Belden | macmon
A BELDEN BRAND

Comprehensive product integrations for solid security

Connect macmon Network Access Control (NAC) with technology partners' leading security solutions

belden.com

Connect to what's possible.

The macmon NAC solution, developed in-house, helps you protect your network against unauthorized access and is seamlessly integrated with other security solutions, including:

- Asset management
- Compliance
- Identity stores
- Infrastructure

Asset management systems and identity stores can be bi-directional integrations.
Some vendors offer more than one type of integration.
Discover below our long-term partnerships with leading technology brands.

Allied Telesis

Integrations with
infrastructure

About the company
Allied Telesis is a global provider of secure IP/ Ethernet switching solutions. The company is well-known for its reliable and high-performance networking equipment.

Product integration benefits
macmon NAC reads ARP information from Allied Telesis network switches. This enables macmon NAC to isolate or physically disconnect non-compliant endpoints.

baramundi

Integrations with
asset management, compliance

About the company
baramundi is a German software company specializing in Unified Endpoint Management (UEM) and IT management solutions.

Product integration benefits
enables macmon NAC to be connected to the baramundi Management Suite (bMS) Unified Endpoint solution. This integration allows you to address and control macmon NAC centrally from the bMS. With bMS as the leading system, you only need to maintain new devices or relocations in one place.

In addition, you can define rules that automatically move non-compliant devices from your NAC solution to a secure network.

Barracuda

Integrations with
compliance, identity stores

About the company
Barracuda CloudGen Firewalls include full next-generation security paired with all network optimization and management functionality (known as Secure SD-WAN).

Product integration benefits
expanded protection on the corporate network at any entry point against unauthorized access, malware and advanced persistent threats. In addition, the macmon NAC integration enables detection of bot-controlled endpoints immediately at the gateway. While macmon NAC gathers ARP information from all devices on the network and enforces policies at the MAC level, Barracuda CloudGen Firewalls (which feature advanced threat protection and botnet detection) sends macmon live updates on identified threats at the client. Subsequently, affected endpoints can be automatically disconnected from the network or moved to a quarantine segment.

In addition, 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 both segment- and endpoint group-based. Group member lists are continuously maintained through macmon's active endpoint discovery, which ensures your communication policies are up to date. Guest devices are separated from the rest of the network by the Barracuda CloudGen Firewall.

BlueCat

Integrations with
asset management

About the company
BlueCat Networks provides DDI (DNS, DHCP and IP address management) solutions.

Product integration benefits
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, including DHCP leases.

This information is fed into macmon NAC and complements endpoint data collection, including DHCP hostnames and IP data. This improves the detection of ARP spoofing attacks and protection against them.

Check Point

Integrations with
identity stores

About the company
Check Point is a multinational provider of software and combined hardware and software products for network security, endpoint security, cloud security, mobile security, data security and security management.

Product integration benefits
Check Point Identity Awareness allows you to apply firewall policies based on the properties of an identity. In addition to the classic use of a firewall at the gateway, this option, paired with macmon NAC, offers new possibilities for effective network segmentation. While previously rules were defined per segment and maintenance per device was too complex, the seamless integration of macmon NAC now maintains these granular rules automatically.

The integration of macmon NAC and Check Point is delivered conceptually ready to consider all daily workflows and endpoint lifecycles. Devices are logged on and off when entering and leaving the network. Changes due to relocation, long runtimes and changes of properties such as IP address, name or other details automatically lead to an update.

CONTECHNET

Integrations with
asset management

About the company
CONTECHNET's modular software solution INDART Professional® allows you to create and maintain complete IT emergency planning.

Product integration benefits
the integration of INDART Professional allows macmon NAC to continuously fetch relevant data from routers, switches and servers. The emergency reference list is always kept up to date. If a registered system becomes unreachable or a new system shows up, appropriate action is requested as defined in the emergency documentation.

DECOIT

Integrations with
compliance

About the company
CLEARER from DECOIT® GmbH quickly detects threats like malware in the corporate network.

