TECHNOLOGIEPARTNERSCHAFTEN FÜR IHRE SICHERHEIT

macmon
nac intelligent einfach

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.
Wir unterscheiden dabei grundlegend die Kategorien Compliance-Anbindungen, Infrastruktur-Anbindungen, Asset-Management und Identitätsquellen wobei letztere zwei Kategorien bidirektional erfolgen können. Einige Hersteller bieten auch Integrationen zu mehr als einer Kategorie an, aber die Unterscheidung lässt eine Einteilung nach Einsatzzwecken zu, die Ihnen helfen soll, die für Sie effektivsten Anbindungen zu erkennen.
Im Folgenden stellen wir Ihnen Integrationen mit langjährigen Technologiepartnern vor – ist Ihre bevorzugte Lösung nicht dabei, sprechen Sie uns gerne an um gemeinsam die Möglichkeiten zu evaluieren.

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!

Barracuda

Die CloudGen Firewalls von **Barracuda** sind weltweit zur sicheren Anbindung aller Unternehmensstandorte, Absicherung von Unternehmensnetzwerken direkt am Perimeter aber auch zwischen Netzwerksegmenten im Einsatz. Der Schutz vor unberechtigten Zugriffen, Malware, Advanced Persistent Threats oder auch das Auffinden von durch Bot-Netzen übernommenen Endgeräten direkt an den Gateways, wird durch die Integration mit macmon auf jegliche Eintrittspunkte zu Unternehmensnetzwerken ausgedehnt.
Während macmon die ARP Informationen aus den Firewalls ausliest, informieren die CloudGen Firewalls von Barracuda macmon auch aktiv über erkannte Bedrohungen, um die betroffenen Endgeräte automatisch vom Netz zu trennen oder in Quarantäne zu verschieben. Gleichzeitig werden die Informationen über die Endgeräte im Netzwerk aktiv von macmon an Barracuda übertragen, um so passenden Richtlinien zuzuweisen. Die Kommunikationsregeln zwischen zwei getrennten Netzwerksegmenten erfolgen dadurch nicht mehr nur segmentbasiert, sondern auf Basis von Gerätegruppen – die Mitglieder dieser Gruppen werden dabei durch macmon anhand der aktiven Erkennung gepflegt, was stets aktuelle, gerätegenaue Kommunikationsregeln gewährleistet. Auch Gastnetzwerke können durch die Barracuda CloudGen Firewall effektiv vom restlichen Netzwerk getrennt werden, um durch macmon registrierten und genehmigten Gastgeräten sehr granulare Zugänge wie z.B. Internet aber ohne YouTube und Peer2Peer zu gewähren.

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 Dokumentationsaktion eingefordert.

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 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 „RansomWare Aktivität festgestellt" gefunden wurden, automatisch vom Netzwerk isoliert werden.

Die **finally safe** Advanced Threat Detection Appliance (ATD) analysiert die gesamte Layer 2- bis Layer 7-Kommunikation und bietet durch die so korrelierten Daten essentielle Informationen über die Sicherheit. Dabei erkennbare Angriffe erfordern in der Regel sofortige Maßnahmen, die durch die Network Access Control-Lösung macmon in Echtzeit umgesetzt werden. Durch die direkte Kopplung der beiden Systeme und die damit verbundene automatisierbare Reaktion auf Angriffe und Anomalien können infizierte Maschinen isoliert werden, noch bevor eine Bedrohung von Sicherheitsexperten eingehend analysiert wird. Malwarekommunikation oder Botnetzverbindungen von infizierten Endgeräten, genau wie das Aufdecken von versteckten Kommunikationskanälen, sind dabei nur 3 der wichtigsten Situationen, in denen die Integration die Reaktionszeit von „Nicht sichtbar & nicht reagiert" auf nahezu null reduziert.

FireEye Network Security ist eine effektive Cybersicherheitslösung, die komplexe, gezielte und im Internetverkehr versteckte Angriffe in Echtzeit aufdeckt und abwehrt und damit das Risiko kostspieliger Sicherheitsverletzungen senkt. Zudem liefert FireEye Network Security binnen weniger Minuten konkrete Beweise, verwertbare Daten und Handlungsempfehlungen für die effektive Behebung der aufgedeckten Sicherheitsvorfälle.
Mit FireEye Network Security können sich Unternehmen effektiv vor Bedrohungen schützen – unabhängig davon, ob diese eine Schwachstelle in Windows, Apple OS X oder einer bestimmten Anwendung ausnutzen, ob der Hauptsitz oder eine Niederlassung angegriffen wird und wie gut die Bedrohung in dem umfangreichen eingehenden Internetdatenverkehr versteckt ist, der in Echtzeit überwacht werden muss.

F-Secure gehört zu den führenden Anbietern von Endpoint Security- und insbesondere AntiMalwarelösungen.
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-Konnector gezielt und schnell reagieren kann. Ergänzend ermittelt macmon NAC zyklisch die Informationen zu dem Alter der Virensignaturen von allen bekannten Endgeräten und stuft diese darauf basierend als „Compliant" oder „Non-Compliant" ein. Neben der vollständigen Übersicht zum Compliance Status können Geräte mit veralteten Signaturen so automatisch in Quarantäne verschoben werden.

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.

MICROSENS GmbH & Co. KG steht für Fiber Optic Solutions und als einer der Pioniere von Glasfaser-Übertragungssystemen deckt das international agierende Unternehmen sämtliche Leistungsbereiche der Glasfasertechnologie ab. macmon NAC liest ARP-Informationen aus Netzwerkswitches von Microsens aus und ermöglicht damit, dass Endgeräte, deren Zustand den Unternehmensrichtlinien widersprechen, isoliert oder physikalisch vom Netzwerk getrennt werden können.

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 Sicherheitsanforderungen entsprechen, automatisch isoliert werden.

NCP ist Anbieter von Remote Access VPN-Lösungen für den hochsicheren Fernzugriff auf zentrale Datenbestände und Ressourcen.
Im Zusammenspiel mit macmon werden die Systeme und Benutzer, die gerade per NCP-VPN mit dem Netzwerk verbunden sind, dargestellt und – falls notwendig – die zugehörige VPN-Verbindung aktiv beendet. Darüber hinaus sorgt die Integration vor allem dafür, dass nicht mehr nur die Identität des VPN-Zugangs geprüft wird (z.B. Zertifikat oder AD-Konto) sondern auch die Identität des Endgerätes. Zeitgleich werden so mehr Merkmale kontrolliert um sicherzustellen, dass nur autorisierte Mitarbeiter mit autorisierten Endgeräten Remote-Zugang zum Unternehmen erhalten. Fremden Geräte mit kopierten oder kompromittierten Zugangsdaten kann somit einfach der Zugang verwehrt werden

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.

Eine Portallösung, um Benutzer und Berechtigungen zentral und übersichtlich zu verwalten, bietet **Certex tenfold**.
Es regelt z.B. die Rechte, eigene oder Gastgeräte 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 Übertragungmittels 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, reintegrieren). 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.

Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu