Belden

Eliminating network blind spots improves production uptime and OT security

Belden's macmon Network Access Control solution gives an industrial plant complete OT network visibility.

Case Study

Customer

This large industrial plant, located in the Middle East, relies on more than 1,000 IP nodes for automation and control. Its network infrastructure is made up of PLCs, HMIs, distributed I/Os, energy management systems (ENMS), robots, wireless access points, SCADA servers and clients.

For 15 years, the plant's operational technology (OT) network has supported a diverse array of production equipment and systems, including legacy and modern machines.

To ensure business continuity and optimize manufacturing processes, the plant is prioritizing digital transformation. Because the plant is transitioning to connected systems to ensure efficiency and smart decision-making, protecting OT infrastructure is critical to reinforce uptime and safety.

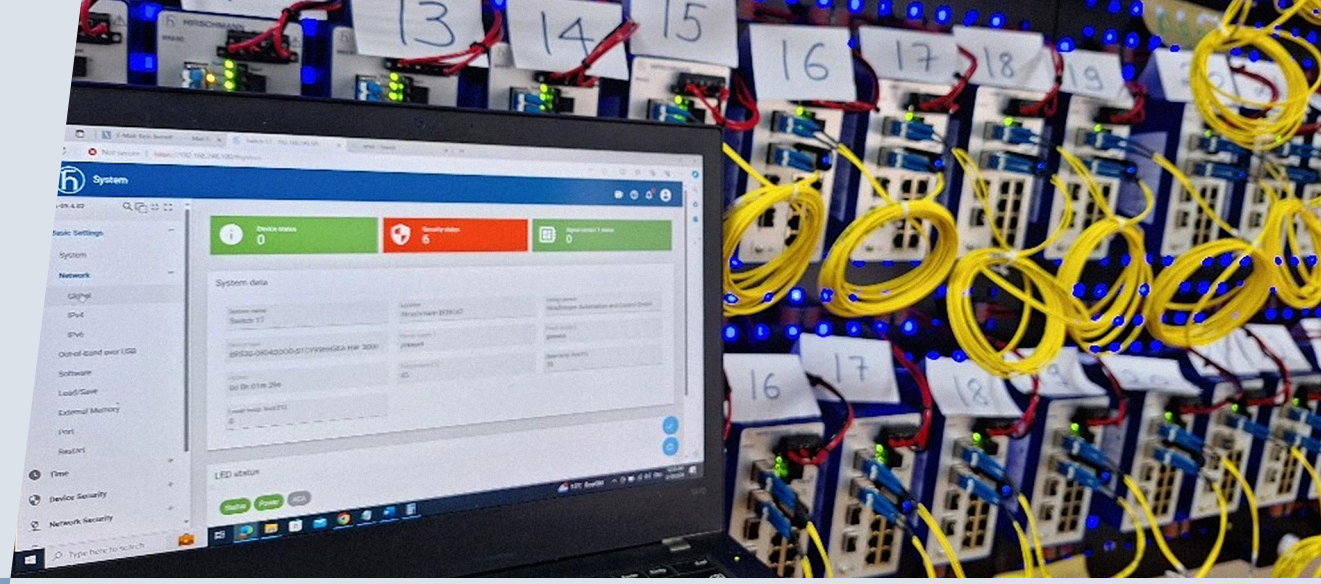
Challenges

To minimize cybersecurity risks, every device in an OT network must be identified and authorized. But this plant struggled to secure its production equipment and systems.

Because maintaining an up-to-date view of all connected devices in a brownfield network can be difficult, this gap makes it easier for unknown and unauthorized devices to gain network access.

"Especially in heterogeneous infrastructures, the use of Belden's macmon NAC proves to be extremely advantageous: It is vendor-agnostic and offers a unified security solution for different network components."

Jochen Füllgraf, NAC Product Manager, Belden



For example, this industrial plant couldn't identify anomalies like unknown cables connected to various devices and nodes across network segments: VLANs, IP subnets and even devices without IP addresses. This lack of visibility exposed the plant to serious security risks and created entry points for operational disruptions.

To address this, the plant wanted to improve network visibility and security and implement advanced monitoring and access control solutions that could detect unauthorized connections, manage devices and eliminate blind spots.

