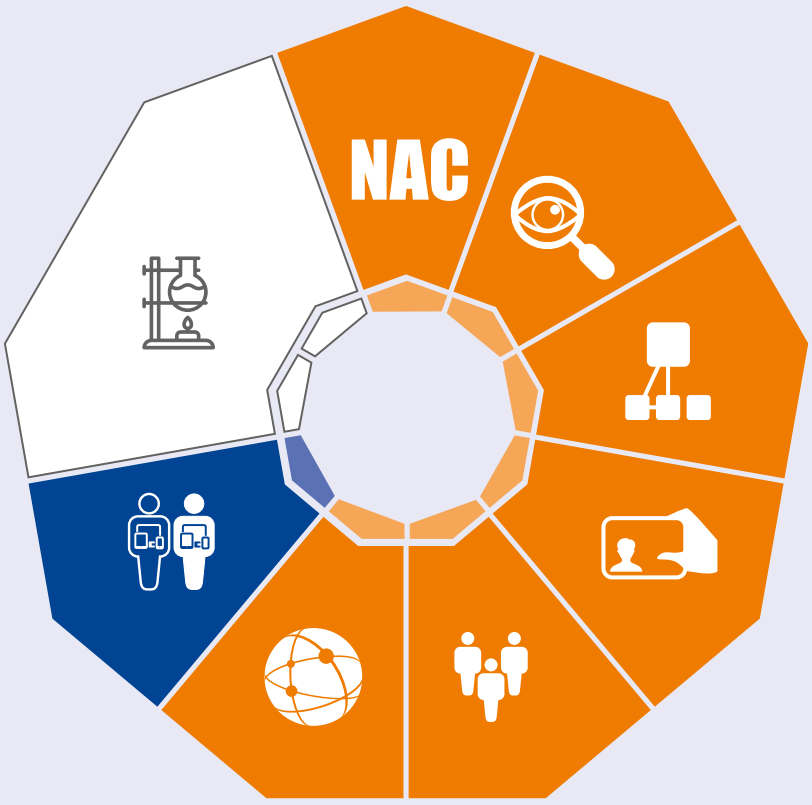
macmon

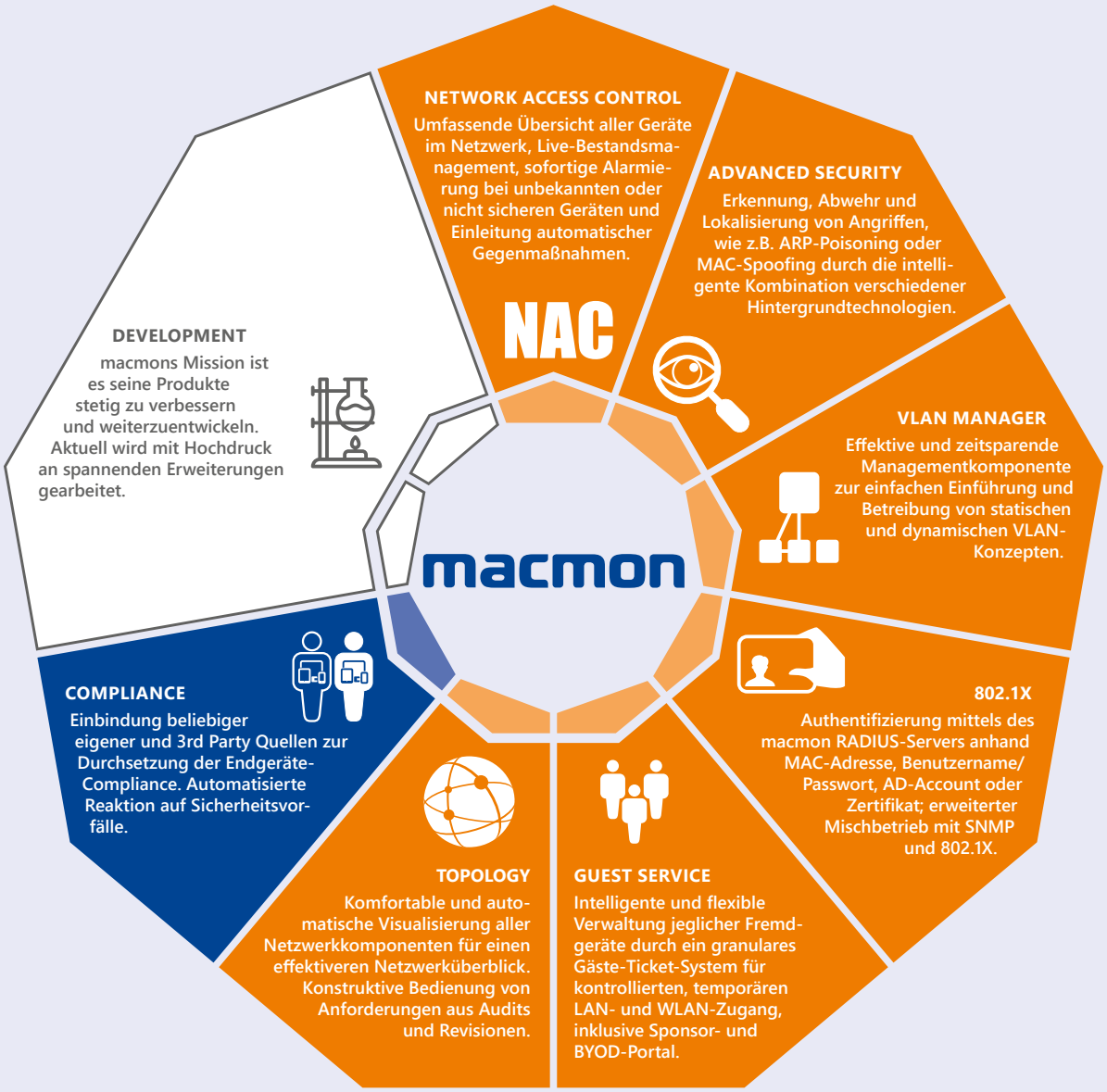
nac intelligent einfach



NETWORK ACCESS CONTROL

ÜBERSICHT. KOMFORT. SICHERHEIT.

MACMON MODULE & BUNDLES



NETWORK ACCESS CONTROL

macmon Network Access Control bietet Ihnen den Schutz, den Sie für eine effiziente Netzwerkzugangskontrolle benötigen. Es schützt Ihr Netzwerk vor dem Eindringen unerwünschter Geräte, verschafft Ihnen eine Übersicht aller Geräte in Ihrem Netzwerk und bietet Ihnen damit ein aktuelles IT-Bestandsmanagement.

Durch die zentrale Administration aller Unternehmensswitche via SNMP oder SSH/Telnet sorgt macmon NAC dafür, dass Sie die Kontrolle in Ihrem Netzwerk haben. macmon kann Sie durch switchportgenaue Regeln informieren und Zugänge gewähren oder verweigern. Das umfangreiche und benutzerspezifische Reporting bietet Ihnen stets aktuelle Auswertungen.

ADVANCED SECURITY

Um effektiv auf Angriffe zu reagieren, ist im Network Bundle das Advanced Security Modul enthalten. Aufbauend auf macmon NAC sind darin verschiedenste intelligent kombinierte Technologien eingeflossen, die bei einfachster Verwendung, effizienten Schutz bieten.

