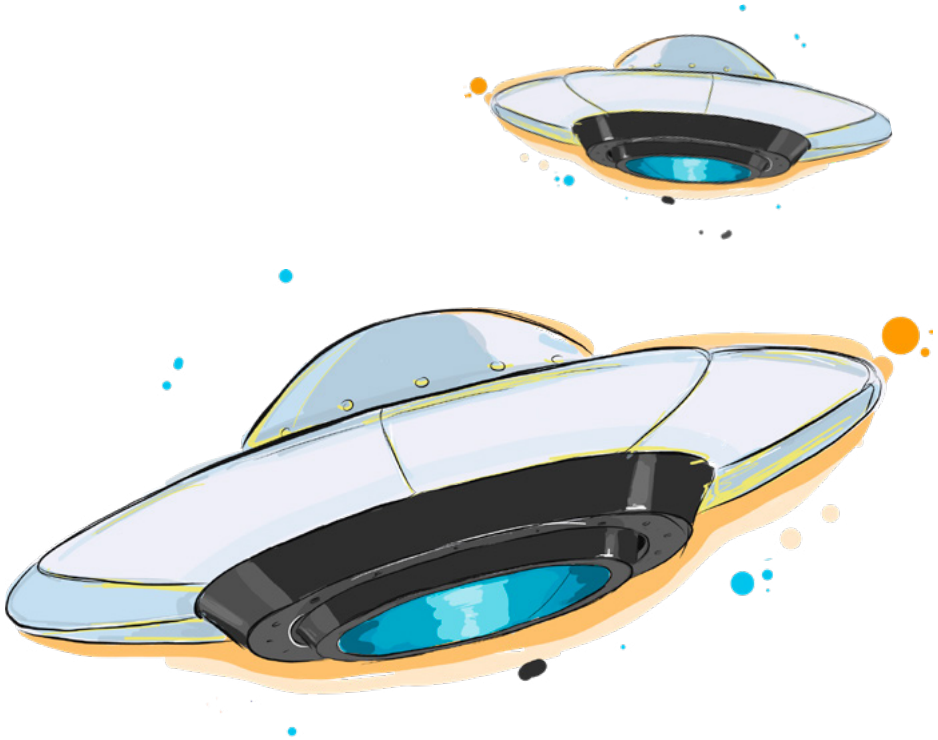
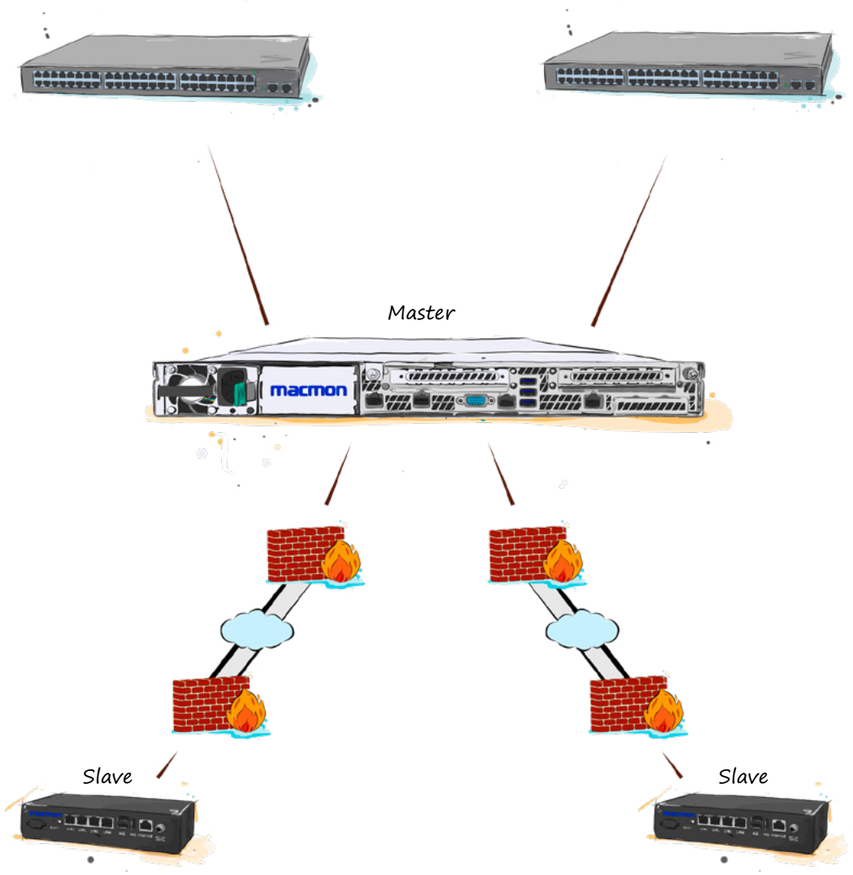
macmon
smartly simple



MACMON NAC-STORY

How we prevent UFOs on your network

CONTENTS



macmon NAC offers a scalable architecture as based on master/slave method to cover any network size and structure.

THE BEGINNING

Overview using convenient and automatic visualization

Network Access Control is usually introduced for three reasons:

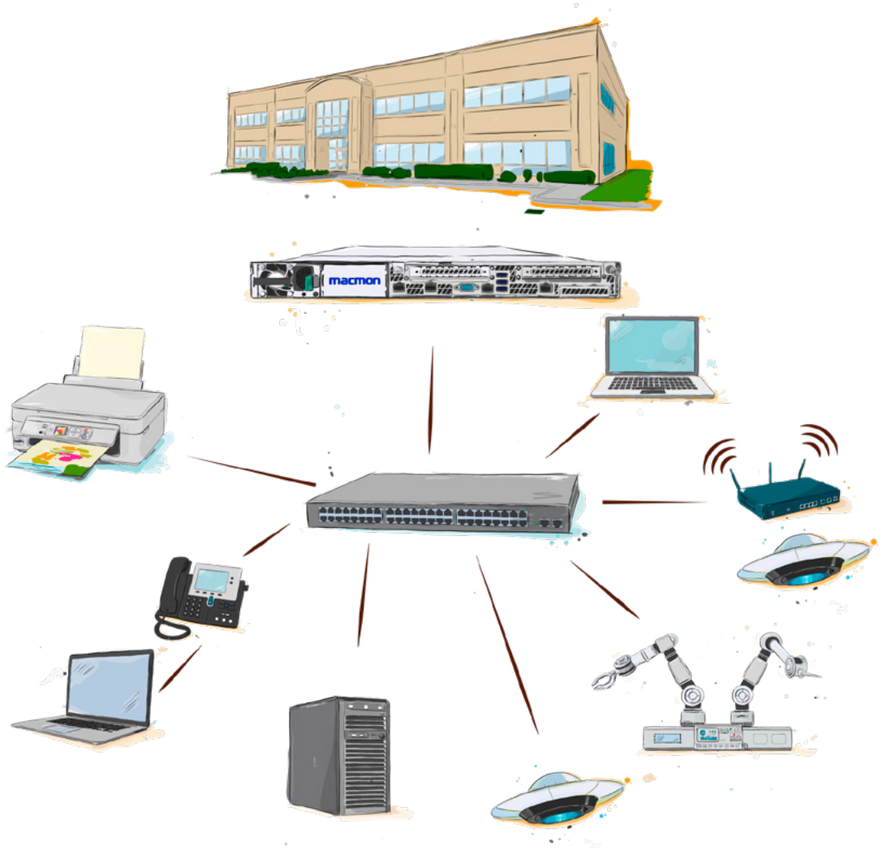
- To gain a **complete overview of the network**,
- to **control access based on the identities** of endpoints and
- to **control access based on the security status** of endpoints.

With macmon NAC, you can achieve these objectives quickly and easily. Furthermore, macmon additionally offers interesting options for your network security.

The decisive factor is that the existing infrastructure will be used and a **complete overview of the network is automatically available** in just a few hours on macmon NAC's intuitive web GUI. The focus is therefore on a rapid implementation accompanied by low operating costs.

For this, macmon NAC communicates via SNMP, SSH, HTTPS DHCP, DNS and other protocols and interfaces (i.e. REST API) with the switches, routers and other network components, in order to **automatically record and identify the topology of the network** with all connected devices, vendor-independent. The white list principle has proven successful for this identification process for over 15 years. For any remaining unknown endpoints, macmon NAC can provide support using various technologies, such as WMI, SNMP or footprinting.

The provided offers an initial evaluation of the status regarding the number and type of unknown endpoints in the network. At the same time, the status of the network for introducing NAC and which steps still have to be taken into consideration for implementing NAC is determined. With your decision for macmon NAC, the course is set for introducing successfully Network Access Control without having to make any changes to the existing network.

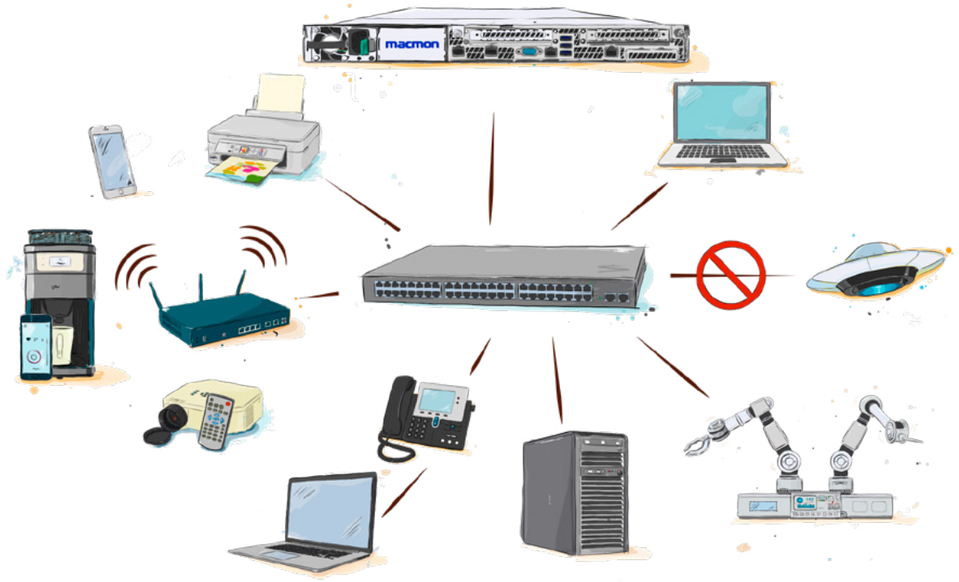


Quickly you get a complete overview of all endpoints in the network and you can find unknown frightening objects (UFOs).

COMPLETE OVERVIEW OF THE NETWORK

Achieve overview, convenience and security on your network

- **Record the entire infrastructure** and all endpoints as live inventory management
- Cover every network **regardless of the manufacturer**, even when using a mixed bag of components of different generations
- **Implementation without** the need for **restructuring** beforehand
- **Graphical overview** of the network topology with extensive analysis options
- **Comprehensive reporting** of data gathered on the network
- **Individual dashboard** for each user with a central overview of relevant details
- **Highly versatile programmable interface** for third party solutions via the open **REST API** for asset management, CMDB solutions and many more
- Display network events:
  - Change of endpoint location within the corporation
  - Activity of known endpoints at unusual times
  - Attacks such as ARP spoofing or MAC spoofing
  - Detection of endpoints on the network
  - Overview of the usage of ports (free and used)



macmon NAC helps you to control your network access and isolates unknown or unauthorized devices.

CONTROLLING THE ACCESS

Protect all of the endpoints used on your network

As soon as the user has identified which endpoints are on the network by using macmon NAC, the effective control of the network access will be simplified. The endpoints that have already been learned are **categorized by groups**. These groups can be used to define what kind of access the endpoints should get when they are positively authenticated.

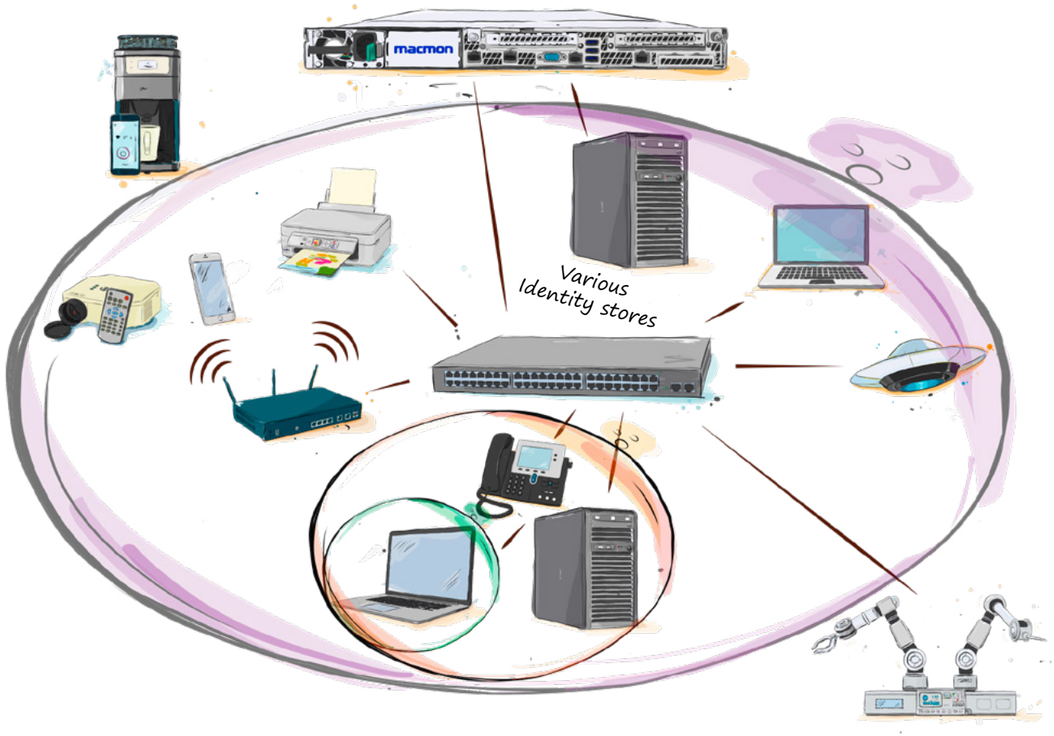
You could use the reactive approach to control the switchports via SNMP, or use the proactive approach via 802.1X with the integrated macmon RADIUS Server. You could even use a mixed operation with no difference in administration, thanks to the automatic set of rules of the policy engine in macmon NAC.

One GUI – one policy engine.

Depending on the kind of identification – starting from the MAC address, username and password and AD accounts, all the way to certificates – security zones can be introduced in parallel.

This **simple group-based configuration** uses policy engine´s **automatic set of rules** integrated into macmon NAC. This ensures that the administrator only has to look after exceptional cases managing the network access – macmon NAC takes care of everything else.

The VLAN management of macmon NAC also offers absolutely crucial simplification and relief when it comes to day-to-day operations. In addition to the general access control, it offers the option to grant individual and fitting exactly access. The options are extensive and allow “appropriated access“, which grants specific access only where the situation requires it. So for example, printers are always assigned to the printer network, while mobile employees in all areas are always assigned to their appropriate network segment.



Security zones and network segmentation harden the network.

ACCESS MANAGEMENT

The right access – automatically and appropriate

As a result of a network segmentation, security is increased on the network and, "incidentally", BSI-compliant (BSI = German Federal Office for Information Security) security concepts are mapped. Relocation of endpoints is possible without manual intervention, which increases flexibility and greatly reduces the workload of the IT department.

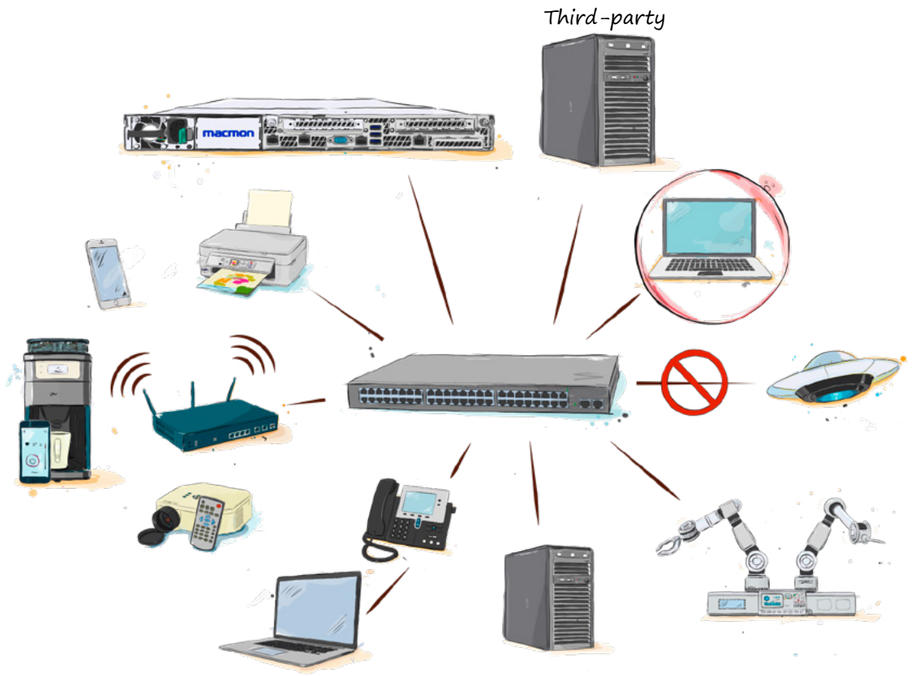
Savings of more than one man-day per month have been reported from experience. Combining macmon NAC with existing Identity stores – CMDBs, Asset Management, AD/LDAP, even Mobile Device Management (MDM) or Unified Endpoint Management (UEM) – leads to a central and complete view which is always up-to-date. New endpoints are also automatically given the required access in accordance with the existing workflows and the maintenance effort is kept to a minimum.

Naturally, in addition to checking network access, the provided **guest portal grants guest endpoints temporary and restricted access**. At the same time, the portal can be used by sponsors to issue guest identities (vouchers) and by employees to register their own endpoints.

When guests and third-party endpoints are managed this way, the IT department's workload will be further reduced significantly, as the staff often do not have to be involved in the process of granting access to the endpoints.

Access control – advantages of macmon NAC:

- *Technology-independent:* Operate it with or without 802.1X/RADIUS or in mixed mode.
- *Powerful:* Get quick results with our dynamic and automatic policy engine's set of rules.
- *Variable:* Design and implement any VLAN concepts.
- *Compatible:* Bind any identity store and maintain systems automatically.
- *Efficient:* Reduce administrative efforts with the guest, sponsor and BYOD portal.
- *Flexible:* Establish security zones and benefit from appropriate access.



Unsafe or infected endpoints are isolated and separated from the network.

SECURITY LEVEL

Endpoints that do not meet the requirements are automatically isolated

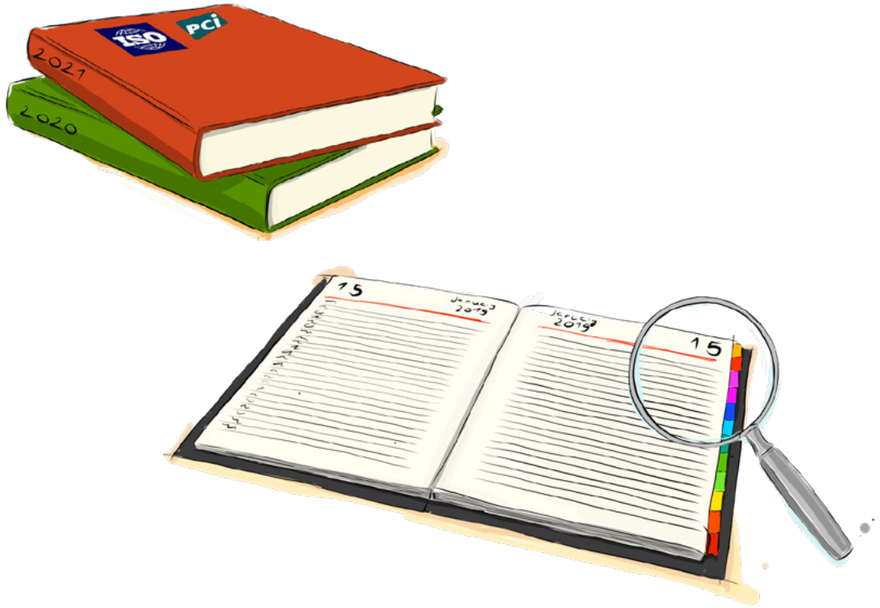
After establishing the overview of the network with all active network components and the detailed display of the endpoints, macmon NAC is the **central power in the network**. Furthermore, the endpoints' security settings and/or their security level can be checked. macmon NAC offers various options for checking this. An agent can be used to carry out the checks directly on the endpoint. In addition, the antivirus management server for example is checked for events in order to automatically isolate infected endpoints from the network.