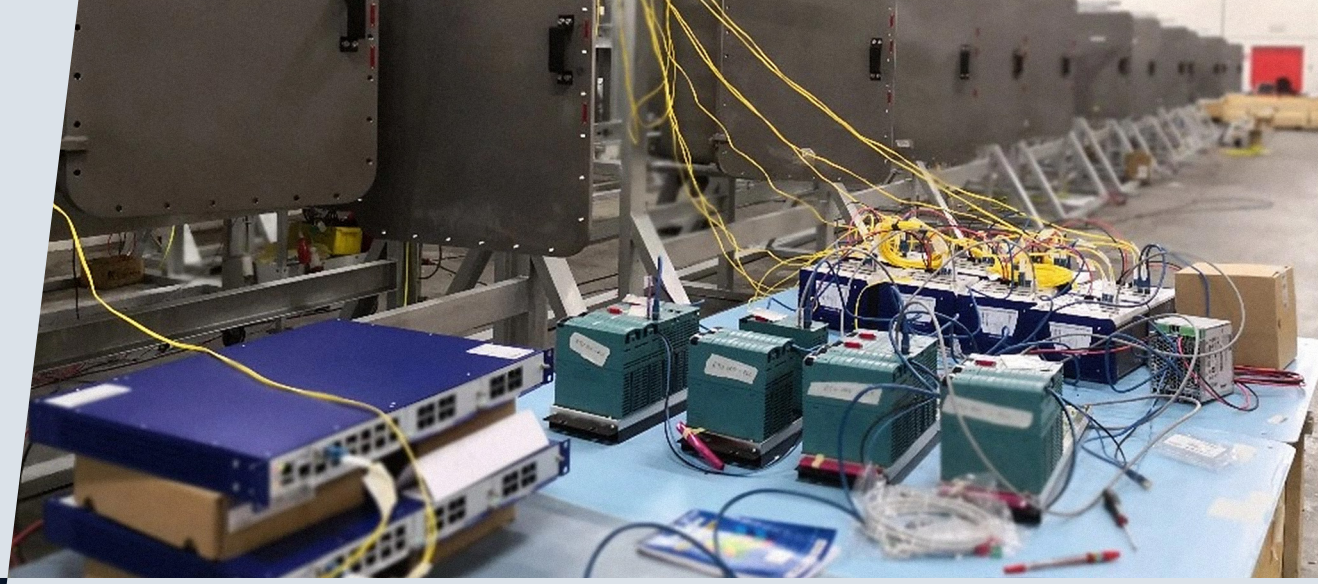
Discovery

As its need for network access control (NAC) grew, the manufacturer turned to ZMS Digital Industry Solutions LLC for guidance. With expertise in operational technology, ZMS could help identify a solution that was:

- Designed to operate in an OT environment
- Easy to deploy
- Capable of providing state-of-the-art security
- Aligned with the requirements of OT technicians without burdening them with complexity.

After evaluating several solutions, ZMS chose Belden's macmon NAC to serve the plant for many reasons:

- **It's simple to use.** An intuitive user interface lets OT engineers administer the network without extensive IT knowledge.
- **It supports legacy systems.** It enables the management of legacy switches without 802.1X authentication.
- **It's vendor agnostic.** Because it works with equipment from any vendor, all SNMP-manageable switches can be controlled.
- **It can be tailored to a network-specific configuration.** As operations change, the solution can be adjusted to align with OT network requirements.



"Previously, administrators had to manually inspect the network to identify nodes with missing or unknown IP addresses. With macmon NAC, this process is now automated—MAC addresses are retrieved directly from the switches, enabling remote monitoring. This not only strengthens security but also drastically cuts administrative overhead."

Shariq Khan, CEO, ZMS Digital Industry Solutions LLC

Solutions

macmon NAC ensures that new and legacy devices and systems can co-exist without compromising security. It provides real-time visibility, secure authentication and role-based access control so only authorized devices can connect to the OT network.

With the ability to instantly map and monitor network activity, OT teams now have a clear view of all connected devices at any time. They can detect unauthorized access attempts, identify possible security issues and segment networks into zones to isolate possible threats.

To ensure a seamless NAC deployment, ZMS set up a state-of-the-art test environment that replicated the plant's production network, including:

- A high-level infrastructure, including Cisco distribution centers and firewalls
- Numerous network topologies and VLAN configurations
- Sensors, PLCs, SCADA systems and HMIs

By testing in an OT lab vs. the actual production network, potential weaknesses and errors could be identified and resolved before the solution went live. Belden was able to simulate real production scenarios to fine-tune macmon NAC parameters according to the plant's requirements.

The test lab also provided an environment for training and education. Plant employees learned how to use the systems effectively and respond to potential problems without disrupting operations.

Results

As Shariq Khan, CEO, at ZMS Digital Industry Solutions LLC explains, unplugging a network cable can create significant security challenges and impact production performance. Before the macmon NAC solution was in place, the plant's OT team struggled to determine which cable was unplugged, preventing fast response to downtime.

"In the past," Khan explains, "administrators had to physically inspect the network to identify the issue. With macmon NAC, this process is now handled remotely, enhancing security and significantly reducing administration costs."

The OT team no longer has to worry about network blind spots that cause security problems. It has complete visibility and can identify and monitor every connected device—including those without an IP address or spread across different VLANs—for proactive management. Unwanted behavior and critical network events are detected immediately, and unauthorized devices can no longer connect to the OT network or impact production. Temporary access can be granted to specific network areas for defined tasks.

As operations expand, the NAC solution can scale to support the integration of new technologies while still ensuring strong security control.

With this level of protection, the plant can trust that its systems will remain secure and operational, ensuring uninterrupted business continuity.

ZMS OT Labs
Industry 4.0 & beyond..

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