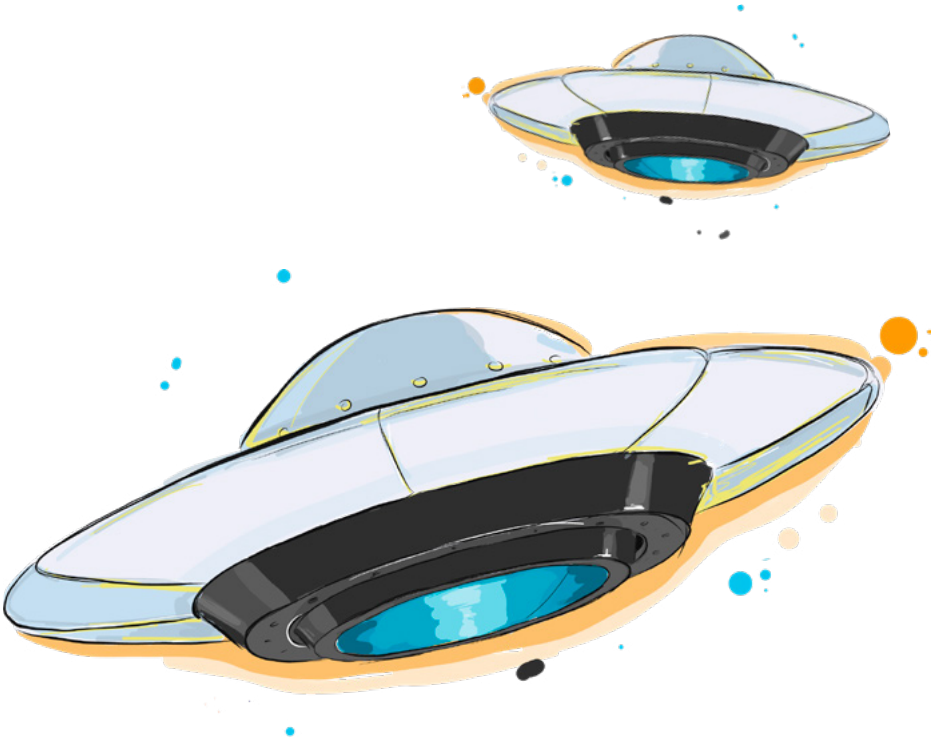
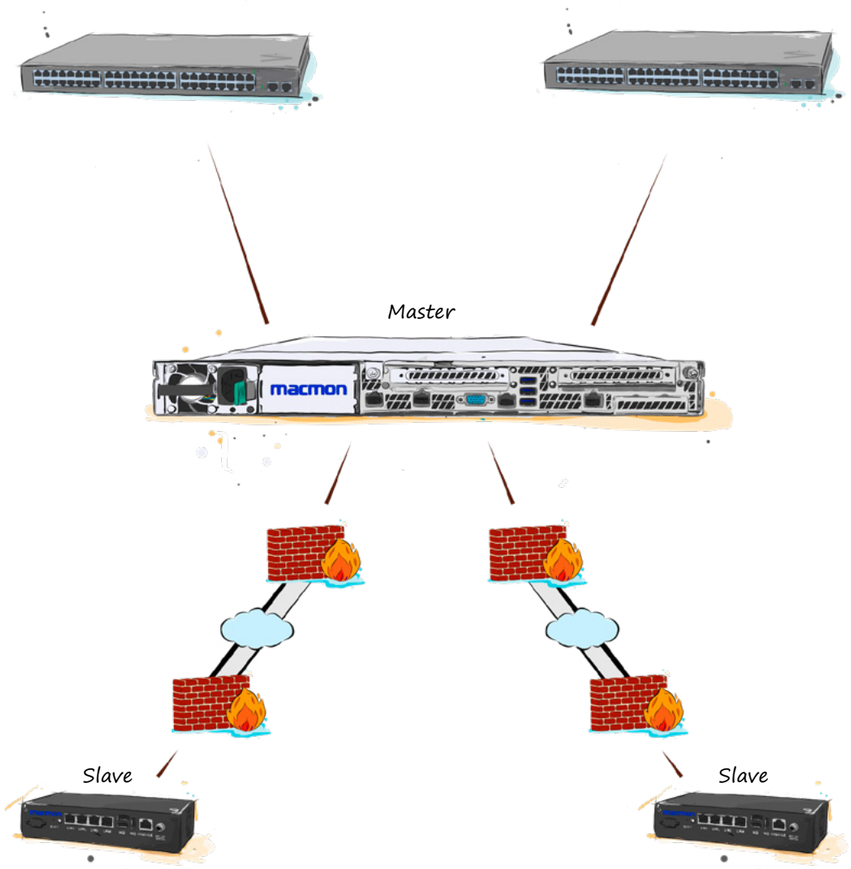
macmon
intelligent einfach



MACMON NAC-STORY

Wie wir UFOs in Ihrem Netzwerk verhindern

INHALTSVERZEICHNIS



macmon NAC bietet eine skalierbare Architektur im Master/Slave Prinzip zur Abdeckung jeder Netzwerkgröße und -struktur.