A further option to make your network more secure is offered with the integration of third-party solutions. Usually, a solution is already available which checks the security level and therefore holds important information. Using the open REST API or the special Compliance API that comes with macmon NAC, ensures that these sources of information can be easily bind to supply status updates.

This way, the power of macmon NAC is put to good use and endpoints that do not comply with the policies are automatically isolated. After a successful recovery, regular access will be restored.

The security level – advantages of using macmon NAC:

- **Proactive reaction to infection sources**
- **Automatic isolation of unsafe endpoints** on the network
- **Simple implementation** without having to make changes to the infrastructure
- **Easy integration** of third-party solutions
- **Scale effects** by using of all existing systems and investments



The macmon Past Viewer simplifies verification and documentation liabilities or forensic analyses.

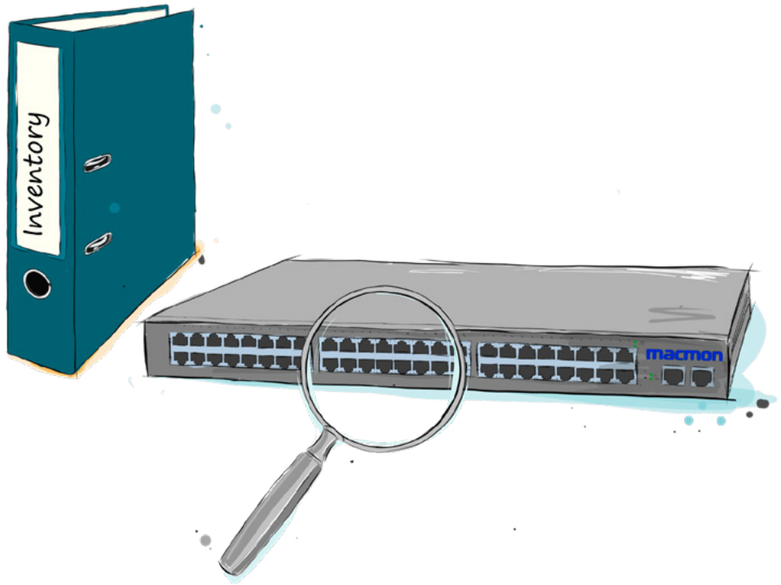
HISTORICAL FACTS

Perform forensic and impact analyses

macmon Past Viewer offers additional option to **collect and process** "old" **data that is usually purged whilst operating** Network Access Control, to not only get a live view, but also a historical view. For each endpoint, you can display when and where the device was active on the network, which IP addresses and names or VLANs were used.

Each switch interface or WLAN access point can be retraced allowing you to see which endpoints were active where and when. IP address, name of endpoints and type of access can all be determined. Having this information means that forensic analysis is possible in order to satisfy the usually cumbersome **ISO or PCI compliancy checks**. The data can then be passed to the data protection officer if required.

In addition to this, if suspicious activities or special incidents occur, the corresponding network connections can be checked afterwards. As the data is being collected continuously with macmon NAC Past Viewer, access to the **information over the entire lifespan** is now possible. At the same time the data can be used to plan redesign or other actions on the network.



More details and overview of network devices and secured RADIUS-based login.

