DEMYSTIFYING NAC

Network Access Control
mit macmon NAC einfach erklärt

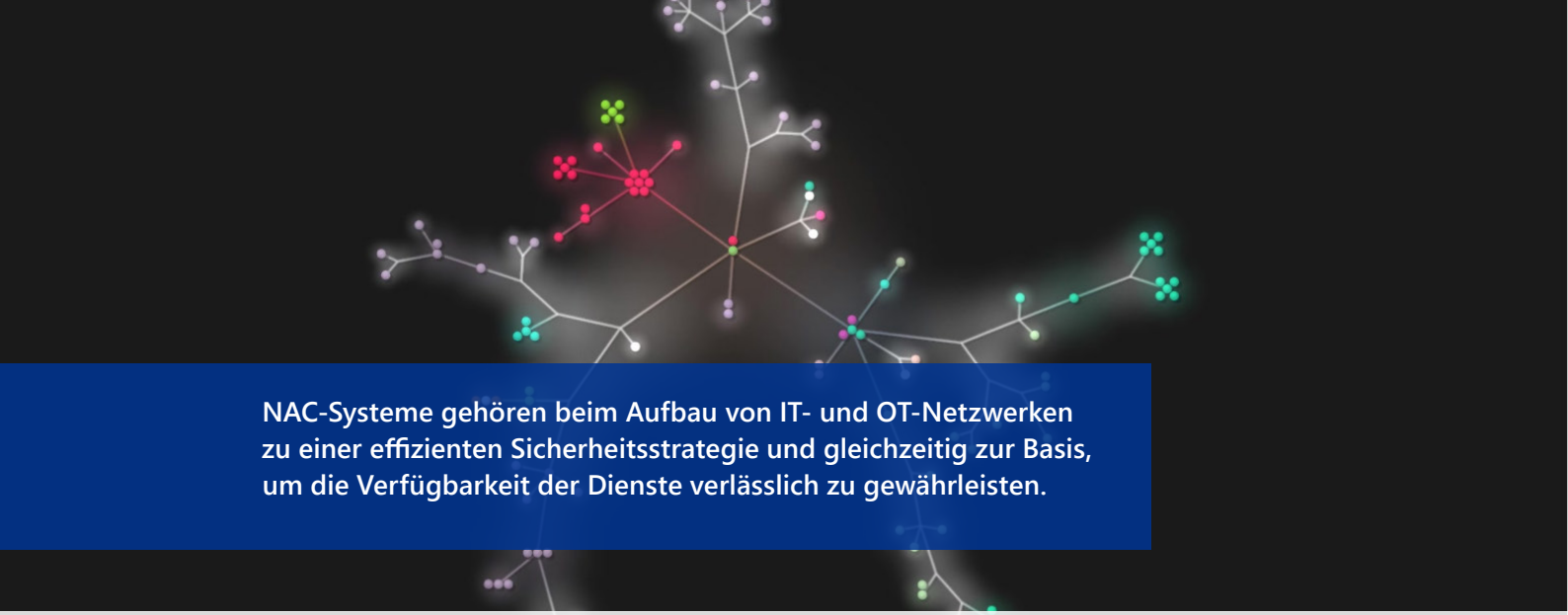
nac

macmon
intelligent einfach

Demystifying NAC

Network Access Control mit macmon NAC einfach erklärt

INHALT:



NAC-Systeme gehören beim Aufbau von IT- und OT-Netzwerken zu einer effizienten Sicherheitsstrategie und gleichzeitig zur Basis, um die Verfügbarkeit der Dienste verlässlich zu gewährleisten.

WARUM NAC?

NAC – Basisschutz in industriellen Netzwerken

Durch die fortschreitende Nutzung von Netzwerktechnologien und die Abhängigkeit der Geschäftsprozesse von eben diesen Technologien, ist nahezu jedes Unternehmen auf eine **vernetzte** und **stets verfügbare Netzwerkumgebung** angewiesen.

Gleichzeitig nimmt die Nutzung vom Internet der Dinge (IoT), die Zugriffe von mobilen Endgeräten und die Vernetzung von IT- und OT-Netzwerken zu. Mit der wachsenden Zahl unterschiedlichster Geräte, die aufs Netzwerk zugreifen, **erhöhen sich die Sicherheitsrisiken** enorm, während die Übersicht im Netzwerk zunehmend verloren geht. Kommt ergänzend noch die Anbindung an Cloud-Dienste zur digitalen Produktionsoptimierung (Industrie 4.X) hinzu, ist das Bedrohungsszenario komplett.

Um diesen Herausforderungen zu begegnen, gehören Systeme für die **Netzwerkzugangskontrolle** (Network Access Control/NAC) beim Aufbau von IT- und OT-Unternehmensnetzwerken zu einer effizienten Sicherheitsstrategie und gleichzeitig zur Basis, um die Verfügbarkeit der Dienste verlässlich zu gewährleisten.

Neben der Antwort auf die Frage, wie fremde, unbekannte und unerwünschte Geräte vom eigenen Netzwerk ferngehalten werden – also der Zugriff verweigert wird, bieten moderne NAC-Produkte auch die Lösung um gezielt Endgeräte von Besuchern, wie Dienstleistern **zeitlich befristete Zugänge** auf einzelne Netzwerkbereiche oder Geräte zu gewähren.

Lösungen für Netzwerkzugangskontrolle bleiben deshalb immer ein **essenzieller Bestandteil** integrierter IT- und OT-Sicherheitssysteme, die heutige und zukünftige Risiken reduzieren und mittlerweile eine ganz zentrale Rolle im Netzwerk übernehmen.

Da ein großer Teil der Systeme in Produktionsnetzen nicht mit Mitteln wie Virenscannern etc. geschützt werden kann, MUSS das Grundprinzip sein, alle nicht zwingend notwendigen Geräte vom Netzwerk fernzuhalten und je nach Kritikalität Sicherheitszonen zu schaffen – das ist die exakte Beschreibung von Network-Access-Control.

Mit der Entscheidung für macmon NAC werden alle Weichen für ein erfolgreiches Network Access Control gestellt ohne im Vorfeld das Netzwerk verändern zu müssen.

DER ERSTE SCHRITT

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 Endgeräteidentitäten**
- **Steuerung der Zugänge auf Basis des Sicherheitsstatus von Endgeräten**

Mit macmon NAC werden diese Ziele schnell umgesetzt. 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.

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 eventuell noch berücksichtigt werden müssen.

macmon NAC kommuniziert mit den **aktiven Netzwerkkomponenten**, wie unter anderem Switches, Routern und Firewalls, um die Topologie des Netzwerks mit allen verbundenen Geräten herstellerunabhängig automatisch zu erfassen und zu identifizieren.

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 einen vollständigen Überblick aller Geräte im Netzwerk erhalten und auch längst vergessene, unbekannte Geräte finden.

VOLLSTÄNDIGE NETZWERKÜBERSICHT

Übersicht, Kontrolle und Sicherheit im Netzwerk gewinnen

macmon NAC ermöglicht die umfassende Kontrolle über das Netzwerk und bietet:

- **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**

macmon NAC erlaubt die vollständige Übersicht über das Netzwerk und zeigt:

- **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 bei der effektiven Kontrolle aller Netzwerk-zugänge und schließt unbekannte oder ungewollte Geräte aus.

STEUERUNG DER ZUGÄNGE

Alle eingesetzten Geräte im Netzwerk werden geschützt

Sobald durch macmon NAC bekannt ist, 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 der reaktive Ansatz genutzt wird per SNMP die Switch-Ports zu schalten, der proaktive Ansatz über 802.1X mit dem integrierten macmon RADIUS-Server oder ein gemischter Betrieb umgesetzt werden soll, macht administrativ durch das einheitliche und automatische Regelwerk in macmon NAC keinen Unterschied.

Eine Benutzeroberfläche – ein Regelwerk – nur mit macmon NAC. 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. Geräte einer definierten Produktionsblase ein gemeinsames und vielleicht sogar isoliertes Segment zugewiesen, während mobile Mitarbeiter in allen Netzwerkbereichen immer automatisch das für sie vorgesehene Netzwerk-segment erreichen.

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 Netzwerk-Abteilung massiv entlastet. Einsparungen von über einem Personentag pro Monat werden aus der Praxis berichtet.

Die Kombination von macmon NAC mit bestehenden Identity-Integrationen – 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 übergibt die Kontrolle an die korrekten Fachbereiche, was für eine allgemeine Entlastung sorgt, da nur relevante Personen involviert werden.

Die Vorteile von macmon NAC

- **Technologieunabhängig:** Mit oder ohne 802.1X/RADIUS bzw. gleich im Mischbetrieb
- **Mächtig:** Schnelle Ergebnisse mit dem dynamischen und automatischen Regelwerk
- **Variabel:** Umsetzung beliebiger VLAN-Konzepte
- **Kompatibel:** Anbindungen beliebiger Identitätsquellen zur automatischen Pflege der Systeme möglich
- **Effizient:** Reduktion von Administrationsaufwand durch das Gäste-, Sponsor- und BYOD-Portal
- **Flexibel:** Etablierung von Sicherheitszonen mit zweckgebundenen Zugängen

Vielfältige nicht-invasive Reaktionsmöglichkeiten auf unsichere oder infizierte Endgeräte.

SICHERHEITSLEVEL

Mehr als Identitäten?

Nach dem Herstellen der Übersicht des Netzwerkes mit allen Netzwerkzugängen und der detaillierten Darstellung der Endgeräte, ist macmon NAC die zentrale Macht im Netzwerk.

Network Access Control hat in erster Linie den Fokus auf die **Kontrolle der Identitäten**, wobei ergänzend auch der **Sicherheitsstatus** kontrolliert werden sollte. Während in IT-Netzwerken häufig auch die Entscheidung über die Gewährung des Netzwerkzugangs vom Sicherheitsstatus des jeweiligen Gerätes abhängt, sieht die Reaktion auf Geräte mit zu niedrigem Sicherheitslevel in OT-Netzwerken ganz anders aus.

Veränderungen der Netzwerksegmentierung, Anpassen von Firewall-Regeln, Einrichten von Zeitfenstern zum Ausrollen von kritischen Patches oder auch die Anpassung der langfristigen Investitionsplanung zur Anschaffung modernerer Geräte sind eher die Art von Folgen in der Industrie.

Mit der zentralen Position im Netzwerk, der Macht über die Netzwerkzugänge und den umfangreichen Schnittstellen, nimmt macmon NAC eine äußerst geeignete Rolle in der **Umsetzung von Sicherheitsmaßnahmen** ein. Während Informationen über Sicherheitsstatus von Endgeräten einfach an macmon NAC übertragen oder auch umgekehrt aktiv eingeholt werden können, bieten die Reaktionsmöglichkeiten von macmon NAC die Option, **Maßnahmen** einzuleiten die **wenig bis gar nicht invasiv** sind und den fortwährenden **Betrieb der Produktion sicherstellen**.

Eskalierende Alarmierungen aber auch die Einschränkung der Kommunikationsmöglichkeiten von oder zu stark gefährdeten Systemen sind nur zwei Beispiele für sinnvolle Maßnahmen, wenn der Sicherheitsstatus eines Gerätes kritisch wird.

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 die Möglichkeit, die bei Network Access Control üblicherweise verworfenen „alten" Daten strukturiert zu sammeln und aufzubereiten.

Neben der Live-Sicht gewinnt man durch dieses **NAC Add-On** auch eine **historische Sicht** der Netzwerkaktivitäten. 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.

Das Switch Viewer Add-On liefert mehr Details und Übersicht über die Netzwerkgeräte sowie gesichertes RADIUS-basiertes Einloggen.

BLICK INS DETAIL

Sichere Anmeldung an Netzwerkgeräten und mehr Details

Vielerorts sogar bereits gesetzliche oder regulatorische Vorgabe, ist die Authentifizierung an Netzwerkgeräten mittels eines RADIUS-Servers ein wichtiger Aspekt der Securitystrategie.