Man-In-The-Middle-Angriffe, wie ARP-Spoofing oder ARP-Poisoning werden durch die zentrale Sicherheitsinstanz erkannt und verhindert. macmon Advanced Security erkennt Systeme eindeutig und erhöht den Zugangsschutz um ein Vielfaches. Umfangreiche Systeminformationen, wie z.B. Hostname, IP-Adresse, Betriebssystem, offene oder geschlossene IP-Ports, werden im Hintergrund abgeglichen, um Adressmanipulationen und weitere Angriffsversuche vollständig zu unterbinden.

VLAN MANAGER

Mit dem macmon VLAN Manager können zentral und kinderleicht alle Vorzüge der Netzwerksegmentierung genutzt werden. Die administrativen Einsparungspotenziale sind:

- mobilen Benutzern überall im Unternehmen ihre gewohnten Ressourcen anbieten
- Umzüge von Abteilungen, einzelnen Büros oder bestimmten Systemen ermöglichen
- Gastzugänge in öffentlichen Bereichen gewährleisten
- Dienstleistern den Zugriff auf dedizierte Ressourcen gewähren
- sensible Ressourcen vor dem allgemeinen Zugriff schützen
- BSI-konforme Sicherheitskonzepte umsetzen

Mit dem macmon VLAN Manager werden sowohl statische als auch dynamische VLAN Konzepte mit geringem Aufwand eingeführt und betrieben. Auch die BSI-Empfehlung, ungenutzte Ports abzuschalten (oder in ein Unassigned VLAN zu konfigurieren) und erst bei Bedarf produktiv zu stellen, wird voll unterstützt.