A LOOK INTO THE DETAILS

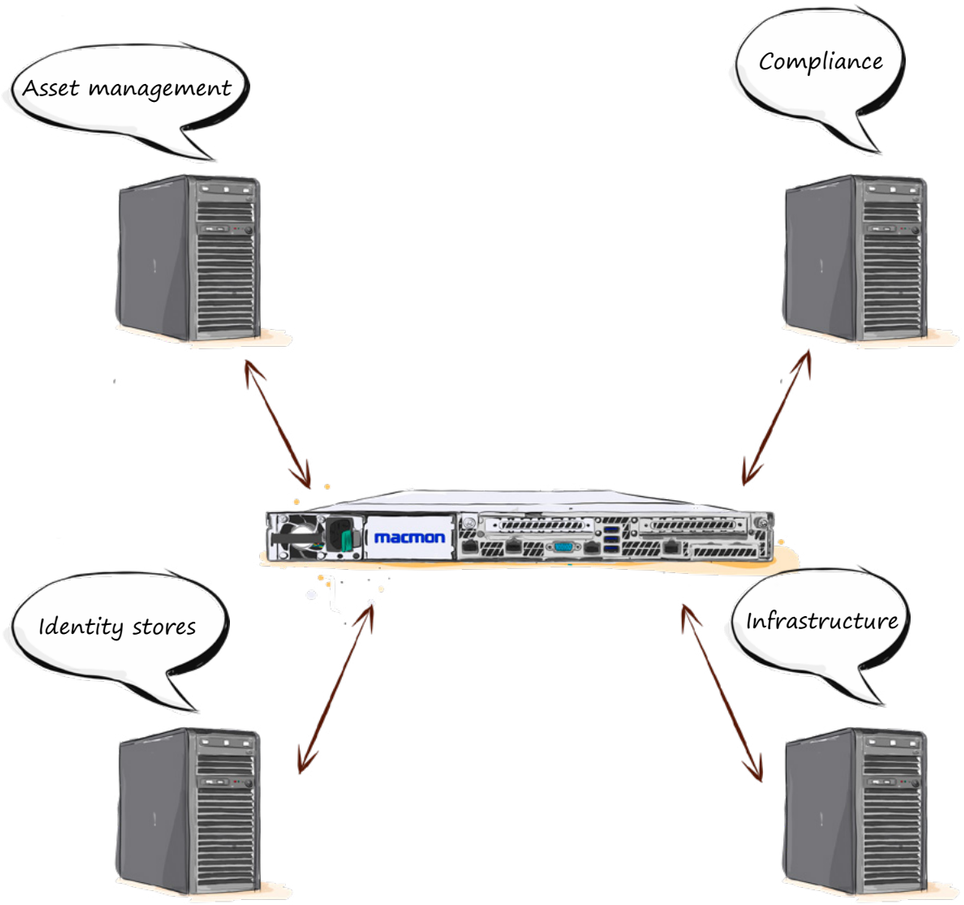
More details and security

Another addition to network access control is given by the usage of collected data down to the last detail. With **macmon Switch Viewer, various additional information details about the network devices is recorded** and available. This includes serial numbers and other port-related configuration details.

In addition to network device details, Switch Viewer also offers the option to use macmon as RADIUS Server for authentication on the network device. This further increases security and eliminates the need of a separate RADIUS Server.

A graphical view of the interfaces displaying their actual arrangement on the network device offers a **quick way to check the port status**.

If necessary, it is possible to **determine the correct physical port** and to switch it.



macmon NAC provides seamless integration for other security products delivering automatization and save valuable time.

MACMON TECHNOLOGY PARTNER

Combine macmon NAC with other leading security solutions

macmon NAC can also be **seamlessly integrated with other security products** with a bidirectional exchange of information. In the following four categories this provides great flexibility, security benefits and even more reduced administration efforts.

Compliance
When checking endpoints on the network, the existing security solution may detect an anomaly that does not meet the security standards, because it's infected by malware, or is part of a botnet. macmon NAC uses thise information to isolate the endpoint with better discernments.

Infrastructure
macmon NAC reveals endpoints on the network extremely quickly by reading the data from network devices in the infrastructure or by receiving it from other platforms. Thanks to our active dialogue with the manufacturers of these infrastructure devices, we can guarantee that this data is reliably and correctly processed and displayed in macmon NAC for a better visibility of your network.

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 network and endpoint information. Depending on the approach, either the third-party solution or macmon NAC can be the primary system. macmon's live inventory manager usually learns about newly introduced systems first and then shares this information to keep all solutions up to date.

Identity stores
Existing identity stores on the network, such as Mobile Device Management or Unified Endpoint Management solutions, AD/LDAP services, SAML, RADIUS Servers or other systems, can be used by macmon NAC to verify endpoint authentications. On the other hand, individually verified identities along with the current status, can be posted to third-party solutions, such as firewalls and other systems.