Product integration benefits
once configured in CLEARER, detected threats or anomalies are recorded as incidents and transferred to macmon NAC. CLEARER and macmon NAC's integration enables threat detection and isolation of affected endpoints.

CLEARER collects information about your network's endpoints and derives a compliance decision, which is enforced in the corporate network with the help of macmon NAC. The macmon web GUI provides an overview of all endpoints' compliance status. CLEARER SIEM GUI provides additional details about the incident with recommendations for action.

CLEARER reliably detects anomalies because the solution regularly queries macmon's endpoints inventory and can therefore differentiate between the network's known and unknown endpoints.

Dell EMC

Integrations with
infrastructure

About the company
Dell EMC, a division of Dell Technologies, focuses on IT infrastructure solutions for enterprises, like servers, storage, networking and data protection technologies.

Product integration benefits
macmon NAC reads ARP information from Dell network switches and allows you to isolate or physically disconnect non-compliant endpoints.

EgoSecure

Integrations with
compliance

About the company
EgoSecure is a market-leading vendor of data security solutions and protects organizations from data loss, malware and unauthorized devices, e.g., USB drives.

Product integration benefits
the connection with EgoSecure allows endpoints' compliance status to be sent to macmon. This enables the non-compliant devices' disconnection from the network or their movement to a quarantine segment, and transfers them back after their cure. Additionally, EgoSecure informs macmon immediately about any compliance breach, including "unauthorized application executed" or "too much data copied to USB drive."

ExtraHop

Integrations with
compliance

About the company
ExtraHop is the global leader in real-time wire data analytics. The innovative approach of the ExtraHop Operational Intelligence platform provides the correlated, cross-tier visibility essential for application performance, availability and security in today's complex and dynamic IT environments.

Product integration benefits
ExtraHop detects unusual activities, such as many login attempts in a short period at a server or database. Its integration with macmon NAC allows endpoints' instantaneous isolation from the network.

FireEye

Integrations with
compliance

About the company
FireEye Network Security helps organizations 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 signatureless, 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.

Product integration benefits
using its advanced persistent threat detection engine, FireEye Network Security can detect a malicious threat in the corporate network within the blink of an eye. Pairing FireEye Network Security and macmon NAC provides a powerful combination of threat detection and network enforcement. macmon NAC enables FireEye Network Security to enforce an endpoint's compliance status based on its health state, as determined by FireEye Network Security.

F-Secure

Integrations with
compliance

About the company
F-secure is a leading provider of endpoint security, especially anti-malware solutions.

Product integration benefits
macmon reacts quickly and specifically to events from F-Secure, such as critical virus detections, using the AntiVirus Connector. In addition, macmon NAC cyclically determines the age of all known endpoints' virus signatures and uses the information to classify them as "compliant" or "non-compliant." In addition to the complete overview of compliance status, devices with outdated signatures can be automatically moved to quarantine.

Greenbone

Integrations with
compliance

About the company
the Greenbone Security Manager (GSM) of Greenbone Networks identifies security gaps in corporate IT and evaluates their risk potential. In addition, the GSM recommends measures to remedy the found vulnerabilities.

Product integration benefits
macmon NAC has GSM scan new endpoints for vulnerabilities when they are connected to the corporate network and regularly analyzes the compliance status to protect your corporate network.

Infoblox

Integrations with
asset management

About the company
Infoblox provides network services such as DNS or DHCP.

Product integration benefits
the solution works universally with the same data that macmon uses for Network Access Control. Using the available open interfaces, you're able 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 automations that guarantee an effective and up-to-date overview.

Ivanti

Integrations with
compliance

About the company
Ivanti acquired MobileIron on 1 December 2020 and is now managed in the portfolio under Ivanti Endpoint Manager Mobile (EPM mobile).

Product integration benefits
the integration of Ivanti allows you to read out all managed mobile devices to make them known in the macmon NAC solution and grant or deny them access to the network. The unique approach to mapping those devices enables you to link a Ivanti label to a group in macmon. You don't need to manually enforce policy to control access on your network. Each device's compliance status can also be transmitted, and macmon isolates any devices that Ivanit/MobileIron deems non-compliant.

