BELDEN

CASE STUDY

NAC in Automotive — The Extra Level of OT Network Security and Control

Belden's field-proven, manufacturer-agnostic NAC solution secures the operational networks of one of the world's biggest car manufacturers

Executive Summary

Companies worldwide are the focus of cyber criminals who want to gain access to production networks, a disruption that companies need to protect themselves against to remain competitive.
In a globally operating company with distributed production sites, international security standards and hybrid infrastructures, Belden provides a field-proven, manufacturer-agnostic solution with macmon NAC (Network Access Control).

Customer Characteristics

The customer is a globally operating company in the automotive industry. Belden´s macmon NAC is deployed in one of the most modern production facilities in the world.

macmon nac

Customer Challenges

The customer uses PROFINET, a widely used Ethernet-based communication protocol in the automation industry.

It offers high bandwidth and real-time capability, making it attractive for many applications. However, the use of PROFINET can complicate security, as it provides a larger attack surface than conventional fieldbuses.

Solution Definition

Belden's macmon NAC is specifically designed to protect the PROFINET network from cyber-attacks by providing the following functions:

- Restrict access to network resources to authorized or trusted devices
- Integration with existing security solutions
- Isolation or quarantine of problematic or compromised devices, without disrupting production

Implementation / Project Pathway

The customer's specific requirements, identified in a Proof of Concept (POC), were implemented by Belden's cybersecurity experts in a remarkably short time.

Additional investments in hardware and consulting were not required. Special functionalities were even integrated into the product in just a few days.

The challenge was to create a simple way to completely disconnect a production area or "production bubble" for unknown endpoints. This means that all endpoints inside the bubble can continue to produce unless there is an immediate attack on a certain endpoint.

The challenge was to create a simple way to completely disconnect a production area or "production bubble" for unknown endpoints.

This ensures that potential threats cannot spread to other parts of a plant by creating an artificial air gap. In addition, other parts of the system are not affected in this use case until the problem has been resolved. macmon NAC does not rely on the mandatory use of RADIUS/802.1x in certain parts of the system, but there are other strategies for detecting unwanted behavior in parts of the system that cannot use RADIUS/802.1x.

Impact Highlights

Belden's macmon NAC uses multiple technologies to collect information about an endpoint's operating system, domain name and network ports. This improves network visibility and helps the administrator better classify, identify and localize endpoints.

Belden's macmon NAC also compares the collected information with existing data to prevent ARP (Address Resolution Protocol) spoofing and attacks. It detects and stops man-in-the-middle attacks and alerts and isolates devices with duplicate IP addresses.

With the Advanced Security feature, Belden's macmon NAC can inspect every device that enters the network. It can communicate with devices using their IP address. It can also verify that the endpoint is the same or similar to the one that was previously authorized. If not, it can remove the device from the network or move it to a quarantine network.

There, it can review the device's threat level and activity in a secure environment. Alternatively, it can simply notify or log the event.

Another way to verify the device is through SSH, a fingerprinting protocol. The SSH fingerprint can uniquely identify each client.

TLS (Transport Layer Security) is used for additional certificate checks, and other protocols are also available for verification.