DER ANFANG

Übersicht durch komfortable und automatische Visualisierung

Die Einführung einer Netzwerkzugangskontrolle geschieht in der Regel aus drei Gründen:

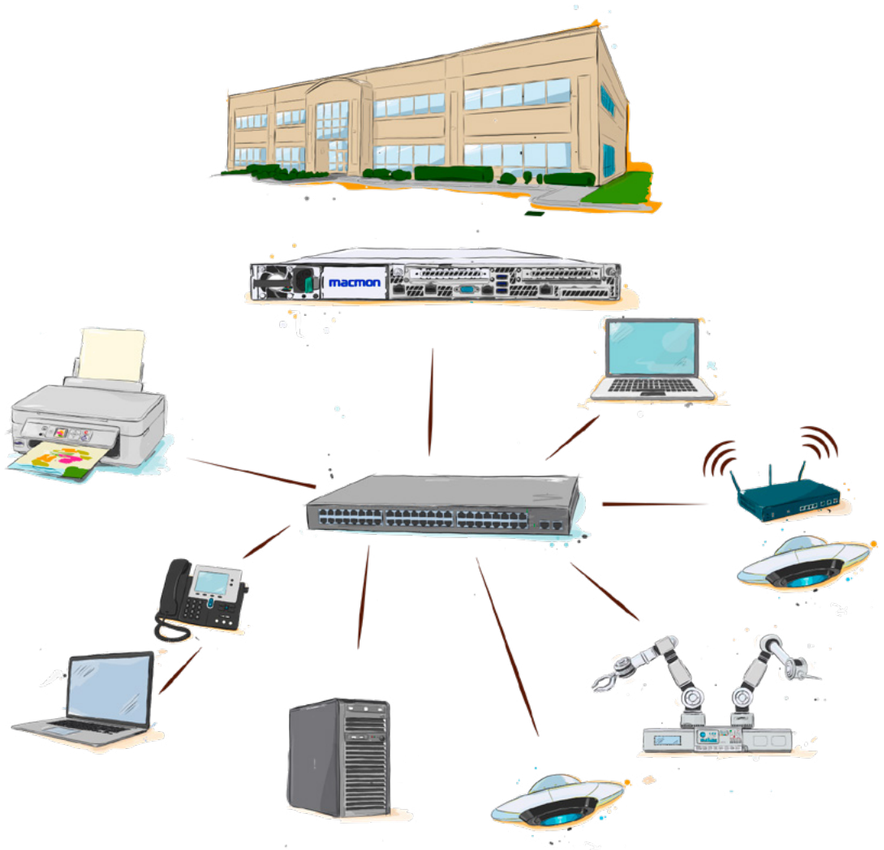
- Erhalten der **vollständigen Netzwerkübersicht**,
- **Steuerung der Zugänge** auf Basis der **Endgeräte-identitäten**,
- **Steuerung der Zugänge** auf Basis des **Sicherheitsstatus von Endgeräten**.

Mit macmon NAC setzen Sie diese Ziele einfach und schnell um. Darüber hinaus bietet macmon zusätzliche interessante Optionen für Ihre Netzwerksicherheit.

Das Entscheidende ist, dass die bestehende Infrastruktur genutzt wird und die **vollständige Netzwerkübersicht** bereits innerhalb weniger Stunden in der intuitiven Web-GUI von macmon NAC automatisch zur Verfügung steht. Der **geringe Einführungs- und Betriebsaufwand** liegt klar im Fokus.

Dafür kommuniziert macmon NAC über SNMP, SSH, HTTPS (REST), DHCP, DNS sowie weitere Protokolle und Schnittstellen (z. B. REST API) mit den Switches, Routern und weiteren aktiven Netzwerkkomponenten, um die Topologie des Netzwerks mit allen verbundenen Geräten herstellerunabhängig automatisch zu erfassen und zu identifizieren. Bei der Identifizierung der Endgeräte hat sich seit über 15 Jahren das Whitelist-Prinzip bewährt – für die übrigen unbekannten Geräte unterstützt macmon NAC diverse Technologien wie WMI, SNMP oder Footprinting.

Die gewonnene Übersicht erlaubt eine erste Beurteilung des Netzwerkzustands in Bezug auf die Menge und Art der unbekannten Endgeräte. Gleichzeitig wird ermittelt welchen Status das Netzwerk für die Einführung von NAC hat und welche Schritte dafür noch berücksichtigt werden müssen. Mit der Entscheidung für macmon NAC werden alle Weichen für ein erfolgreiches Network Access Control gestellt ohne im Vorfeld das Netzwerk verändern zu müssen.