LANCOM

Integrations with
infrastructure

About the company
LANCOM Systems GmbH is the leading German manufacturer of network solutions for business customers and the public sector. LANCOM offers professional users secure, reliable and future-proof infrastructure solutions for all local and multi-site networks (WAN, LAN, WLAN) and central network management based on software-defined networking technologies (SD-WAN, SD-LAN, SD-WLAN).

Product integration benefits
during intensive collaboration, macmon NAC automatically detects all LANCOM devices and uses verified communication methods to identify all components, including connected endpoints. NAC strategies can thus be implemented "out of the box" using both conventional network protocols, such as SNMP, and advanced techniques, such as RADIUS-based 802.1X.

ManageEngine

Integrations with
compliance

About the company
ManageEngine crafts comprehensive IT management software. ManageEngine's 90+ products and free tools cover a variety of IT needs
From network and device management to security and service desk software, the company brings IT together for an integrated, overarching approach to IT optimization.

Product integration benefits
macmon NAC analyzes Patch Manager Plus and Mobile Device Manager Plus assets. In both cases, macmon NAC provides an overview of the compliance status of every corporate device on the network. A predefined policy could isolate a non-compliant corporate device by moving it into a special network segment and notify the administrator in charge to look at it.

Matrix42

Integrations with
asset management

About the company
Matrix42 specializes in digital workspace management, providing a comprehensive suite of solutions. The company's offerings allow organizations to effectively optimize their IT infrastructure, endpoints, applications and services.

Product integration benefits
integrate macmon NAC into Matrix42 Asset Management and manage your endpoints from the Service Store. The lmbit macmon connector for the Matrix42 Service Store allows you to organize macmon endpoints' management. The macmon installation's endpoint information is automatically kept up to date via the REST API.

McAfee

Integrations with
compliance

About the company
McAfee is one of the largest vendors of security solutions worldwide. With its ePolicy Orchestrator (ePO), it offers a platform that lets you centrally manage various security solutions at once.

Product integration benefits:
integration with macmon NAC Compliance allows you to 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.

MICROSENS

Integrations with
infrastructure

About the company
as a pioneer of fiber optic transmission systems since 1993, the worldwide company MICROSENS GmbH & Co. KG covers all performance sectors of fiber optic technology. Starting with solutions for future-safe office networking and high-availability in rough environments, the product portfolio ranges from large-scale site networking and interconnection of computing centers to high-performance wide area networks (WANs).

Product integration benefits
macmon NAC reads ARP information from MICROSENS network switches. Based on that information, macmon NAC isolates or physically disconnects endpoints that are deemed non-compliant.

NCP

Integrations with
identity integration

About the company
NCP is the German leading vendor of remote access VPN solutions for high-security access of central-based data and resources. Companies with a high number of professional mobile users or Industry 4.0-driven businesses benefit from simplified administration via NCP's Secure Enterprise Solution for professional remote access networks.

Product integration benefits
macmon can provide an overview of the systems and users connected through the NCP VPN. If an endpoint is disconnected from the internal network because of a specific event (e.g., security breach, compliance offense, etc.), macmon can enforce the NCP Gateway to drop the VPN connection actively. A common whitelist of approved endpoints can also be used – this ensures that network access to trusted endpoints is given by covering WLAN, LAN and VPN.

Belden

Nexans

Integrations with
infrastructure

About the company
Nexans is a leader in the design and manufacturing of cable systems and services across four main business areas: PWR-Transmission, PWR-Grid, PWR-Connect and Industry & Solutions.

Product integration benefits
macmon NAC reads ARP information from Nexans' network switches. This information enables macmon NAC to isolate or physically disconnect endpoints that are deemed non-compliant.

