnetze „wachsen“ oft unkontrolliert, da proprietäre Kommunikationssysteme (Feldbus, Interbus, Profibus, …) zunehmend durch Ethernet ersetzt werden
- Roboter und Maschinen können nicht mit üblichen Mitteln (Virenschutz, Patches, …) geschützt werden
- Dienstleister müssen für Störungsbeseitigungen und Wartungs-arbeiten Zugang zum Netz haben
- Sicherheitsvorfälle können Sach- und Personenschäden bewirken

macmon NAC für den Schutz Ihrer Produktionsnetze

macmon®
nac intelligent einfach

- Einbinden der gesamten Produktionstechnik ohne Gefahr für das bestehende Netzwerk oder die Produktion selbst
- Erfüllung der Anforderungen von Industrie 4.0
- Gewährleistung des spontanen und dedizierten Zugangs zu den Produktionssystemen für Wartungstechniker
- Unterstützung bei der Zertifizierung nach ISO 27001 und der Umsetzung des BSI Grundschutzes
- Überwachung und Kontrolle aller im Netzwerk befindlichen Geräte
- Definition von gezielten Datenrouten und Übergabeschnittstellen zum besseren und gezielteren Schutz von Technologie-Know-how oder Produktionsdaten

Kontakt

Wir freuen uns auf das persönliche Gespräch mit Ihnen!

zusammen mit der

Netzwerk Kommunikationssysteme GmbH

An der Sülze 4 in 39179 Barleben

macmon secure GmbH

Charlottenstrasse 16
10117 Berlin

Fon +49 30 2325 777 - 0
Fax +49 30 2325 777 - 200

vertrieb@macmon.eu
www.macmon.eu