Mit **macmon Switch Viewer** werden **diverse weitere Informationen der Netzwerkgeräte** erhoben und zur Nutzung angeboten. Beispiele dafür sind die Seriennummern und weitere Portkonfigurationen.

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.

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.

Durch Scalability wird die Verfügbarkeit von macmon NAC sichergestellt und damit der Betrieb von kritischen Systemen gewährleistet.

SCALABILITY

Permanente Verfügbarkeit der Infrastruktur und der Sicherheit

Maximale Ausfallsicherheit durch flexible Hochverfügbarkeitsoptionen für lokale oder verteilte Infrastrukturen inkl. zentralem Management & Reporting = macmon NAC Scalability.

Die **skalierbare Architektur** von macmon NAC bietet die Möglichkeit, statt mit nur einem zentralen Server auch eine ganze Gruppe von Servern zu betreiben und zentral zu verwalten. So können **hochverfügbare Konzepte** für effektive NAC-Strategien umgesetzt werden.

Die Leistung von macmon NAC ist parallel aber auch durch Ressourcen innerhalb eines zentralen Systems so erweiterbar, dass verteilte Strukturen auch mit einem einzigen System abgedeckt werden können.

Der Einsatz hängt dabei stark von den Anforderungen bzw. den Zielsetzungen ab. Vom „Hidden Master"-Prinzip über einfache Ausfallsicherheit bis hin zur Kompensation von WAN-Verbindungsausfällen wird so die Verfügbarkeit von macmon NAC sichergestellt und damit der Betrieb von kritischen Systemen gewährleistet.

Der einzigartige Mischbetrieb von verschiedenen NAC-Technologien stellt zudem sicher, dass gerade kritische Systeme oder ganze Produktionsblasen auch bei einem sehr unwahrscheinlichen Ausfall der NAC-Lösung ungehindert weiter operieren.

Bidirektionaler Informationsaustausch und nahtlose Integration von macmon NAC mit Security-Lösungen anderer Hersteller.

TECHNOLOGIEPARTNER

Koppelung von 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, Identity-Integrationen 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.

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

Als Lösungsanbieter vereint Belden mit macmon NAC die Kompetenz zur sinnvollen, angemessenen und vor allem auch realisierbaren Absicherung industrieller Netzwerke.

DIE LÖSUNG

Belden & macmon NAC – Synergien zu Ihrem Vorteil

Die erfahrenen Security-Experten von macmon secure bieten seit 2003 hersteller-unabhängige Lösungen, die heterogene Netzwerke dank sofortiger Netzwerktransparenz vor unberechtigten Zugriffen schützen.
Gemeinsam mit der einzigartigen und umfassenden Erfahrung von Belden in industriellen Netzen und bei der Digitalisierung von Produktionsanlagen entsteht eine spannende Kompetenz zur sinnvollen, angemessenen und vor allem auch realisierbaren Absicherung Ihres industriellen Netzwerks.

Über 1.600 Kunden von mittelständischen Firmen bis hin zu großen internationalen Konzernen verschiedenster Branchen vertrauen beim Thema Netzwerksicherheit bereits macmon NAC. Mit seinen branchenweit meistverkauften industriellen Switches, Routern, Firewalls und Edge-Gateways ist Belden einer der weltweit größten Infrastrukturanbieter für industrielle Netzwerke.

Ein ergänzendes durchgängiges Produktportfolio – von der Verkabelung über industrielle Steckverbinder und I/O-Module, Remote Access Lösungen auf ZTNA (Zero-Trust-Network-Access) Basis, bis hin zu Dienstleistungen und Tools – macht Belden zum Partner Ihrer Wahl und liefert die Infrastruktur, die den digitalen Wandel einfacher, intelligenter und sicherer macht. Weltweit verteilte Entwicklungszentren arbeiten an maßgeschneiderten Lösungen, die eine kontinuierliche Entwicklung hin zu einer Zukunft ermöglichen, die durch integrierte KI, IoT, Cloud und Edge Computing angetrieben wird. Lassen Sie uns die Reise zu Ihrer digitalen Produktion gemeinsam vorantreiben.

macmon secure GmbH

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

macmon
intelligent einfach