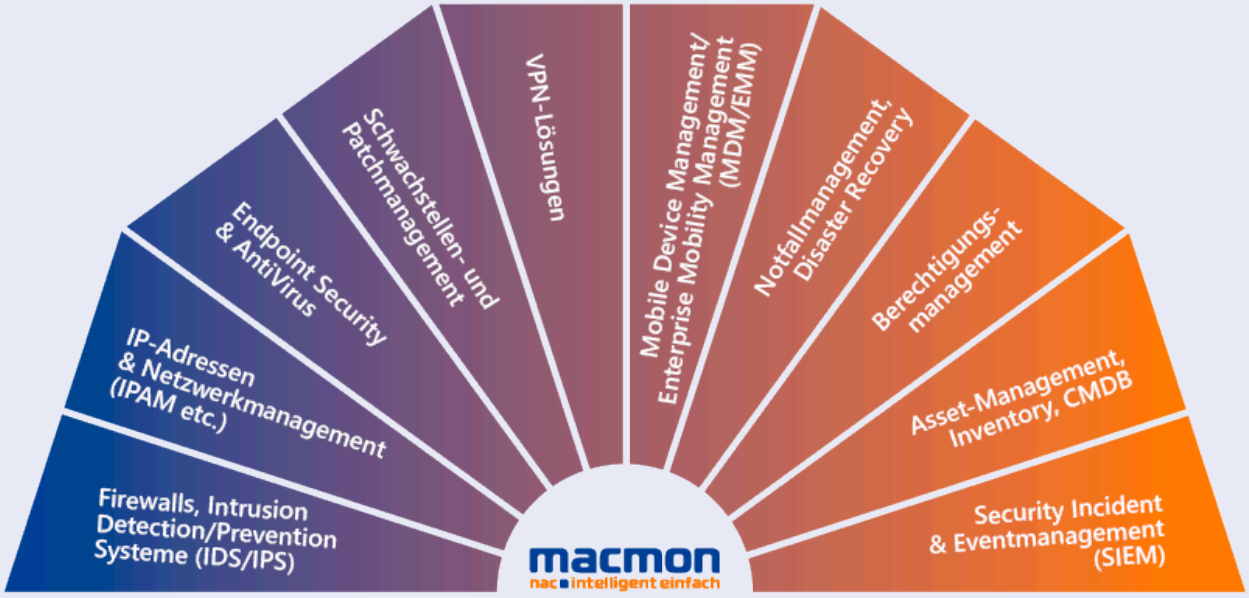
TECHNOLOGIEPARTNERSCHAFTEN FÜR IHRE SICHERHEIT

Koppeln Sie macmon Network Access Control (NAC) mit führenden Sicherheitslösungen und erzielen Sie echte Mehrwerte!

Unsere selbst entwickelte NAC-Lösung macmon liefert Ihnen nicht nur die beste Antwort darauf, wie Sie ungesicherte Netzwerkzugriffe verhindern können, macmon NAC lässt sich nahtlos in andere Security-Produkte integrieren: z.B. Endpoint Security Lösungen, Notfallmanagement und Firewalls/IPS. Wir nutzen unsere langjährigen Technologiepartnerschaften mit namhaften Herstellern von Security-Produkten wie Certex tenfold, CONTECHNET, EgoSecure, ExtraHop, NCP, F-Secure und vielen weiteren, um den Wissensaustausch voranzutreiben.

Profitieren Sie von weitreichenden Möglichkeiten, damit Ihre komplexen Anforderungen optimal erfüllt werden. Nutzen Sie diesen Wissensvorsprung und sichern Sie sich echte Mehrwerte durch Produktintegrationen.



Unsere Produktintegrationen schaffen echte Mehrwerte!

CONTECHNET

Mit der INDART Professional Lösung von **CONTECHNET** erlangt ein Unternehmen in 8 Schritten einen softwaregestützten Notfallplan.
Dank der Integration von INDART und macmon, können Informationen über Router, Switche und Server permanent von macmon eingeholt werden und damit das Notfallhandbuch aktualisieren. Sind die definierten Systeme im Netzwerk nicht mehr sichtbar oder tauchen neu auf, so wird innerhalb von INDART automatisch eine entsprechende Dokumentations-Aktion eingefordert.

EGOSECURE

ENJOY DATA PROTECTION

Die Endpoint Security Lösung von **EgoSecure** schützt Unternehmen vor Datenverlust, z.B. durch unerlaubte USB-Sticks oder Malware.

Durch die Kopplung wird der Compliance Status von Endgeräten an macmon übertragen, um nicht konforme Geräte vom Netzwerk zu trennen oder in Quarantäne zu verschieben, sowie nach der „Heilung" zurückzuführen. Ergänzend bietet EgoSecure die Option einen Compliance-Verstoß auch bei beliebigen auftretenden Ereignissen wie „unerlaubte Applikation ausgeführt", „zu viele Daten auf einen USB-Stick kopiert" und vielen anderen direkt an macmon zu eskalieren.

