



Precision in Sheet Metal Processing and Reliable IT Security

“Made in Germany” quality, two times over

In the last few years, ARKU Maschinenbau GmbH in Baden-Baden, Germany has faced an increasing number of malware attacks. Working closely with the Freiburg branch of the IT systems house NetPlans, it has introduced extensive measures to defend itself. In its search for reliable and scalable network protection, it quickly became clear macmon NAC was the right option: NetPlans is a Platinum macmon partner with certified and continuously trained macom experts who have provided first-class support for their customers – from the SME sector especially – with the implementation of a huge number of projects.

“We are an innovative, internationally active family-owned company with more than 200 employees worldwide. With more than 50 years of experience, we are the world’s market leader in leveling technology and experts in sheet metal processing machines. That makes us an appealing target for cyber-criminals. Deploying a comprehensive IT security strategy – with the Network Access Control solution from macmon — has given us the capabilities to fight off continuous attacks.”



Felix Pflüger | IT & Digitization Team Leader | ARKU Maschinenbau GmbH

RADIUS authentication provides even more security

To authenticate endpoints, ARKU uses macmon’s integrated RADIUS server to make the decisions on granting access. As the ID or means of authentication, a number of different properties can generally be used, such as the MAC address, user name/password or certificate. Since the network is not accessed by the system until the RADIUS server has confirmed it, there are no unused or insecure ports, which increases security significantly. While granting access, the IT team can define and specify additional rules for the switch to implement. If the switch is technically capable of doing so (layer 3), a specific VLAN, defined ACLs or almost any other attributes can be assigned in this way.

macmon NAC at ARKU:

- Comprehensive oversight over all devices on the network
- Continuous live inventory management
- Immediate alert in the event of unknown devices
- Initiation of automatic countermeasures
- The number of **macmon-Nodes aktuell: 1,063**



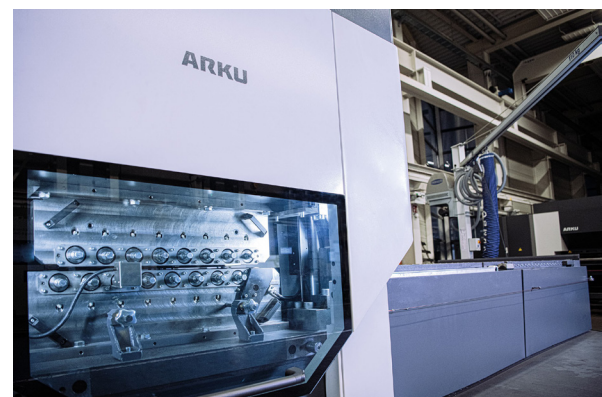
ARKU Maschinenbau GmbH runs its worldwide operations from its base in Baden-Baden, Germany. German SMEs in particular have.

An access control list (ACL) limits access to data and functions. The ACL determines the extent to which individual users and system processes have access to certain objects such as services, files or registry entries. Felix Pflüger: "We use a variety of security solutions in our company. Thanks to macmon NAC, we always have oversight over our extensive IT infrastructure. Our switches are administered via SNMP and RADIUS, meaning macmon sets the appropriate VLAN on the switch port, or the port is blocked if there are unknown devices. That prevents unauthorized devices from gaining access via network outlets, for example."

Visitor management made easy

Frequent visits by customers and suppliers present companies with the challenge of preventing these users' end devices from accessing the company's internal network. The functions of the "Guest Service" module provide an intelligent and flexible management system for any external device with a granular guest ticket system for controlling temporary LAN and WLAN access.

Since the number of external visitors was manageable during the Coronavirus period, the IT department was responsible for deciding whether or not visitors were granted access. In the future, however, this task will be delegated to authorized employees with the macmon guest portal. Without having to deal with the macmon NAC administration, they can generate access data directly in the portal or confirm visitors who have registered themselves. The resources shared and the duration of access can be defined while creating the access data, ensuring each visitor can access only the specific resources approved for them. For instance, a service technician who has to maintain machine equipment has different access rights than a customer who is visiting the company for a meeting.



With the macmon-Guestportal Access to resources is precisely controlled.



Hardware used in the network area:

- **Firewall:** Sophos XG
- **Switches:** Aruba
- **WLAN:** Aruba Controller, Aruba APs
- **Endpoint:** Sophos Intercept X

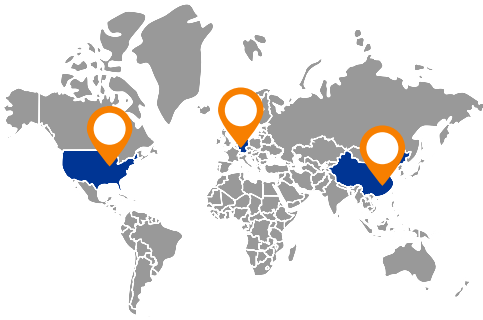
Barramundi
as client management solution

Barracuda
Mail Security Essentials

Its independence from manufacturers and large number of technology partnerships enables important synergies for optimizing network security and resource management.

World market leader in leveling technology with more than 50 years of experience

Founded in 1928, the family-owned company ARKU Maschinenbau GmbH has become the world market leader in leveling technology with over 50 years of experience to call on. ARKU offers the largest selection of high-performance and high-precision leveling machines as well as deburring and rounding machines. Its range is rounded off with solutions for handling parts for leveling and deburring machines.



With headquarters in Baden-Baden (Germany) and ISO-certified subsidiaries in Kunshan (China) and Cincinnati (U.S.), the company has market coverage in more than 30 countries.



Once macmon NAC had proven itself at HQ, a successful roll-out was achieved in the U.S.



Deployment of macmon NAC as a standalone solution in the U.S.

Companies that operate on an international stage have varying requirements with regard to availability. macmon NAC meets these needs by being able to operate with a distributed server structure and using this structure in different architectures or design variants.

macmon NAC ensures availability through options such as the "hidden master" principle, simple failover and compensation for WAN connection failures. Each macmon server can be established using either a virtual or physical appliance. A standalone solution was chosen for deployment in the U.S., while scalability was required as a solution with redundancy for the German locations. In the fall of 2022, macmon NAC was set up on a local server in Cincinnati by NetPlans staff, with a workshop held to provide colleagues with training. It gives IT experts the ability to analyze the local network of the U.S. office easily and quickly. Here too, full oversight over the network was available on the intuitive web GUI within just a few hours. The overview that was provided allowed for an initial assessment of the condition of the network with regard to the number and type of unknown endpoints that constituted a potential security risk. At the same time, the extensive analysis options made it possible to determine the current status of the network in the U.S. for the introduction of NAC and to decide what steps were still required.

CONCLUSIO by Felix Pflüger | IT & Digitization Team Leader at ARKU:

Using macmon NAC and the macmon guest portal has allowed us to significantly improve our network security and end point management.

In our region, the macmon Platinum partner NetPlans is our expert implementation and support partner for issues related to IT infrastructure and security, which have been improved over the years and maintained at the highest standard. Only by continuously optimizing existing solutions can intelligent attacks be successfully repelled in the long term. The rollout of macmon NAC in the U.S. was a success; further projects are in the pipeline.



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