802.1X

Das Institute of Electrical and Electronics Engineers (IEEE) ist ein weltweiter Verband mit Gremien für die Standardisierung von Techniken, Hardware und Software. Der Standard 802.1X stellt eine ausgereifte Empfehlung zur sicheren Authentifizierung von Geräten in Netzwerken dar. macmon unterstützt diesen Standard und erleichtert die Einführung und den Betrieb:

- Möglichkeit des gemischten Betriebs mit und ohne 802.1X
- Geräteortung durch Kommunikation mit den Switches und Access Points
- Anbindung von AD/LDAP und weiteren Identitätsquellen
- dynamisches und automatisches Regelwerk
- einfache Implementierung und kinderleichter Betrieb
- gruppenbasierte Konfiguration statt umfangreiches Regelwerk
- Etablierung und Umsetzung von Konzepten für Sicherheitszonen

GUEST SERVICE

Heute hat nahezu jede Person mindestens ein mobiles Device und erwartet überall Internetzugang. Mobile Mitarbeiter, Dienstleister, Lieferanten und Kunden benötigen jedoch häufig detaillierteren Zugriff auf bestimmte Ressourcen im Firmennetzwerk, so dass weder UMTS & LTE, noch ein komplett getrenntes Gästenetz eine ausreichende Lösung sind. Hier bietet der macmon Guest Service, auch macmon Gästeportal genannt, die ideale Lösung:

- intelligente BYOD-Lösung
- herstellerunabhängige Passung für jede Umgebung
- schnelle und einfache Inbetriebnahme
- Nutzung und Betrieb bereits bestehender Prozesse
- Entlastung der IT-Abteilung durch delegierte Genehmigungen (Sponsor-Portal)
- hochflexible Zugangssteuerung für jede Situation
- aktueller und vollständiger Überblick aller Gastgeräte

TOPOLOGY

Infrastrukturen selbst kleinerer Unternehmen werden immer komplexer und unübersichtlicher. Mit der grafischen Topologie von macmon wird das Netzwerk grafisch abgebildet, womit die Übersicht über alle angeschlossenen Geräte jederzeit möglich ist. Wird, wie in den meisten Netzwerken, das Ganze zusätzlich in virtuelle Netzwerke unterteilt und sollen darin Fehleranalysen betrieben werden, wird dies nicht nur komplex, sondern kann auch zu gravierenden Fehlentscheidungen führen:

- herstellerunabhängige Passung für jede Umgebung
- effektiv nutzbare Informationen – visualisiert
- Erfüllung von Anforderungen aus Revision & Audits
- auch im 802.1X Betrieb möglich
- Vermeidung von Fehlentscheidungen in der Netzwerkplanung
- Zurückgewinnen der vollen Netzwerkübersicht

COMPLIANCE

Durch die macmon Compliance kann, je nach Anforderung, der Compliance Status von externen Quellen empfangen, durch die Anbindung fremder Datenbanken aktiv eingeholt oder durch den macmon-Agenten ermittelt werden. Zusätzlich kann macmon Meldungen aus der Nutzung der integrierten IF-MAP-Technologie verwenden:

- flächendeckende Abbildung der Compliance Zustände durch beliebige, herstellerunabhängige Datenlieferanten und wahlweise den macmon-Agenten
- proaktive Reaktion auf Infektionsquellen
- schnelle und automatisierte Isolation von unsicheren Systemen im Netzwerk
- einfaches und schnelles Implementieren, da keine Veränderung der Infrastruktur erforderlich ist
- sofortige Erhöhung des ROI durch die Nutzung aller bereits vorhandenen Systeme und Investitionen

macmon NAC ist EAL2+ zertifiziert gemäß dem BSI-Zertifizierungreport unter www.macmon.eu\bsi-cc.

5x EINFACH

1. GRUPPENBASIERTE KONFIGURATION

Unternehmensendgeräte werden in logische Gruppen sortiert, an denen wiederum die Konfiguration für die Behandlung der Endgeräte im Netzwerk erfolgt. So können gruppenbasierte Vorgaben zu den Endgeräteeigenschaften (Betriebssystem, Domäne, IP-Ports) und die Autorisation definiert werden.
Für die Autorisation können über einfache vordefinierte Felder das VLAN und weitere Berechtigungen vorgegeben werden. Dabei können die Vorgaben für drei Level gemacht werden in Abhängigkeit von der Qualität der Identifizierung (nur MAC-Adresse = Niedrig, Benutzername & Passwort = Mittel, Zertifikate = hoch).
Durch diese Vorgaben ist macmon in der Lage, das Regelwerk selbstständig zu erstellen und zu pflegen. Manuelle Regeln müssen nur noch für Sonderfälle definiert werden.

2. 802.1X (MIT UND OHNE ZERTIFIKATE)

802.1X bzw. eine RADIUS-basierte Authentifizierung kann grundlegend über 3 Stufen erfolgen: MAC-Adresse (niedrigster Level), Benutzername & Passwort (mittlerer Level) oder Zertifikat (hoher Level). In macmon können in der gruppenbasierten Konfiguration für die verschiedenen Level unterschiedliche Berechtigungen definiert werden, um in Abhängigkeit der Ausweisqualität unterschiedliche Netzwerkzugänge zu gewähren.
Da die wenigsten Unternehmen bereits über eine fertig ausgerollte Zertifikatsinfrastruktur verfügen, ist die Wahl des mittleren Identifizierungslevels in Kombination mit AD-Konten häufig die einfachste Antwort für einen schnellen Weg zur Netzwerksicherheit.
Die größte Komplexität in 802.1X liegt jedoch in der Administration und der Pflege des RADIUS Servers, da oft eine Fülle an Regeln erstellt und gepflegt werden müssen. Egal ob 802.1X mit Zertifikaten umgesetzt werden soll oder ohne, die Produktstrategie von macmon und die damit verbundenen Vorteile wie das dynamische Regelwerk reduzieren den Aufwand und die Komplexität erheblich!

3. GÄSTE PORTAL

Das macmon Gäste Portal ist für hohe Flexibilität und verschiedenste Einsatzzwecke ausgelegt. So können beliebige Instanzen an unterschiedlichen Stellen im Unternehmen platziert und individuell gestaltet werden. Neben den mitgelieferten Sprachen Deutsch und Englisch können beliebige Sprachen (mit allen Schriftzeichen) ergänzt werden.
Es wird zwischen Gästen und Gast-Geräten unterschieden, um auch für die Besucher jede Variante abbilden zu können. So kann man bspw. bei Bedarf mehrere Geräte registrieren oder einen Dauergutschein erhalten, während man sein Gerät zwischendurch wechselt.
Das integrierte Sponsor-Portal erlaubt die Delegierung der Gutscheinerstellung und -verwaltung an beliebige Mitarbeiter im Unternehmen über einfache AD-Gruppenmitgliedschaften. Das Sekretariat kann somit z.B. Gäste zulassen ohne die IT-Abteilung in Anspruch nehmen zu müssen.
Das ebenfalls enthaltene BYOD-Portal bietet zudem die Chance, einen Überblick über die Mitarbeitergeräte zu erhalten.
Nicht verwaltete Endgeräte, wie z.B. Mitarbeitersmartphones (kein Unternehmenseigentum) können durch den Mitarbeiter selbst registriert werden, wenn er das Recht dafür erhält.

4. EFFEKTIVE VLAN-BERECHNUNG

Zur weiteren erheblichen Vereinfachung des Regelwerkes und zur Unterstützung bei der Abbildung mehrerer Standorte oder gewachsener Infrastrukturen bietet macmon die einzigartige Funktion der Berechnung des effektiven VLANs.
Wird ein Endgerät im Netzwerk gesehen (sowohl per SNMP als auch per 802.1X), so errechnet macmon – falls notwendig – das Ziel-VLAN anhand verschiedener Informationen, um immer das in der Situation passende VLAN zu konfigurieren.
Dabei wird einbezogen, ob an dem Endgerät in macmon ein VLAN vorgegeben wurde, das Endgerät gerade compliant ist oder nicht, bzw. ob an der Endgerätegruppe ein oder mehrere VLANs vorgegeben wurden und welche VLANs der betroffene Switch beherrscht. Es können VLAN-IDs und VLAN-Namen verwendet werden, um jede Situation abbilden zu können.
In größeren Umgebungen führt dies oft sogar zu einem erheblichen Performancevorteil, da die Anzahl der Regeln die für jede Authentifizierung durchlaufen werden müssen viel geringer ist als bei jedem anderen NAC-Produkt.