MACMON SECURE GMBH

German “Best-of-Breed” NAC manufacturer

macmon secure GmbH has been developing network security software since 2003. Its headquarters are located in the heart of Berlin. macmon Network Access Control (NAC) solution is developed entirely in Germany, but is used across the globe to protect networks against unauthorised access.

More than 1,200 customers from various industries trust macmon secure GmbH, ranging from medium-sized enterprises to large international corporations.

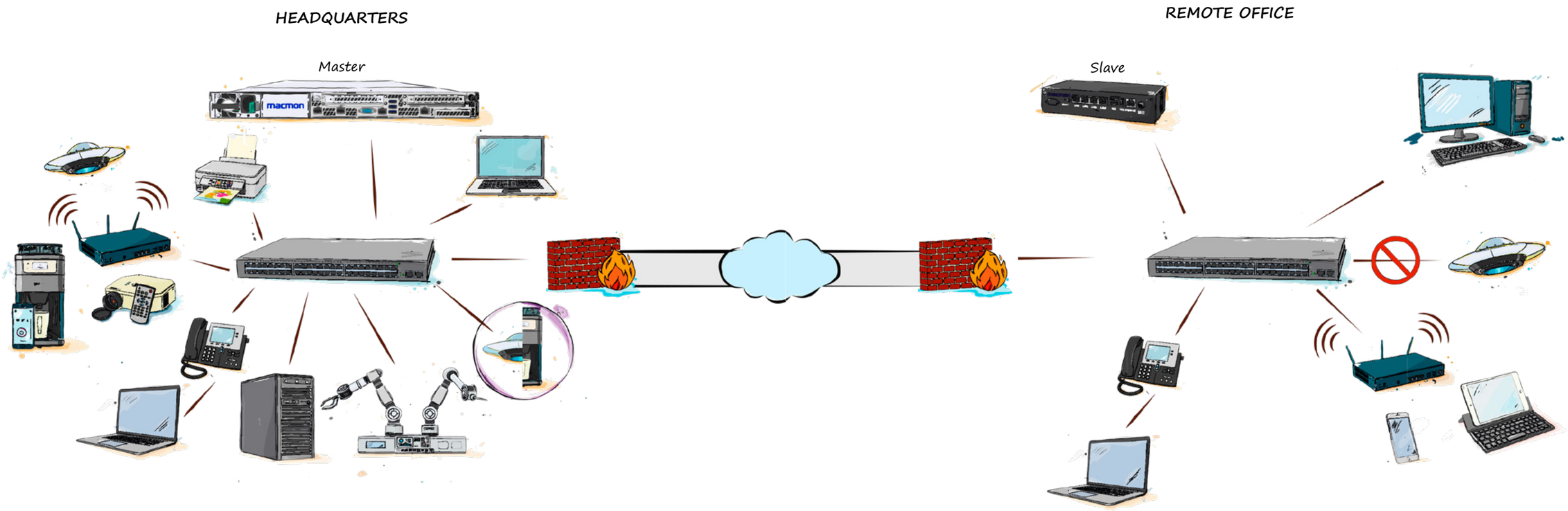
The objective is to offer each and every company a flexible, efficient NAC solution that can be implemented with very little effort but offers significant added value in terms of the company’s network security.

macmon NAC – smartly simple!

Our team, which now consists of over 70 employees, brings together qualified engineers and economists, software engineers, Bachelors and Masters of Science in Applied Computer Science, IT graduates and specialists. They all work together to contribute to the advanced market-oriented development of our macmon NAC software, to the successful implementation of NAC projects for our customer, and as a result, to our success as a company.

LET'S FIND UFOS

Start by discovering your network with us



UFO = unknown frigthening object

Network Access Control

- Immediate network visibility including graphical reports and a topological view
- Dynamic network access control with or without 802.1X for heterogeneous infrastructures
- Powerful enforcement of corporate compliance policies with simple third-party integrations

macmon secure GmbH
Alte Jakobstraße 79-80
10179 Berlin
+49 30 23 25 777-0 | nac@macmon.eu

www.macmon.eu