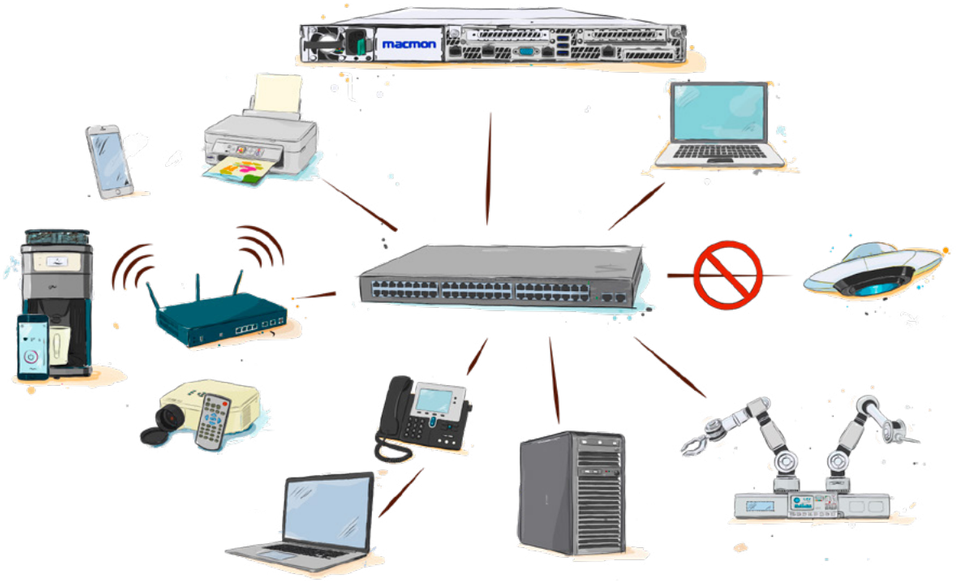


In kürzester Zeit erhalten Sie einen vollständigen Überblick aller Geräte im Netzwerk und finden so auch unbekannte fremde Objekte (UFOs).

VOLLSTÄNDIGE NETZWERKÜBERSICHT

Gewinnen Sie Übersicht, Komfort und Sicherheit in Ihrem Netzwerk

- Erfassung der gesamten Infrastruktur und aller Endgeräte als **Live-Bestandsmanagement**
- **Herstellerunabhängigkeit** zur Abdeckung jedes Netzwerkes auch mit gemischten Komponenten unterschiedlicher Generationen
- Implementierung **ohne** vorherige **Umstrukturierungen**
- Grafische **Darstellung der Netzwerktopologie** mit umfangreichen Analysemöglichkeiten
- Umfassendes **Reporting** über die im Netzwerk ermittelten Messdaten
- Individuelles **Dashboard** je Benutzer mit zentraler Übersicht der relevanten Details
- **Hochflexible Anbindungsmöglichkeiten** von Drittanbieterlösungen über die offene **REST API,** beispielsweise Asset Management- oder CMDB-Lösungen
- Darstellung der Ereignisse im Netzwerk:
  - Standortwechsel von Endgeräten innerhalb einer Organisation
  - Auftauchen bekannter Geräte zu ungewöhnlichen Zeiten
  - Angriffe wie ARP Spoofing oder MAC Spoofing
  - Aufspüren von Endgeräten im Netzwerk
  - Übersicht der Portnutzung (freie und belegte Ports)



macmon NAC unterstützt Sie bei der effektiven Kontrolle aller Netzwerkzugänge und schließt unbekannte oder ungewollte Geräte aus.

STEUERUNG DER ZUGÄNGE

Schützen Sie alle eingesetzten Geräte in Ihrem Netzwerk

Sobald der Benutzer durch macmon NAC weiß, welche Endgeräte sich im Netzwerk befinden, ist der Schritt zur effektiven Kontrolle aller Netzwerkzugänge leicht. Die bereits erlernten Endgeräte werden nach **Gruppen kategorisiert**. In diesen Gruppen kann festgelegt werden, welche Art von Zugriff die Geräte erhalten sollen, wenn sie eindeutig identifiziert werden.

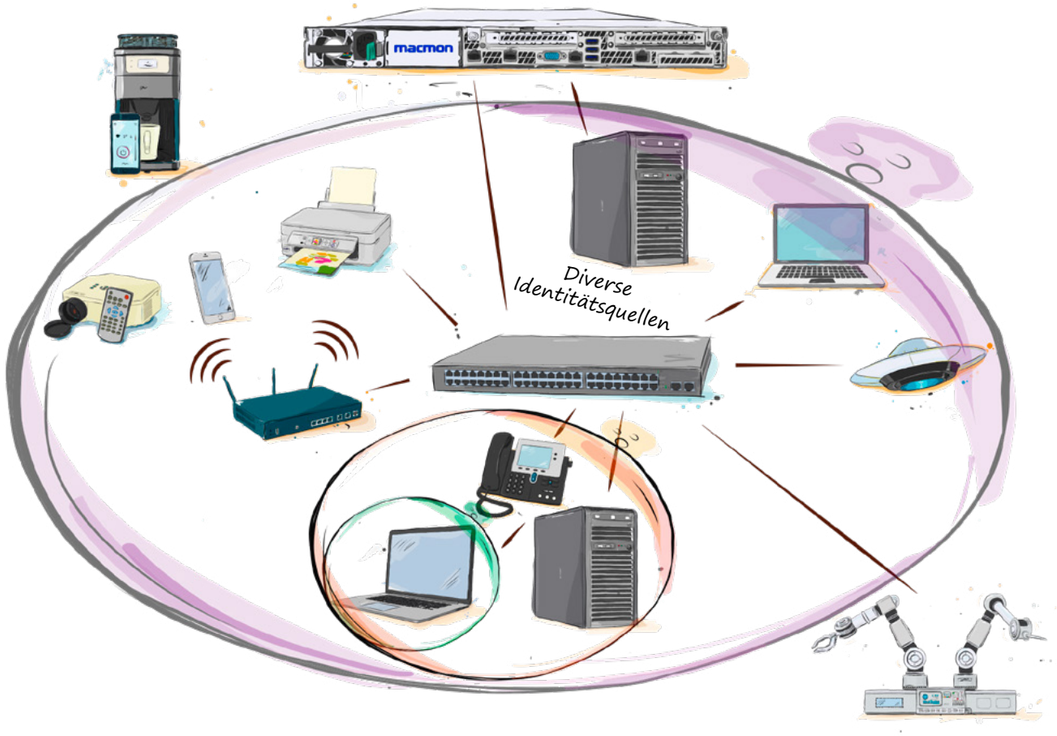
Ob Sie den reaktiven Ansatz nutzen möchten per SNMP die Switch-Ports zu schalten, den proaktiven Ansatz über 802.1X mit dem integrierten macmon RADIUS-Server bevorzugen oder einen gemischten Betrieb umsetzen wollen, macht administrativ durch das einheitliche und automatische Regelwerk in macmon NAC keinen Unterschied.