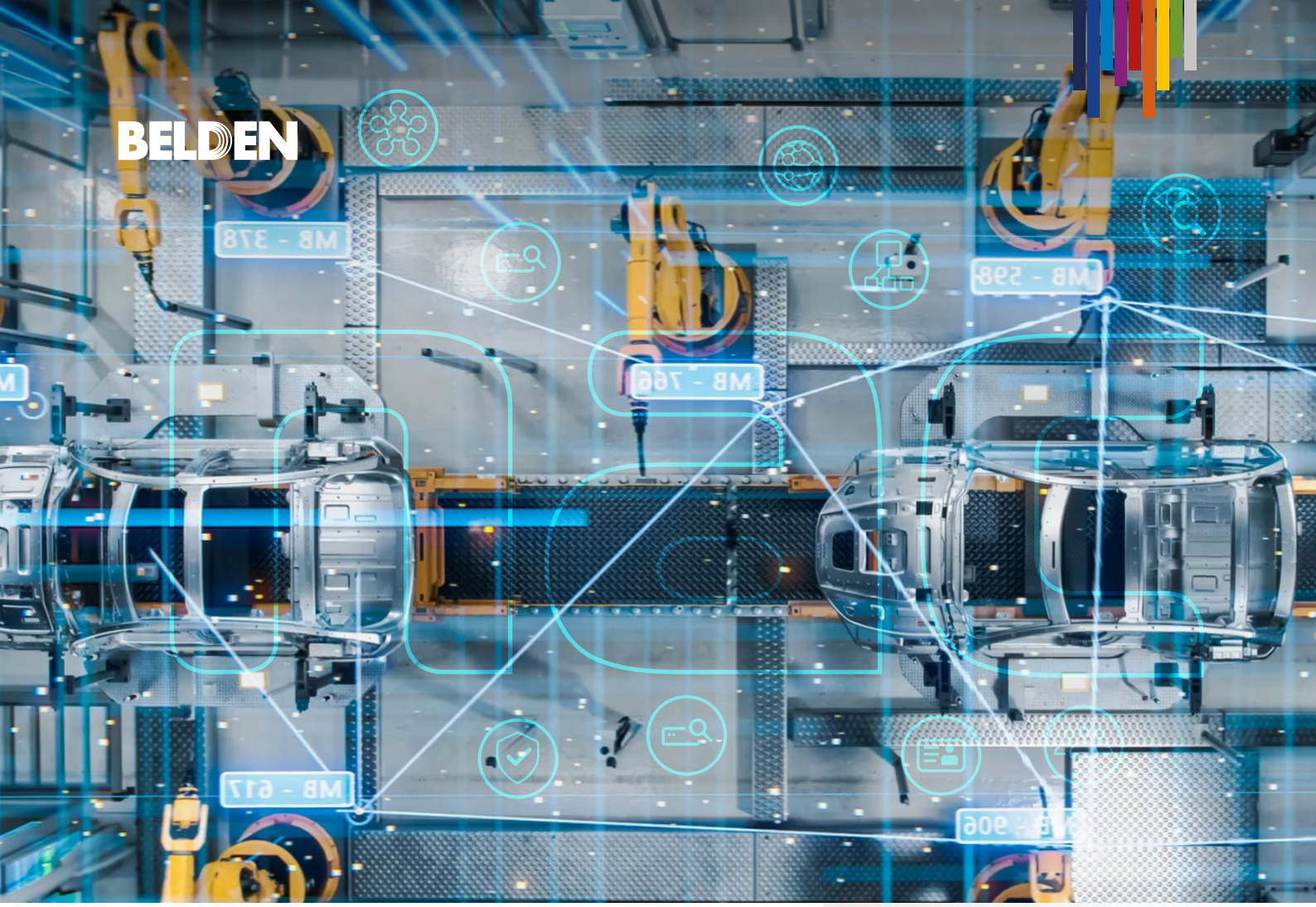
Belden's macmon NAC can periodically check if the devices are still up to date by setting a time value in the web interface, for example, 60 minutes.

By using Belden's macmon NAC Advanced Security, the automotive company has achieved that extra level of OT network security and control for its manufacturing operations – without any negative impact on the production environment's availability.

Advanced Security Features

Belden's macmon NAC Advanced Security provides customers with the following features:

- Identification of operating systems of devices connected to the network
- Location name of the device (physical location)
- Identification of open and closed ports (TCP & UDP)
- Successful login check
- System name
- Active Directory domain name
- Certificate authorities
- Fingerprints
- Prevention of security incidents such as ARP spoofing, MAC IP mismatch, MAC address flooding and MAC spoofing



About Belden

Belden Inc. delivers the infrastructure that makes the digital journey simpler, smarter and secure. We're moving beyond connectivity, from what we make to what we make possible through a performance-driven portfolio, forward-thinking expertise and purpose-built solutions.
With a legacy of quality and reliability spanning 120-plus years, we have a strong foundation to continue building the future.
We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia, and Africa.
For more information, visit us at www.belden.com;
follow us on Facebook, LinkedIn and X/Twitter.

Learn More

For more information
on our solutions for
network security, visit us at:
www.belden.com/networksecurity