5. AD-INTEGRATION MIT MAPPING

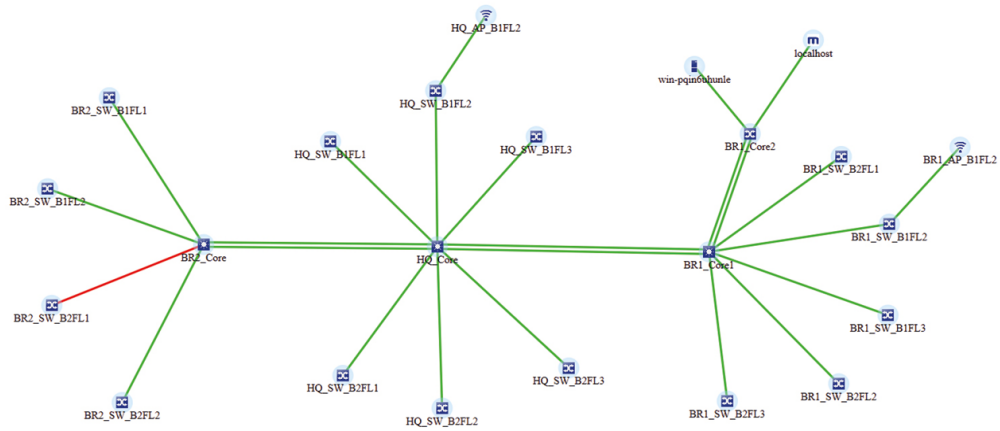
macmon bietet die Möglichkeit der Authentifizierung von Endgeräten mittels ihrer Active Directory Konten (Identitäten) oder auch allgemein LDAP Konten. Dabei können sowohl Benutzerkonten als auch Gerätekonten verwendet werden. Da keine Zertifikate ausgerollt werden müssen, wird so die Einführung von 802.1X erheblich vereinfacht.
Mittels eines einfachen Mappings können dann die AD-Gruppen mit den macmon Endgerätegruppen verknüpft werden. Das bestehende Regelwerk gilt automatisch auch für AD-Gruppen. Für den Fall, dass Endgeräte mal mit der MAC-Adresse und mal mit einem AD-Konto im Netzwerk auftauchen, müssen keine zusätzlichen Regeln konzipiert und angelegt werden.
Durch die Integration und das Mapping können die MAC-Adressen der Endgeräte während der Authentifizierung gelernt und entsprechend dem Mapping in die richtige Gruppe sortiert werden.
So ist es möglich, Endgeräte auf einfachem Wege mit einer höherwertigen Qualität als der MAC-Adresse zu identifizieren.
Über die Wahl der Integration kann unterschieden werden, ob die Netzwerkabteilung entscheidet, welches Gerät welchen Zugang erhält oder ob diese Entscheidung durch die AD-Administratoren getroffen wird.

VORTEILE MIT MACMON

- ✓ Einführung innerhalb eines Tages und intuitives tägliches Handling
- ✓ SNMP & Mischbetrieb mit und ohne 802.1X
- ✓ AD-Integration sowie automatisches und dynamisches Regelwerk
- ✓ Herstellerunabhängig
- ✓ Kostenersparnis durch Verwendung bereits vorhandener Ressourcen
- ✓ Sofortige Netzwerkübersicht mit grafischen Reports und stets aktueller Topologiedarstellung
- ✓ Deutscher Hersteller-Support
- ✓ Live-Bestandsmanagement
- ✓ Hochflexibles Gästeportal zum Zulassen von Mitarbeiter- und Gastgeräten

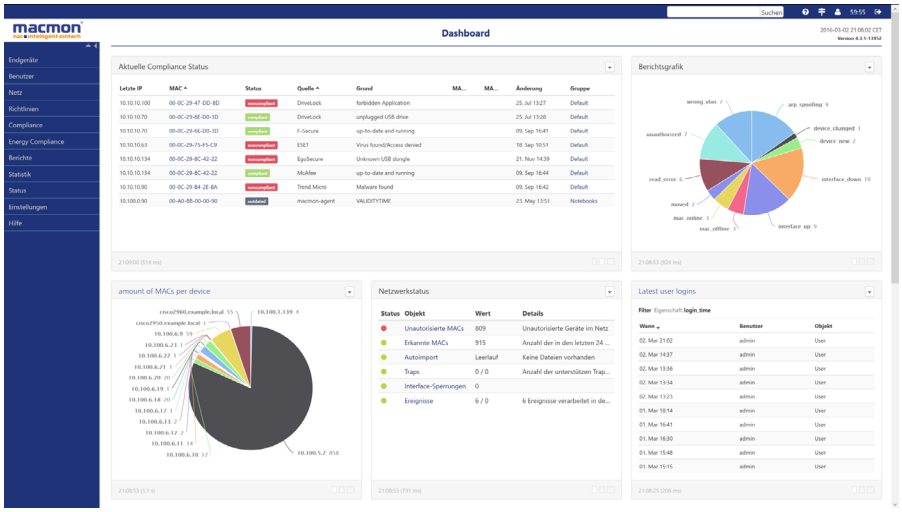
MEHRWERTE MIT MACMON

- ✓ Reduzierung von administrativem Aufwand
- ✓ Live-Bestandsmanagement
- ✓ Einfache und schnelle Netzwerk-Analyse
- ✓ Erweiterte Sicherheit durch Kopplung mit anderen IT-Sicherheitsprodukten
- ✓ Zentrale Macht im Netzwerk
- ✓ Grafische Visualisierung des gesamten Netzwerks
- ✓ BSI-zertifizierte NAC-Lösung



AUTHENTIFIZIERUNG UND AUTORISIERUNG

Die Authentifizierung und Autorisierung der Geräte im Netzwerk erfolgt ganz nach den Gegebenheiten und Möglichkeiten der Infrastruktur. macmon kombiniert dafür SNMP mit dem Standard 802.1X und bietet Ihnen so die Vorteile von beiden Technologien in einem Regelwerk. Von der MAC-Adresse kombiniert mit weiteren Systeminformationen, bis hin zum Industriestandard IEEE 802.1X mit seinen verschiedenen Ausprägungen, (wie z.B. Benutzername/Passwort, Active Directory/LDAP-Konto, Identitäten aus fremden weiteren Quellen, Zertifikat), sind alle Möglichkeiten enthalten.



6 GRÜNDE FÜR NETWORK ACCESS CONTROL

Übersicht, Komfort & Sicherheit im Netzwerk gewinnen

Mit macmon NAC lassen sich jederzeit alle im Netzwerk befindlichen Geräte erkennen. Die eingesetzten PCs, Drucker, Laptops und medizinischen, technischen und sonstigen Geräte werden effizient überwacht und vor unbefugten Zugriffen geschützt. Mithilfe eines dynamischen Managements der Netzwerksegmente können im Gäste Portal Gast- und Mitarbeitergeräte (BYOD) einfach und sicher zugelassen werden.
macmon NAC ermöglicht Ihnen neben sofortiger Netzwerktransparenz für LAN und WLAN auch die Einhaltung aktuell gültiger IT-Sicherheitsstandards (u.a. DIN ISO 27001 oder DIN 8001-1). Die Software kann innerhalb eines Tages und ohne Veränderungen der bestehenden Infrastrukturen implementiert werden.

Übersicht

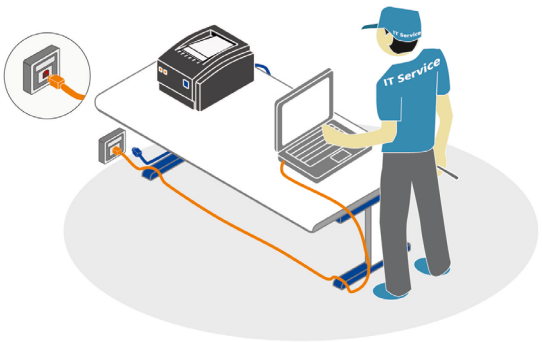
Ein Administrator verschafft sich den Überblick über das Netzwerk mit vielen Standorten durch die Visualisierung der Netzwerkkomponenten.

Ein externer Mitarbeiter schließt sein Notebook an und verbindet sich per LAN oder WLAN mit dem Firmennetzwerk.

Komfort

Ein Mitarbeiter zieht innerhalb des Unternehmens um und benötigt Zugriff auf die gewohnten Ressourcen.

Ein Externer verbindet sein Gerät mit einem Port, an dem vorher ein Drucker angeschlossen war.



Sicherheit

Ein Mitarbeiter hört Internetradio, welches mit dem Unternehmens-WLAN verbunden ist.

Ein Dienstleister / Fremder schließt sein Notebook an eine Unternehmens-Dockingstation an und erhält Vollzugriff im Netzwerk.

macmon secure GmbH
Alte Jakobstr. 79-80 | 10179 Berlin
Telefon +49 30 2325 777-0 | Telefax +49 30 2325 777-200
nac@macmon.eu | www.macmon.eu