Eine Benutzeroberfläche – ein Regelwerk.

Abhängig von der Qualität der Identifizierung über MAC-Adresse, Benutzername und Passwort, AD-Konten bis hin zu Zertifikaten, können Sicherheitszonen parallel eingeführt werden.

Diese **einfache gruppenbasierte Konfiguration** sorgt durch das **automatische Regelwerk** von macmon NAC dafür, dass sich der Administrator für die Kontrolle der Zugänge nur noch um Sonderfälle kümmern muss – alles andere übernimmt macmon NAC.

Eine ganz entscheidende Vereinfachung und Erleichterung im täglichen Betrieb bringt dazu das dynamische VLAN-Management von macmon NAC. Es bietet ergänzend zur generellen Zugangsentscheidung die Möglichkeit, individuelle und passgenaue Zugänge zu gewähren. Die Möglichkeiten der Nutzung sind dabei sehr umfangreich und erlauben „zweckgebundene Zugänge“, die genau und auch nur den Zugang gewähren, der in der entsprechenden Situation benötigt wird. So erhalten z. B. Drucker immer ein Druckernetzwerk zugewiesen, während mobilen Mitarbeitern in allen Bereichen immer genau ihr Netzwerksegment zugewiesen wird.



Sicherheitszonen und automatisierte Netzwerksegmentierung härten das Netzwerk.

ZUGANGSVERWALTUNG

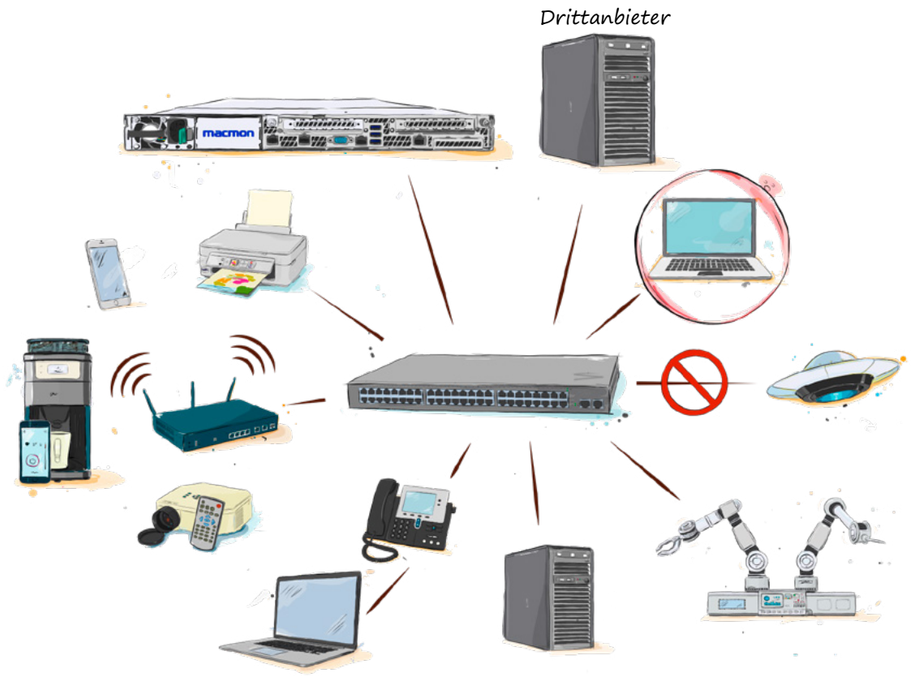
Die richtigen Zugänge – automatisch und zweckgebunden

Die Netzwerksegmentierung erhöht als Folge die Sicherheit im Netzwerk und bildet auch BSI-konforme Sicherheitskonzepte „nebenbei" ab. Umzüge von Endgeräten sind ohne manuelles Eingreifen möglich, was die Flexibilität erhöht und die IT-Abteilung massiv entlastet. **Einsparungen von über einem Personentag pro Monat** werden aus der Praxis berichtet. Die Kombination von macmon NAC mit bestehenden Identitätsquellen – CMDBs, Asset Management, Active Directory/LDAP oder auch Mobile Device Management (MDM) bzw. Unified Endpoint Management (UEM) führt zu einer zentralen und vollständigen Sicht, die permanent aktuell ist. Auch neue Geräte werden durch bestehende Workflows automatisch mit den notwendigen Zugängen versorgt, so dass der Pflegeaufwand auf ein Minimum reduziert wird.

