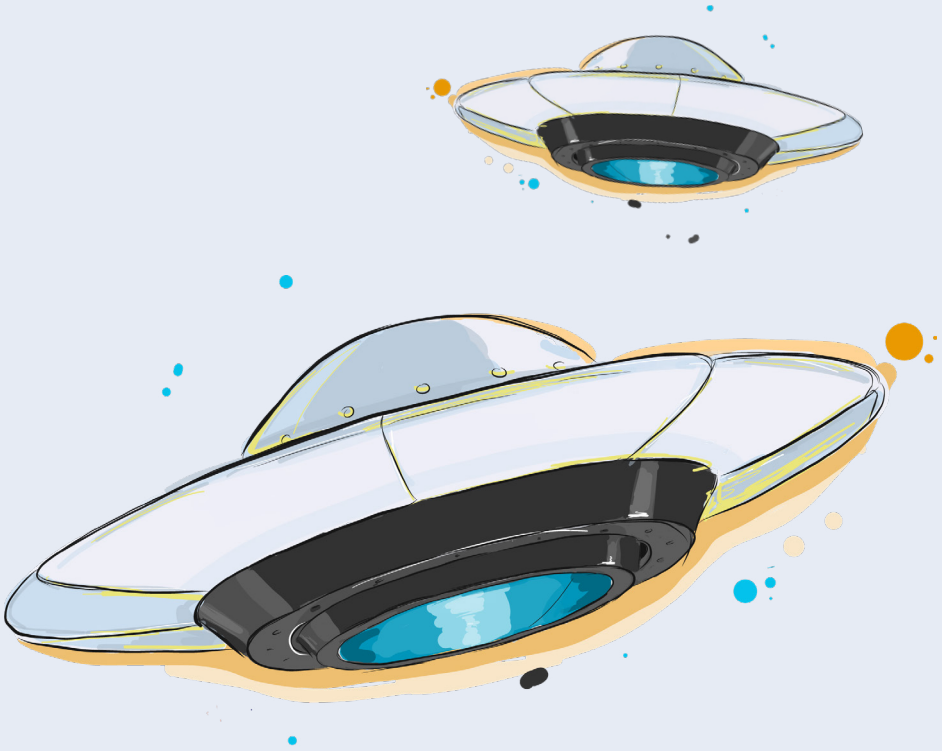
macmon
smartly simple



nac

DETECT UFOS WITH MACMON NETWORK ACCESS CONTROL

UFOS = unknown frightening objects

MACMON NAC LIFECYCLE

The macmon NAC LifeCycle is divided into three phases, which at the same time form the basis of successful NAC projects:

1 Get a complete network overview and detect UFOs

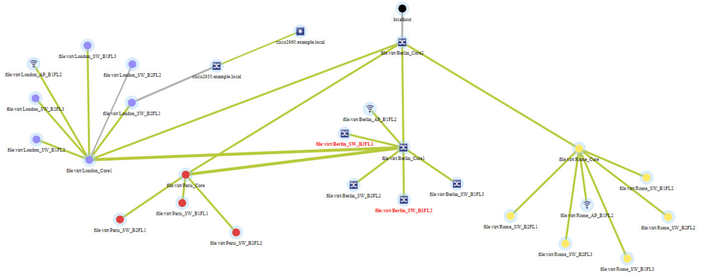
2 Access control based on endpoint identities

3 Access control based on the security status of terminal endpoints

OVERVIEW

The decisive factor is that the existing infrastructure is used and a complete network overview is already available on the intuitive web GUI of macmon NAC within a few hours. The focus is on low implementation and operating costs. The resulting overview allows an initial assessment of the network state with regard to the number and type of UFOs (unknown frigthening objects). At the same time, the status of the network for the implementation of NAC can be seen and a decision can be made which steps still need to be considered.

- Recording of the entire infrastructure and all endpoints as live inventory management
- manufacturer-agnostic to cover every network, even mixed component environments with older and newer models
- Display of events on the network, e.g. attacks such as ARP spoofing or MAC spoofing
- Highly flexible third-party integrations using the open REST API for Asset Management, CMDB and other solutions
- Visualized network topology offering extensive features for in-depth analysis
- Comprehensive reporting on collected network data
- Detection of UFOs and known endpoints on the network

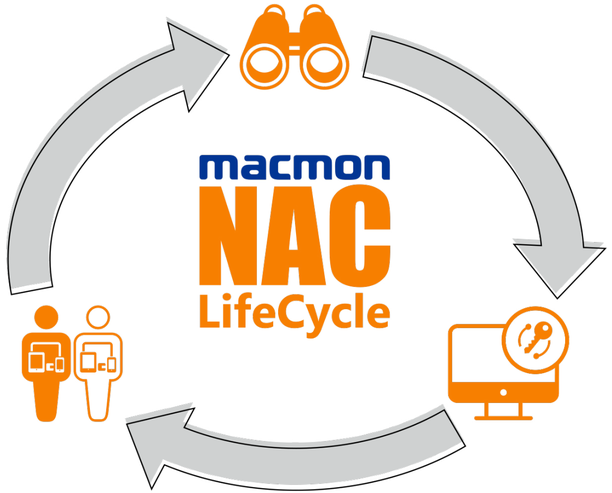


NETWORK ACCESS CONTROL

Whether you want to use the reactive approach via SNMP, the proactive approach via 802.1X or a mixed operation for access control, the uniform and automatic macmon NAC rules engine makes no difference administratively.

Network segmentation increases security on the network and also maps BSI-compliant security concepts. The combination of macmon NAC with existing Identity Stores - CMDBs, Asset Management, AD/LDAP or Mobile Device Management (MDM) - leads to a central and complete view that is always up-to-date.

- Technology independent: Mixed operation with and without 802.1X/RADIUSS
- Adjustable: mapping and implementation of any VLAN concepts
- Compatible: integration with any Identity Store for seamless system maintenance
- Efficient: guest portal with sponsor and BYOD functionality to reduce the workload
- Flexible: establishing security zones and earmarked access
- Powerful: dynamic and automatic rules and policies
- Automatic: Isolation of UFOs



COMPLIANCE

macmon NAC is the central power on the network. In addition, the endpoints are also checked for their safety and their security level. To achieve this, macmon NAC offers various verification processes. The most powerful one is the integration of third-party platforms. Usually a solution is already in use that checks for security violations and provides this crucial information. Endpoints that do not pass the check are automatically isolated. After the endpoint was cured, it returns to the original point of network access.

- Proactive response to sources of safety-related info
- Automated isolation of compromised systems on the network
- Comprehensive mapping of compliance policies, supported by vendor independent security integrations, and optionally the macmon agent
- Connect to antivirus solutions from industry leading vendors to automatically respond to critical events
- Trouble-free third-party integrations

Last compliance Issues

Source	Reason	MAC	Status	Change	Group
macmon-agent	Firewall aktiviert	00-00-71-00-00-77	compliant	25. Mar 10:36	Network
Finally_Save	Malicious_behaviour	00-1A-A0-B3-9E-2E	noncompliant	08. Feb 16:10	PC
AVC-F-Secure	Infected_with_Malware	00-60-B0-E6-9E-07	noncompliant	08. Feb 16:10	PC
Barracuda	Downloaded_Malware	00-0F-3F-00-00-59	noncompliant	08. Feb 16:10	Notebooks
Barracuda	Joint_a_Botnet	00-0C-29-B6-86-3E	noncompliant	08. Feb 16:10	Default
WSUS-Script	Long_time_not_updated	00-A0-BB-00-00-90	noncompliant	08. Feb 16:10	Notebooks
WSUS-Script	Updated_successfully	00-60-B0-D5-5B-00	compliant	08. Feb 16:10	PC
Barracuda	Connecting_to_malicious_sites	00-14-5A-00-00-80	noncompliant	08. Feb 16:10	Printer
EgoSecure	Unallowed_camera_detected	08-2E-5F-08-82-76	noncompliant	08. Feb 16:10	PC
Barracuda-URL-Filter	Weapon_sites_visited	00-19-99-7B-7B-30	noncompliant	08. Feb 16:10	Production

WITH MACMON NAC YOUR NETWORK REMAINS UFO FREE

5x SMARTLY SIMPLE

1. GROUP-BASED CONFIGURATION

Corporate endpoints are being sorted into logical groups. These groups manage the configuration of endpoints on the network. That includes advanced access authorization. This way macmon NAC is able to dynamically create a set of rules and adapt it when changes occur. This works both with SNMP-based and RADIUS-based implementations.

2. 802.1X (WITH AND WITHOUT CERTIFICATES)

In macmon NAC, the group-based configuration can be used to define different security levels for different levels of authentication. As a result, network access is granted based on the level of the authentication, e.g. certificate-based as the highest level or Active Directory credentials as a medium level. Regardless of whether 802.1X is implemented with or without certificates, the costs and complexity are being significantly reduced.

3. GUEST PORTAL

Designed for a high level of flexibility and an extremely wide range of applications, the guest portal differentiates between guests and guest endpoints. The integrated sponsor functionality allows you to delegate the creation and management of vouchers to any employee. macmon NAC provides you by default with an always up-to-date overview of the endpoints that are brought into the organization.

4. EFFECTIVE VLAN CALCULATION

On the basis of group-based configuration, you have several options to define specifications for the access authorization. macmon NAC goes through the authorization process and determines the correct VLAN in each situation. Details such as location, switches, compliance status, etc. are included in this process.

5. AD INTEGRATION WITH MAPPING

macmon NAC offers the option to authenticate endpoints using Identity Stores (AD, LDAP, MDM, etc.). Either user accounts or endpoint accounts can be used. This makes the authentication significantly easier when introducing 802.1X because certificates do not need to be rolled out. Endpoint groups or Organizational Units (OUs) in the Active Directory can easily be linked to the macmon endpoint groups. The automated rules engine also applies here.

INTERFACES AND PARTNERSHIPS

FOR YOUR SAFETY

Connect macmon Network Access Control (NAC) to leading security solutions and benefit seamless from our integrations!

Our in-house developed NAC solution is not only the answer to ideally protect your network against unauthorized access, you can also integrate macmon NAC with other security products. The types of integrations are classified into asset management, compliance, Identity Stores and infrastructure, while the exchange of information can take place bi-directionally.

ASSET MANAGEMENT

The bidirectional interface to asset management solutions such as CMDBs, inventory databases, client management platforms and other systems, allows the automatic synchronization of the net- work and endpoint information.

IDENTITY STORES

Existing Identity Stores on the network, such as Mobile Device Management solutions, AD/LDAP services, SAML, RADIUS servers or other systems, can be used by macmon NAC to authenticate the endpoints.

COMPLIANCE

When checking endpoints on the network, the existing security solution may detect an anomaly that does not meet the security standards, because it is infected by malware or is part of a botnet.

INFRASTRUCTURE

macmon NAC reveals endpoints on the network extremely quickly by reading the data from endpoints in the network infrastructure or by receiving it from other platforms.

THE ADD-ONS FOR MACMON NAC:

PAST VIEWER: PERFORMING FORENSIC ANALYSES

The macmon Past Viewer offers a way to collect and process already collected data in a structured way in order to obtain a historical view of the endpoints on the network. For each endpoint and switch port, so called "endpoint sessions" are generated that show the complete course of a connection. Details regarding the IP addresses used, names and authorizations as well as the corresponding Layer 2 and Layer 3 network components used are included from start to finish of a session.

The obligation to provide evidence in accordance with ISO, PCI or DSGVO in the form of security-relevant events on the network is also available, just as the possibility of carrying out a risk analysis for network areas. Knowing the number and type of endpoints that were active in the past, e.g. in a certain building, offers the opportunity to weigh the effects of changes to the network infrastructure or the implications of network-related failures.

SWITCH VIEWER: QUICKVIEW OF CURRENT DEVICE DETAILS

The macmon Switch Viewer reads out details from existing network components such as serial numbers, port configurations regarding speed, operating mode, VLANs, interface details and location as well as other inventory data from existing network components and provides them via the macmon REST API to synchronize them with existing CMDBs or asset management systems.

In addition to the list view of the switch interfaces, macmon Switch Viewer also offers a graphical view of the actual switch layout. Using filters, port configurations such as VLANs etc. can be displayed, while various actions such as switching the VLAN are enabled right on the GUI. If administrators want to log on directly to the switch for more in-depth tasks, the macmon RADIUS server can be used to securely log in using the RADIUS authentication protocol. Unauthorized access attempts can thus be efficiently prevented while the individual authentications are logged.

SCALABILITY: HIGH-AVAILABILITY MACMON NAC SCENARIOS

When using a network access control solution, the availability requirements will differ depending on how the solution is used and the technologies employed. macmon meets these requirements by enabling you to implement a distributed server structure that can be used in different architectures or design variants.

How it is used depends largely on your requirements and objectives. macmon NAC offers a number of options for ensuring the necessary availability, including the "Hidden Master" principle, simple failover and compensation for WAN connection failures. For each macmon server, you can choose whether to use a physical or a virtual appliance.

nac
Network Access Control

Headquarters:
macmon secure GmbH
Alte Jakobstr. 79-80 | 10179 Berlin Germany
Phone: +49 30 2325 777-0
nac@macmon.eu | www.macmon.eu