ExtraHop

ExtraHop bietet Echtzeitanalyse und Visualisierung von Leitungsdaten.
Durch die Integration mit macmon können Endgeräte, zu denen durch ExtraHop anomale Aktivitäten, wie z.B. „extrem häufige Login-Versuche auf einem Server" oder „Ransom-Ware Aktivität festgestellt" gefunden wurden, automatisch vom Netzwerk isoliert werden.

F-Secure gehört zu den führenden Anbietern von Endpoint Security- und insbesondere AntiMalware-Lösungen.
Der direkte Draht zwischen den Entwicklungsabteilungen sorgt dafür, dass die verschiedenen Versionen kompatibel zueinander sind und macmon auf Ereignisse von F-Secure, wie kritische Virenfunde, mittels des AntiVirus Connectors gezielt und schnell reagieren kann.

Infoblox ist eine Lösung, die Netzwerkdienste wie DNS oder DHCP auf eine einfach zu bedienende Weise bereitstellt. Da für diesen Zweck durchgängig mit denselben Daten gearbeitet werden muss, wie sie macmon zur Netzwerkzugangskontrolle verwendet, ist diese Kombination ideal.
Unter Verwendung der jeweiligen offenen Schnittstellen ist es möglich, die Datenbestände miteinander abzugleichen und dabei die Gruppenzugehörigkeit zu spiegeln. Eine Pflege der Systemdaten, wie z.B. MAC-Adresse oder IP-Adresse, muss nur noch an einer Stelle stattfinden. Sowohl Infoblox als auch macmon selbst verfügen über entsprechende Automatismen, die eine permanent aktuelle Übersicht effektiv gewährleisten.

MobileIron als führende Mobile Device Management (MDM) Lösung sichert, verwaltet und überwacht alle unternehmenseigenen bzw. mitarbeitereigenen Mobilgeräte, die auf unternehmenskritische Daten zugreifen.
Durch die Integration mit macmon NAC sind automatisch alle verwalteten mobilen Geräte auch unserer NAC-Lösung bekannt, und können im Netzwerk direkt zugelassen werden. Das einzigartige Mapping von macmon erlaubt dabei eine direkte Verlinkung von macmon Gruppen und MobileIron Labels. Die Steuerung der Zugriffe ist dadurch ohne manuelle Regeln möglich. Gleichzeitig kann der Compliance Status der Endgeräte mit übertragen werden, so dass Geräte, die laut MobileIron Richtlinie nicht den Sicherheits-anforderungen entsprechen, automatisch isoliert werden.

NCP ist Anbieter von Remote Access VPN-Lösungen für den hochsicheren Fernzugriff auf zentrale Datenbestände und Ressourcen.
macmon kann die Systeme und Benutzer, die gerade per NCP-VPN mit dem Netzwerk verbunden sind, darstellen und – falls notwendig – eine VPN-Verbindung aktiv beenden.

Eine Portallösung, um Benutzer und Berechtigungen zentral und übersichtlich zu verwalten, bietet **Certex tenfold.**
Es regelt z.B. die Rechte, eigene oder Gast-Geräte zum Netzwerk zuzulassen oder zu sperren.
Über das macmon Gäste-/BYOD-Portal sind diese Genehmigungen entsprechend sofort verfügbar. Bei direkter Sperrung des AD-Kontos wird gleichzeitig dem registrierten Gerät der Zugriff zum Netzwerk verwehrt.

MACMONS MULTIPLE COMPLIANCE

Die sogenannte „multiple Compliance" Funktion von macmon ist im Compliance Modul enthalten. Dieses ist Bestandteil des macmon Premium Bundles. Sie bietet die Möglichkeit beliebige Quellen in Form von z. B. Sicherheits-Software anzubinden, die in der Lage sind einen Compliance Status von Endgeräten zu liefern. Dabei erfolgt die Übertragung mittels eines einfach zu verwendenden https Aufrufs, welcher durch die Quelle oder eine entsprechende Middleware erfolgen muss. Ein Aufruf erfordert dabei 4 Details und setzt sich wie folgt zusammen:

https://macmon-host/macutil/?compliance&address=**MAC-ADRESSE-DES-ENDGERÄTES**&source=**QUELLE**&reason=**GRUND-DES-STATUS**&status=**NONCOMPLIANT**

macmon übernimmt dabei den gelieferten Status für das jeweilige Endgerät und führt Aktionen gemäß des Regelwerkes aus (Isolieren, Alarmieren, Re-integrieren). Da die Anbindung immer durch das jeweils andere System erfolgen muss, erfordert die Anbindung jedoch das Wissen über die Möglichkeiten des betreffenden Systems. Für viele Produkte gibt es bereits Whitepaper und Beschreibungen zu der Integration. Das macmon Team übernimmt gerne die Unterstützung bei der Anbindung weiterer Compliance-Quellen und arbeitet gemeinsam mit Ihnen und dem Experten für das liefernde System die Umsetzung aus. Sprechen Sie uns hier gerne an, welche Integrationen Sie realisieren möchten und welche Erfahrungen wir dazu bereits mitbringen können.

AUTOMATISCHE ISOLATION INFIZIERTER ENDGERÄTE
MACMON ANTIVIRUS CONNECTOR

Conficker und andere MalWare-Ausbrüche haben gezeigt, dass in der Regel jede manuelle Reaktion oft zu spät erfolgt. Daher bietet macmon durch die zentrale Kontrolle der Netzwerkzugänge und seine offene Architektur die machtvolle Position, genau hier automatisiert zu unterstützen. Mit dem macmon AntiVirus Connector wurde eine Schnittstelle zwischen der NAC-Lösung macmon und gängigen AntiVirus Lösungen wie F-Secure, G Data, Kaspersky, McAfee, Sophos, Symantec (MS SQL) oder TrendMicro (MS SQL) geschaffen, die automatisch reagiert, wenn der VirenScanner einer Bedrohung einmal nicht mehr Herr werden kann.

Betroffene Clients werden schnellstmöglich aus dem Netzwerk ausgesperrt – durch das Herunterfahren des Switchports sogar physikalisch – und Sie werden umgehend über die Maßnahme informiert. Sie erfahren, um welches Endgerät es sich handelt, wo es sich befindet und Sie werden in die Lage versetzt, das betroffene System in aller Ruhe säubern und wieder in Betrieb nehmen zu können.

SCHNITTSTELLEN

Als Anwender der NAC-Lösung macmon profitieren Sie nicht nur vom hohen Sicherheitsniveau der Software bei einfachem Handling und Betrieb, sondern insbesondere auch von der Schnittstellenfähigkeit mit anderen führenden Security-Produkten. Dazu zählen neben gängigen AntiVirus Lösungen auch Endpoint Security, IT-Notfallmanagement, Intrusion Detection oder Prevention Systeme (IDS/IPS), Asset Management, Inventory, Security Incident & Event Management (SIEM).

BlueCat Networks

Die BlueCat IP-Adressmanagement (IPAM)-Lösung vereinheitlicht mobile Sicherheit, Adressmanagement, Automation und Self-Services. Die Schnittstelle zu BlueCat ermöglicht den Import von DHCP-Daten bzw. DHCP-Leases. Mit deren Hilfe werden die in macmon verwendeten Daten nochmals mit DHCP-Hostnames und IP-Verbindungen angereichert. Dies verbessert u.a. die Erkennung und damit den Schutz vor ARP-Spoofing Angriffen.

Matrix42 – Empirum

Matrix42 bietet mit Empirum eine zentrale Instanz zur Standardisierung der Endgerätesoftware und zum allgemeinen Endpoint Management. Durch die Kombination mit macmon entstehen gleich zweierlei Möglichkeiten: Bei einem Compliance-Verstoß, der von Empirum aufgedeckt wird, kann macmon einfach über die Compliance Schnittstelle informiert werden und übernimmt die Isolation des gefährlichen Systems. Um auf beiden Seiten einen einheitlichen Stand des Inventars zu gewähren, kann die Liste der im Netzwerk zugelassenen Systeme von macmon mit der Inventarliste von Matrix42 abgeglichen werden. Je nach Wunsch und bestehenden Prozessen kann dabei ein System die Führung übernehmen.

McAfee

McAfee zählt zu den größten Security Anbietern der Welt und bietet mit dem ePolicy Orchestrator (ePO) ein zentrales Management für diverse Sicherheitslösungen. Durch die Anbindung über macmons multiple compliance, kann zu nahezu beliebigen Ereignissen bei den McAfee Produkten, eine automatische Alarmierung an macmon erfolgen. Auf diese Weise als „Nicht-Compliant" markierte Endgeräte werden automatisch in dafür vorgesehene Netzwerkbereiche verschoben. Mittels des flexiblen Regelwerks in macmon kann dabei einfach, je nach Art des Ereignisses, unterschiedlich reagiert werden.

Restorepoint

Restorepoint ermöglicht es, von zentraler Stelle Backups und Restore Funktionalitäten für diverse Produkte durchzuführen und dabei die Backups chronologisch zu archivieren und wieder nutzbar zu machen. Durch die direkte Anbindung zu macmon, werden die Konfiguration sowie die Installation der macmon Appliance automatisch und zeitgesteuert abgerufen. Im Vergleich zur bereits vorhandenen macmon Funktion – Backups zeitgesteuert zu erzeugen und abzulegen – bietet Restorepoint damit einen zentralen Ansatz, der gerade im Havarie Fall für schnellere Reaktionen sorgt.

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

Ihr Ansprechpartner: