# SUBSTANTIAL TECHNOLOGY PARTNERSHIPS FOR YOUR SOLID SECURITY

## Connect reliable macmon Network Access Control (NAC) with leading security solutions and profit from real benefits!

**Our in-house developed NAC solution is not only the answer to ideally protect your network against unauthorized access, but our product also offers a way to seamlessly integrate with other security solutions.**
**We differentiate between integrations with endpoint compliance platforms, whole infrastructures, asset management systems and identity stores, whereas asset management systems and identity stores can be bi-directional integrations. Some vendors offer more than just one integration of different types, but to identify which is the right one for you we classified them this way.**
**Below you will find our long-term partnerships with leading technology brands - if your preferred brand is not on the list, talk to us so we can evaluate a potential integration.**

**Take advantage of this opportunity and profit from our sophisticated interface to meet your high standards. Make use of this advantage and get true benefits from our product integrations.**


## True product integration offers you:

**Barracuda** CloudGen Firewalls include full next-generation security paired with all network optimization and management functionality today known as Secure SD-WAN. The integration with macmon expands the protection on the corporate network at any entry point against unauthorized access, malware, Advanced Persistent Threats and detection of bot-controlled endpoint devices immediately at the gateway.
While macmon gathers ARP information from all devices on the network and enforces policies at the MAC level, Barracuda CloudGen Firewalls with Advanced Threat Protection and Botnet detection sends macmon live updates on identified threats at the client. Subsequently affected endpoint devices can be either automatically disconnected from the network or moved to a quarantine segment. At the same time, macmon reports information on detected endpoints, allowing enforcement of appropriate security policies with Barracuda CloudGen Firewall. Communication policies that apply between two network segments, are not only segment based anymore, but also endpoint group based. Group member lists are continuously being maintained through macmon's active endpoint discovery, which leads to your communication policies always being up to date. Guest devices are also being separated from the rest of the network by the Barracuda CloudGen Firewall. macmon will allow these guest devices to pass a registration process that lets you granularly define what type of access is granted, for example only access to the web, but not to YouTube or peer-to-peer.

With INDART Professional®, **CONTECHNET** offers a modular software solution for creating and maintaining a complete IT emergency planning. Thanks to the integration of INDART Professional®, relevant data is continously fetched from routers, switches and servers by macmon. The emergency reference list is always kept up-to-date. In case any of the registered systems becomes unreachable, or a new system shows up, appropriate action is requested as defined in the emergency documentation.

**EgoSecure** is a market-leading vendor of data security solutions and protects organizations from data loss, malware and unauthorized devices, e.g. USB drives. The connection with EgoSecure makes it possible to pass the compliance status of endpoints to macmon. This enables the isolation of non-compliant devices from the network or their movement to a quarantine segment as well as transfering them back after their cure. Additionally, EgoSecure informs macmon straight away about any type of breach of compliance, for instance “unauthorized application executed” or “too much data copied to USB drive” and more.

**ExtraHop** offers real-time wire data analytics and visualizations of it. By integrating with macmon, endpoints can be isolated from the network instantaneously, when, for example, an unusual activity takes place, like a large number of login attempts in a short time period to a server or database, which is detected by ExtraHop.

The **finally safe** Advanced Threat Detection Appliance (ATD) analyzes all layer 2 to layer 7 communications, providing essential security information through correlated data. Identifiable attacks typically require immediate action that can be implemented in real-time by macmon NAC. The direct connection of both systems and the corresponding automated response to attacks and anomalies can isolate infected machines before a threat is thoroughly analyzed by security experts. Malware communications or botnet connections from infected devices, just like uncovering hidden communication channels, are only 3 of the most important situations where the integration reduces the response time from “Not visible & not responded” to near zero.

FireEye Network Security helps organizations of all sizes minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic. At the core of FireEye Network Security is the Multi-Vector Virtual Execution™ (MVX) and Intelligence-Driven Analysis (IDA) technologies. MVX is a signature-less, dynamic analysis engine that inspects suspicious objects to identify targeted, evasive and unknown threats. The IDA engines detect and block malicious objects based on machine-, attacker- and victim-intelligence.

**F-Secure** is one of the leading software providers of Endpoint Security and, in particular, Anti Malware Solutions.
The close collaboration of both developer teams at macmon secure and F-Secure makes sure that all macmon versions are compatible with F-Secure. It also enables macmon to take specific measures against critical virus events and act on them quickly.

**Infoblox** is a solution that provides network services such as DNS or DHCP in a simple way. This combination is ideal, because the solution works universally with the same data that macmon uses for Network Access Control. Using the available open interfaces, it is possible to synchronize the databases with each other and to mirror the group memberships. The maintenance of system data such as MAC addresses or IP addresses only needs to be done in one place. Both Infoblox and macmon have corresponding automatisms that guarantee an effective and up-to-date overview.

**MobileIron** is the leading Mobile Device Management (MDM) solution that keeps track, manages and monitors all corporate devices and mobile BYOD devices that have access to sensitive information within the organization. The integration of MobileIron allows you to read out all managed mobile devices to populate the list of known endpoints in the macmon NAC solution. This enables it allowing or denying them to access the network. The unique approach to mapping those devices enables you to link a MobileIron label to a group in macmon. You do not need to do any manual policy enforcement to control access on your network. At the same time, the compliance status can also be passed and in case MobileIron identifies a device as non-compliant, macmon is going to isolate the device.

**NCP** is a vendor of Remote Access VPN solutions for high-security remote access to central datasets and resources. macmon can display the systems and users that are currently connected to the network via NCP VPN and - if necessary - shut down a VPN connection.

**Restorepoint** is a solution that you can backup and restore a variety of products with. You can chronologically archive their configuration and make your backups available again later. The deep integration of Restorepoint allows you to save the configuration and installation data of your macmon appliance. This process is automated and can be scheduled as well. On top of macmon's own back-up feature, that takes care of your scheduled backups in the background, Restorepoint centralizes this approach and is especially useful and quick in unexpected crash scenarios.

**Tenfold** offers a web-based portal that centrally manages users and their permissions. It manages the permission to register both employee and guest devices- or to deny their access to the network. Combined with macmon's guest/BYOD portal, these permissions are instantly available. When an Active Directory account becomes inactive, the corresponding endpoint is also being locked out of the network.

## macmon's Multiple Compliance Module

macmon's Multiple Compliance Module is part of macmon's Compliance approach, which is included in the Premium Bundle. Multiple Compliance enables you to connect to various platforms at the same time, which can report on the compliance status of an endpoint. To pass the status, you use a simple HTTPS request which can either be called from the source platform or from a middle-ware client. A request is made of 4 parameters:

https://macmon-host/macutil/?compliance&address=**ENDPOINT-MAC-ADDRESS**&source=**SOURCE-PLATFORM**&reason=**REASON-OF-WHY**&status=**NONCOMPLIANT**

macmon analyzes the information and takes the appropriate actions in accordance with your policies (isolate, alert, re-integrate). When you integrate with other security platforms in macmon, the particular system becomes the initiator. That requires you to know what the particular platform is capable of. For many solutions whitepapers and guides to accomplish such integration are available. We at macmon are happy to assist you. Please do not hesitate to tell us about what solution you want to integrate with and to ask if we had experience with a particular solution.

## Automated isolation of infected endpoints - macmon Antivirus Connector

Various malware attacks in the recent past have shown, that a manual reaction to such threats is most of the time too slow. macmon controls your network access centrally and puts you with its open architecture in a powerful position to automate this process.

With the macmon Antivirus Connector an interface between macmon and common Antivirus solutions such as McAfee, Kaspersky, Sophos, Symantec (MS SQL), G Data, F-Secure or TrendMicro (MS SQL) is available. It instantaneously takes over if the virus scanner cannot handle the threat on its own. As a result, affected clients can be locked out of the network by isolation or on a hardware basis and you will be notified of the event right away. You know which endpoints were affected, where on the network the endpoint is connected, so that you can clean the affected system and have it resume normal operation afterwards. The macmon Antivirus Connector is an interactive interface and part of the macmon Compliance module.

# INTERFACES TO LEADING SECURITY SOLUTIONS

As a user of macmon NAC you do not only benefit from the high level of security the software establishes along with easy interaction and operation, as well as the deployment of intelligent technologies, but also from the interface's capability to connect with other leading security solutions.

Apart from the well-known Antivirus solutions, they also include Endpoint security, IT Emergency Management, Intrusion Detection or Prevention Systems (IDS/IPS), Asset Management Inventory, Security Incident & Event Management (SIEM) and many more.

## BlueCat Networks

The BlueCat IP Address Management (IPAM) solution offers unified mobile security, address management, automation and self-services. The interface of BlueCat enables the import of DHCP data, DHCP leases in particular. This information is being fed into macmon and complements the endpoint data collection, including DHCP hostnames and IP data. Among other things, this improves the detection of ARP spoofing attacks and hence the protection against them.

## Matrix42 – Empirum

Matrix42 offers with Empirum a central platform to universally control endpoint software and to manage endpoints in general. Combine that with macmon and you get 2 key advantages: in case of a compliance breach that is detected by Empirum, macmon can be informed through the compliance interface and isolates the dangerous system. In order to have synchronized status updates of the inventory on both ends, the list of the permitted systems on the network in macmon can be synchronized with the inventory list of Matrix42. As you prefer and as your environment permits, either one or the other platform can take the lead.

## McAfee

McAfee is one of the largest vendors of security solutions worldwide and offers with its ePolicy Orchestrator (ePO) a platform that lets you centrally manage various security solutions at once. When integrating with macmon Compliance, you can be alerted of nearly any event that may occur in McAfee. That way the endpoints that are deemed "non-compliant" will be moved to the appropriate network segment. Flexible policy enforcement allows you to react to each event individually.

**Contact**

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