Die logische Ergänzung zur Kontrolle der Netzwerkzugänge ist das Bereitstellen eines Gästeportals, um auch fremden Systemen temporären und eingeschränkten Zugang zu ermöglichen. Gleichzeitig können über ein solches Portal Sponsoren entsprechende Gast-Gutscheine vorbereiten und Mitarbeiter ihre eigenen Geräte registrieren. Die so delegierte **Gast- und Fremdgeräteverwaltung entlastet die IT-Abteilung** damit nochmals erheblich, da sie häufig gar nicht in die Entscheidung über Gerätezugänge eingebunden werden muss.

Die Kontrolle – Vorteile mit macmon NAC:

- *Technologieunabhängig:* Arbeiten Sie mit oder ohne 802.1X/RADIUS bzw. gleich im Mischbetrieb.
- *Mächtig:* Kommen Sie schnell zu Ergebnissen mit unserem dynamischen und automatischen Regelwerk.
- *Variabel:* Bilden und setzen Sie beliebige VLAN-Konzepte um.
- *Kompatibel:* Nutzen Sie die Anbindungen beliebiger Identitätsquellen zur automatischen Pflege der Systeme.
- *Effizient:* Reduzieren Sie Administrationsaufwand mit dem Gäste-, Sponsor- und BYOD-Portal.
- *Flexibel:* Etablieren Sie Sicherheitszonen und profitieren so von zweckgebundenen Zugängen.



Unsichere oder infizierte Endgeräte werden in „Isolationsblasen" vom Netzwerk getrennt.

SICHERHEITSLEVEL

Endgeräte die nicht den Anforderungen entsprechen werden automatisch isoliert

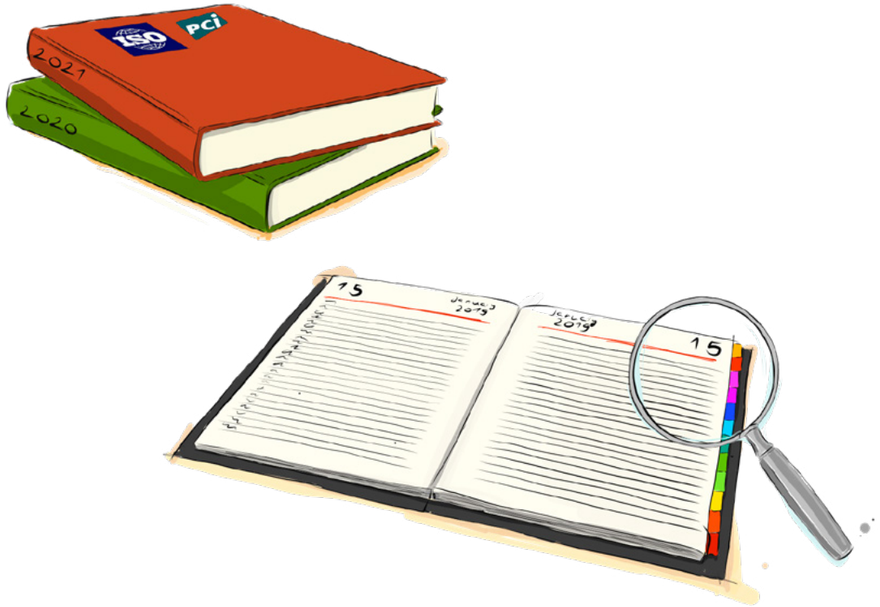
Nach dem Herstellen der Übersicht des Netzwerkes mit allen Netzwerkzugängen und der detaillierten Darstellung der Endgeräte, ist macmon NAC die **zentrale Macht** im Netzwerk. Ergänzend sollten auch die Endgeräte auf ihre Sicherheitseinstellungen bzw. ihr Sicherheitslevel kontrolliert werden. Dafür bietet macmon NAC diverse Überprüfungsmöglichkeiten.

Mit Hilfe eines Agenten kann die Prüfung direkt auf den Endgeräten durchgeführt werden. Zusätzlich können z. B. Antivirus Management Server auf Meldungen von infizierten Endgeräten geprüft werden, um diese direkt vom Netzwerk zu isolieren.