Phoenix Contact

Integrations with
infrastructure

About the company
Phoenix Contact has 100 years' specialization in connection and automation technology, particularly for traffic infrastructure, electromobility, renewable energies, intelligent supply networks and energy-efficient mechanical and plant engineering. The broad product portfolio includes network switches in many forms, such as unmanaged, intelligent or managed switches that implement various protocols and standards such as PROFINET, Ethernet or 802.1X.

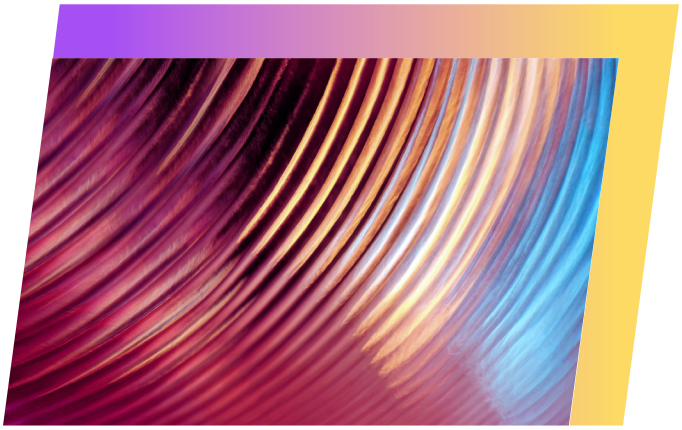
Product integration benefits
with the integration of network switches from Phoenix Contact, you can conveniently read and set VLANs on the interface in macmon NAC, block and unblock network interfaces or read the 802.1X status.

Progress Flowmon

Integrations with
compliance

About the company
Progress Flowmon's Anomaly Detection System (ADS) uses machine learning to detect anomalies hidden in network traffic. It complements traditional security tools and is a multi-layered protection system capable of detecting threats at any stage of compromise.

Product integration benefits
detectable attacks usually require immediate action, which is implemented in real time by macmon NAC. Through the direct coupling of the two systems and the associated automated reaction to attacks and anomalies, infected machines and devices can be isolated immediately, even before security experts identify a threat in detail. The detection of malware communication or botnet activities of infected devices, as well as the uncovering of hidden data, are just some examples in which a short response time is necessary to quickly protect the corporate network.



Restorepoint

Integrations with
infrastructure

About the company
Restorepoint allows you to back up and restore a variety of products. You can chronologically archive their configuration and make your backups available again later.

Product integration benefits
The deep integration of Restorepoint allows you to save your macmon appliance's configuration and installation data. This automated process can also be scheduled. In addition to macmon's backup feature, which manages your scheduled backups in the background, Restorepoint centralizes this approach and is useful and quick in unexpected crash scenarios.

smart2success

Integrations with
asset management

About the company
smart2success is a software manufacturer that specializes in visualizing companies' collaboration of people and technologies. It offers various solutions in risk management, resource management, product management, digital transformation and IT management, in addition to solutions for specific industries.

Product integration benefits
the interface between macmon NAC and smart2project enables IT administrators to collect data on network components, integrate it into project management and monitor the impact on internal services and resources.

Sophos

Integrations with
compliance

About the company
Sophos evolves to meet every new challenge, protecting more than 400,000 organizations of all sizes in more than 150 countries from today's most advanced cyber threats. Powered by SophosLabs, Sophos' cloud-native and AI-enhanced solutions can adapt and evolve to secure endpoints and networks against never-before-seen cybercriminal tactics and techniques.

Product integration benefits
Sophos Intercept X detects threats quickly and provides the threat status via Sophos Central. macmon NAC regularly retrieves the health status from all network endpoints and displays it in the macmon user interface. If an endpoint's health status is insufficient, macmon can isolate the device from the network segment at short notice. This prevents malware from spreading over the network and infecting other network resources.

splunk>partner+

Splunk

Integrations with
infrastructure

About the company
Splunk is the world's first Data-to-Everything platform. Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver.

Product integration benefits
Splunk processes compliance incidents and network session data reported by macmon NAC and visualizes them in concise dashboards in real time.

sycope

Sycope

Integrations with
compliance

About the company
Sycope is a network monitoring tool using real-time flow analysis enriched with business context to help businesses assess performance and protect IT infrastructure. It records, processes and analyzes all parameters contained in flows, enhanced by SNMP, geolocation and security feeds.

Product integration benefits:
Sycope provides a complex mechanism to analyze network traffic and detect violations of security rules. The administrator can integrate Sycope with macmon NAC to detect and actively manage these violations.

swivelsecure

Swivel Secure

About the company
Swivel Secure is an industry-leading authentication solutions provider. Founded in 2001, Swivel Secure protects thousands of organizations in over 54 countries. Swivel's AuthControl provides multi-factor authentication (MFA) and single sign-on (SSO) for intelligent protection of cloud and on-premises architectures.

Product integration benefits
combining macmon SDP and Swivel AuthControl highly protects access to cloud and on-premises solutions. Zero Trust Network Access ensures that only authorized users on compliance-verified systems are allowed to access cloud and on-premises resources, while Swivel AuthControl protects logins to macmon SDP through MFA and simplifies them through SSO. This improves and optimizes security and usability for secure access to corporate resources.

Vectra

Integrations with
asset management

About the company
Vectra is a global leader in AI for real-time detection and defense against cyberattacks in cloud, data center and enterprise infrastructures. This involves helping security analysts perform conclusive incident investigations and AI-powered threat hunting. In today's challenging data environments, comprehensive cyberattack detection and response is essential. Vectra is uniquely positioned to help you proactively find cyber attackers and reduce business risk.

Product integration benefits
in addition to viruses and malware, administrators also have to address suspicious endpoint behavior. If an endpoint becomes infected with malware despite the precautions taken, that endpoint must be isolated from the network segment quickly. This prevents malware from spreading and infecting other network resources. Vectra Cognito quickly detects such threats with the use of AI. Vectra Cognito records the system status of every endpoint in the corporate network and makes these available to macmon NAC. The combination of Vectra Cognito and macmon NAC provides a powerful combination of threat detection and isolation of affected endpoints.

tenfold

Integrations with
asset management

About the company
tenfold offers a web-based portal that centrally manages users and their permissions.

Product integration benefits
tenfold's portal manages permissions to register employee and guest devices—or to deny their access—to the network. Combined with macmon's guest service, these permissions are instantly available. When an Active Directory account becomes inactive, the corresponding endpoint is locked out of the network.

Technology Partners of macmon SDP

WithSecure

Integrations with
compliance

About the company
WithSecure protects critical operations worldwide. These include the largest financial institutions, IT service providers and MSSPs, among others. Using AI-driven security, WithSecure provides endpoint and cloud collaboration protection. To minimize the damage of a cyberattack, the intelligent detection and response function is additionally supported by experts and technology providers.

Product integration benefits
to ensure that an infected endpoint does not infect the entire corporate network, WithSecure and macmon NAC work in close and powerful collaboration. The sophisticated engine of WithSecure Business Suite Premium offers several components to provide effective security locally on the endpoints. macmon NAC can automatically respond to threats according to company policy (such as a direct disconnection from the network or a move to a quarantine network).

Yubico

About the company
Yubico has developed the YubiKey, a highly secure way to protect your online accounts on all your devices. With it, you can effectively protect yourself from cyberattacks. With FIDO 2, a security key pair consists of a public and a private key, ensuring strong authentication. Users can add security keys, such as YubiKey, to log in even more securely.

Product integration benefits
thanks to FIDO 2-based authentication, users can access cloud and corporate resources faster and more securely. Authentication can be easily enabled and disabled by both users and administrators. This provides additional protection and higher security when logging in to macmon SDP resources.

About Belden

Belden Inc. delivers complete connection solutions that unlock untold possibilities for our customers, their customers and the world. We advance ideas and technologies that enable a safer, smarter and more prosperous future. Throughout our 120+ year history we have evolved as a company, but our purpose remains – making connections. By connecting people, information and ideas, we make it possible. We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia and Africa.

For more information, visit us at:
belden.com

follow us on

Belden