Eine weitere Möglichkeit um Ihr Netzwerk zu härten bietet die Integration von Drittanbieterlösungen. In der Regel ist bereits eine Lösung im Einsatz, die das Sicherheitslevel prüft und damit die entscheidenden Informationen bereithält. Mittels der umfassenden REST API oder der speziellen Compliance API von macmon NAC, können diese Quellen als Statuslieferanten einfach angebunden werden. Auf diese Weise wird die Macht von macmon NAC genutzt und Endgeräte, die nicht den Anforderungen entsprechen, werden automatisch isoliert und nach erfolgter Heilung wieder in den ursprünglichen Zugang versetzt.

Die Sicherheitslevelvorteile mit macmon NAC:

- **Proaktive Reaktion** auf Infektionsquellen
- **Automatisierte Isolation** von unsicheren Endgeräten im Netzwerk
- **Einfache Implementierung** ohne Änderungen an der Infrastruktur
- **Einfache Integration** von Drittanbieterlösungen
- **Skaleneffekte** durch die Nutzung aller bereits vorhandenen Systeme und Investitionen



Der macmon Past Viewer erleichtert Nachweis- und Dokumentationspflichten bzw. forensische Analysen um ein Vielfaches.

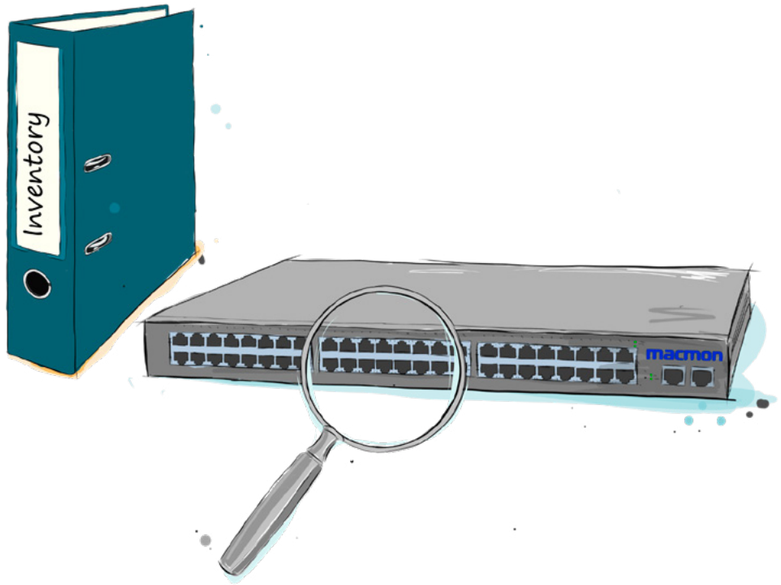
HISTORISCHE TATSACHEN

Forensische und Impact-Analysen durchführen

macmon Past Viewer bietet ergänzend die Möglichkeit, die bei Network Access Control üblicherweise verworfenen „alten“ **Daten strukturiert zu sammeln und aufzubereiten**, um neben der Live-Sicht auch eine historische Sicht zu erhalten. Pro Endgerät lässt sich damit darstellen, wann und wo das Gerät im Netzwerk betrieben wurde, welche IP-Adressen und welche Namen es hatte oder in welchem VLAN es war.

Des Weiteren lässt sich pro Switch Interface oder Access Point nachvollziehen, welche Endgeräte dort wann, mit welcher IP-Adresse, welchem Namen und mit welcher Autorisation betrieben wurden.

Mit diesen Informationen sind forensische Analysen möglich, um Nachweispflichten in Bezug auf z. B. **ISO- oder PCI-Compliance** bzw. für den Datenschutzbeauftragten nachkommen zu können. Zum anderen können bei Verdachtssituationen oder konkreten Vorfällen entsprechende Verbindungen nachträglich überprüft werden. Da diese Daten durch die permanente Erhebung gesammelt werden, ist der **Blick zurück über die gesamte Dauer** des Einsatzes von macmon NAC mit dem Modul macmon Past Viewer möglich. Gleichzeitig erlauben die Daten eine Analyse für geplante Veränderungen oder Maßnahmen innerhalb des Netzwerkes.



Mehr Details und Übersicht über die Netzwerkgeräte sowie gesichertes RADIUS-basiertes Einloggen.

BLICK INS DETAIL

Mehr Details und mehr Sicherheit

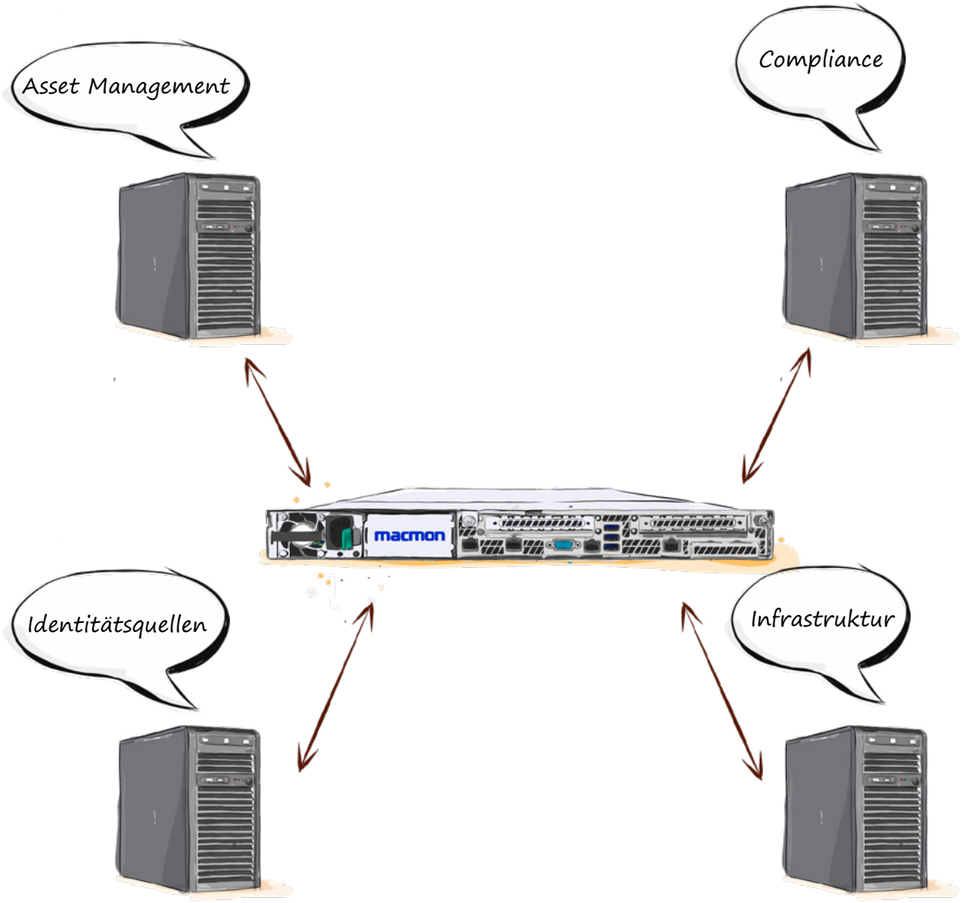
Eine weitere Ergänzung zur Kontrolle der Netzwerkzugänge ist die Nutzbarmachung aller erhobenen Daten bis ins Detail. Mit **macmon Switch Viewer** werden diverse weitere **Informationen der Netzwerkgeräte erhoben und zur Nutzung angeboten**. Beispiele dafür sind die Seriennummern und weitere Portkonfigurationen.

Ergänzend zu den Netzwerkgerätedetails bietet macmon Switch Viewer auch die Option macmon als RADIUS-Server für die Authentifizierung am Netzwerkgerät zu nutzen.

Damit wird eine weitere Sicherheitserhöhung erreicht und die Notwendigkeit für einen separaten RADIUS-Server entfällt.

Eine grafische Darstellung der Interfaces im Original-Layout der Netzwerkgeräte bietet dazu **schnell erfassbare Details über den Ist-Zustand**.

Im Bedarfsfall besteht die Möglichkeit, **zielsicher den korrekten physikalischen Port zu** ermitteln und ggf. zu schalten.



macmon NAC lässt sich nahtlos in anderen Security-Produkten integrieren und spart wertvolle Zeit durch Automatisierung.

MACMON TECHNOLOGIEPARTNER

Koppeln Sie macmon NAC mit anderen führenden Sicherheitslösungen

macmon NAC liefert nicht nur die beste Antwort darauf, wie ungesicherte Netzwerkzugriffe verhindert werden können, es lässt sich auch **nahtlos in andere Security-Produkte integrieren**. Die Einteilung der Anbindungen erfolgt in Asset Management, Compliance, Identitätsquellen und Infrastruktur, wobei der Informationsaustausch jeweils bidirektional erfolgen kann.

Compliance
Wenn eine vorhandene Sicherheitslösung bei der Überprüfung eines Endgeräts im Netzwerk feststellt, dass dieses von den Sicherheitsvorgaben abweicht, von einem Schadprogramm infiziert oder Teil eines Botnetzes ist, übermittelt sie die Identität, den Grund und den neuen Compliance-Status an macmon NAC. Gleichzeitig kann macmon weitere Systeme über die Statusänderung informieren.

Infrastruktur
Welche Geräte sich im Netzwerk befinden, findet macmon NAC sehr schnell heraus, indem es die Daten der Netzwerkinfrastruktur ausliest oder übermittelt bekommt. Durch den Entwicklungsaustausch mit den Herstellern dieser Infrastrukturgeräte ist sichergestellt, dass diese Daten zuverlässig und korrekt in macmon NAC zur Verfügung stehen.

Asset Management
Mit der bidirektionalen Kopplung von Asset Management-Lösungen wie CMDBs, Inventory, Client Management und anderen Systemen, lassen sich die Information über Endgeräte und Netzwerkgeräte automatisch synchronisieren. Je nach Workflow kann dabei das Drittanbieter-Produkt oder macmon NAC die führende Rolle übernehmen, wobei das Live-Bestandsmanagement von macmon in der Regel als Erstes von neuen Geräten erfährt und dieses Wissen teilt.

Identitätsquellen
Bereits im Netzwerk vorhandene Identitätsquellen wie MDM- bzw. UEM-Lösungen, AD-/LDAP-Dienste, SAML, RADIUS-Server oder weitere Systeme können von macmon NAC für die qualifizierte Authentifizierung von Endgeräten genutzt werden. Eindeutig authentifizierte Identitäten können wiederum samt aktuellem Status an Drittsysteme, wie z. B. Firewalls o. ä., übermittelt werden.

MACMON SECURE GMBH

Deutscher Best-of-Breed-NAC-Hersteller

Die macmon secure GmbH beschäftigt sich seit 2003 mit der Entwicklung von Software für Netzwerksicherheit und hat ihren Firmensitz im Herzen Berlins. Die Network Access Control (NAC)-Lösung von macmon wird vollständig in Deutschland entwickelt und weltweit eingesetzt, um Netzwerke vor unberechtigten Zugriffen zu schützen.

Über 1.500 Kunden von mittelständischen Firmen bis hin zu großen internationalen Konzernen verschiedenster Branchen vertrauen beim Thema Netzwerksicherheit bereits auf die macmon secure GmbH.

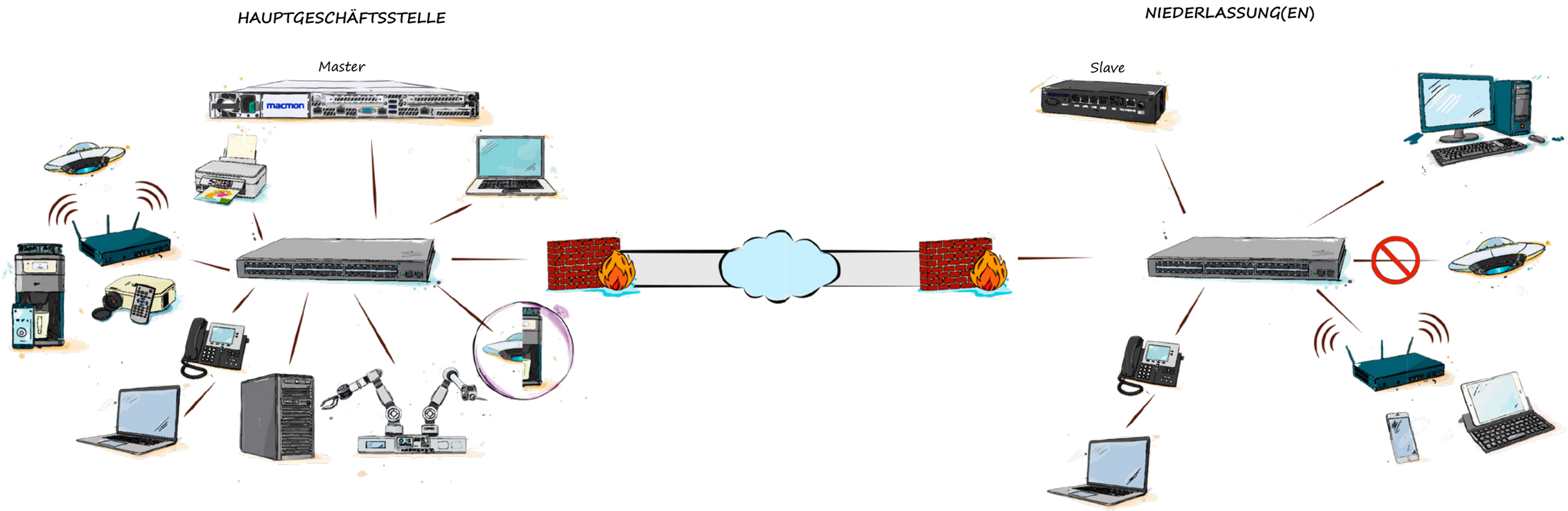
Das Ziel: Jedem Unternehmen eine flexible und effiziente NAC-Lösung anzubieten, die mit geringem Aufwand, aber erheblichem Mehrwert für die Netzwerksicherheit im Unternehmen implementiert werden kann.

macmon NAC – intelligent einfach!

Unsere inzwischen über 70-köpfige Mannschaft vereint Diplom-Ingenieure und -Betriebswirte, Software Engineers, Bachelors und Masters of Science für Angewandte Informatik, Diplom- und Fachinformatiker, die gemeinsam zu einer marktnahen Weiterentwicklung unserer NAC-Software macmon, der erfolgreichen Umsetzung von NAC-Projekten bei unseren Kunden und damit zu unserem Erfolg beitragen.

GEHEN WIR AUF UFO-SUCHE

Starten Sie mit uns die Entdeckung Ihres Netzwerks



UFO = unbekannte fremde Objekte

Network Access Control

- Sofortige Netzwerkübersicht mit grafischen Reports & Topologie
- Dynamische Netzwerkkontrolle mit und ohne 802.1X in heterogenen Infrastrukturen
- Machtvolle Durchsetzung der Unternehmens-Compliance mit einfacher Drittanbieterintegration

macmon secure GmbH
Alte Jakobstraße 79 - 80
10179 Berlin
+49 30 23 25 777-0 | nac@macmon.eu

www.macmon.eu