

The Global Deployment of Network Access Control



CASE STUDY

macmon NAC as a Central Element of Belden's Comprehensive Industrial Cybersecurity Framework

Executive Summary

Industry Transformation Requires Flexible Industrial Cybersecurity Solution

The convergence of Information Technology (IT) and Operational Technology (OT) as well as the related transformation of network processes opens the door to malware and targeted cyber-attacks. Cybercrime has increased dramatically in recent years, causing billions of dollars in losses to companies and economies worldwide. In 2023, ransomware attacks increased by 50 percent. Manufacturing was one of the top target verticals in industrial environments. Therefore, industrial businesses need more powerful cybersecurity programs to deal with today's sophisticated threats. A modern OT network infrastructure and pre-integrated cybersecurity management solutions are essential to address this scenario. The Network Access Control solution macmon NAC is a central component to maintain Belden's network security.

Project Characteristics

Extensive Review by Belden Experts

For more than 120 years, Belden has been a leader in the design and manufacture of insulated wire, cable, and related products. Since then, Belden has transformed itself from a cable company to a signal transmission solutions provider with a complete portfolio of cable, connectivity, and networking products. Since Belden's acquisition of macmon secure in 2022, the company planned the implementation of macmon NAC in its global facilities.

Executive Summary	1
Project Characteristics	1
CIC & PoC	2
NAC Deployment	2
Challenges	2
Solution/Implementation	3
Project Roadmap	3
Impact Highlights	4
Final Statement	5





Customer Innovation Center

To plan the deployment of macmon NAC, Belden used its Customer Innovation Center (CIC) – a centerpiece of the global enterprise.



Belden's Customer Innovation Centers™ (CIC) help businesses to accelerate the design and implementation of robust, reliable and secure industrial networks that deliver the data and insight needed to fuel better business performance. The CIC provides a secure laboratory environment to develop, test, document and implement solutions without jeopardizing ongoing operations. macmon NAC passed the **Proof of Concept**, showing that the solution is deployable in a large-scale facility, in December 2023, and the Belden IT team started the implementation in the Belden facilities. In 2024, the company plans to deploy macmon NAC in 47 Belden facilities all around the globe, interacting with more than 20,000 endpoints.

“Before macmon NAC, there was no oversight, insight, or automated control for network-connected devices in the facilities. But with macmon NAC, we have all of this.”

Charles Crawford
Director of IT | Belden Inc

NAC Deployment at Belden's Richmond plant

To show the process of macmon NAC's implementation with a concrete example, let's have a closer look at Belden's Richmond facility. The plant consists of a distribution center and a manufacturing facility. The distribution center is responsible for warehousing and shipping Belden products to customers in the U.S. and worldwide.

In the manufacturing facility various cable types such as coaxial, fiber optic, and industrial cables are produced. There are a total of around 800 endpoints and 25 network devices in the plant. The implementation in this OT environment provided important insights into the benefits of the OT security features of macmon NAC and poses a blueprint for the further deployment of the solution in other Belden sites. We will also focus on the combination of macmon NAC and the industrial network technology of Hirschmann.

Challenges

Top Priority: Avoiding Production Downtime

The 95-year-old Richmond plant faced several challenges, including costly downtime due to unplanned maintenance, an aging workforce, a lack of machine connectivity and visibility, and a significant number of older and obsolete machines in operation. To address these issues, plant managers worked with data engineering consultants from Belden's CIC. The collaboration between the Belden CIC and the Richmond plant is designed to reduce downtime, increase efficiency, and prepare the plant for the next step in its Industry 4.0 journey.

While manufacturers have historically had IT and OT silos, the two networks are increasingly merging. To fully control today's demanding, heterogeneous networks, a network security solution must also support any authentication technology. With a **scalable, manufacturer-agnostic solution**, the existing infrastructure can simply be used as it is. This reduces the failure rate in the administration of growing IT and OT networks and significantly improves the industrial cybersecurity posture.



THE ROADMAP

1

DISCOVER

2

PROTECT

3

MONITOR

“Our roadmap was broken into three steps: discover, protect, and monitor.”

Discover was installing macmon NAC in read only, just capturing data for a few months. Protect was when we enabled NAC as well as 802.1X. And finally, monitor was ensuring devices were successfully authenticating and joining the network.”

Ryan Buckner
IT Infrastructure | Belden Inc

“Maintaining other NAC tools demands high administrative effort. With macmon NAC, this issue doesn’t occur. One daily check – that’s about it.”

Ryan Buckner
IT Infrastructure | Belden Inc

Solution/Implementation **Full Network Visibility & Control**

At the Richmond facility, macmon NAC allows Belden to have 100% visibility into the OT network infrastructure without having to monitor every change.

macmon NAC handles the movement of devices around the facility – automatically. This saves a lot of administrative resources. For example, an operator is instructed to move a device from zone A to zone B. This requires a change in VLAN assignment on the new interface where the device is plugged in. In the old environment, this would have required administrators to log into the switches onsite and then configure the new interfaces for a device. With macmon NAC, this can be done in seconds with just a few clicks in the central management platform. This is a great benefit in terms of the workload reduction of the network administrators.

The integration of macmon NAC and 802.1X authentication has introduced a new era of automation to the Richmond plant. This powerful combination allows tasks to be performed seamlessly, eliminating the need for manual intervention by administrators.

When an unknown device was connected to the Richmond network, it used to be redirected to a guest network. This unique setup was acting as a holding area for these devices, allowing the necessary analysis to be conducted. It’s important to note, however, that these devices are denied access to any critical resources within the Belden infrastructure.

“macmon NAC allows us to organize this process in a secure way.”

Charles Crawford
Director of IT | Belden Inc

To fulfill a Zero Trust approach nowadays, this guest access is also denied since it’s still a form of network access. Unknown devices are moved into a Layer 2 blackhole so they can’t jeopardize the network in any way.

“Other NAC products are way more complex and complicated to implement. It can take years until they are up and running. In comparison, macmon NAC is a light lift. It’s simple and effective.”

Joel Naumoff

Vice President of Cybersecurity | Belden Inc.

The deployment of macmon NAC at the Richmond factory has been very successful, and Belden is looking forward to further advancements. Belden uses Hirschmann’s industrial switches and firewalls in its OT networks. These products are engineered to perform in the harshest and most demanding environments. A combined solution with macmon NAC offers everything to build a reliable industrial network or improve the existing network architecture for increased industrial cybersecurity.

Belden uses a mix of vendors at its sites. With the implementation of macmon NAC, the premise was “not to rip and replace.” macmon NAC is manufacturer-agnostic. Therefore it was possible to keep the existing infrastructure, making the deployment cost very minimal.

**Most Important Added Values
Through macmon NAC**

NAC provided effective access control, consistent automated rules, and policies to control all IT and OT devices. Using the intuitive web graphical user interface (GUI) of macmon NAC, the Belden team was able to gain a complete network overview within a few hours.

The implementation of macmon NAC was exceptionally fast as it does not require a software agent. In the process, macmon NAC was able to detect unauthorized remote connections, wireless access points, operator workstations and IoT devices.

In Richmond’s OT environment, with various OT-specific endpoints such as robots and programmable logic controllers (PLCs), macmon NAC has effectively prevented unknown endpoints from gaining connectivity that could negatively impact Richmond’s production facility.

macmon NAC has also excelled at detecting unwanted network events. By monitoring a wide range of network events, it immediately identifies unwanted behavior, whether intentional or unintentional. It detects potentially critical network events, such as duplicate IP addresses, and automatically or manually takes appropriate action.

In terms of granular access control or automatic exclusion, macmon NAC automatically excludes unauthorized network devices such as unmanaged switches from network communication.

macmon NAC also ensures the automatic transfer of access rights. In the event of an authorized device replacement, access rights were securely and dynamically transferred to the new devices to be integrated.

The solution also provides time-limited access to specific areas of the network. For example, an external company such as a technical service provider requires time-limited access to very specific network areas for defined endpoints such as notebooks and control devices. Any access beyond that is automatically denied.

Device localization is another area where macmon NAC excels. If a handheld scanner or programming device is lost, the communication history of the device can be quickly and easily viewed, allowing the correct and targeted action to be taken in the shortest possible time.



“Network Access Control is the core piece of our network security.”

Joel Naumoff

Vice President of Cybersecurity | Belden Inc.

In the Richmond plant’s OT network, macmon NAC is combined with Hirschmann products. By using the EAGLE40 Industrial Firewall and the Hirschmann switches, it was possible to roll out segmented networks with a secure zone system. macmon NAC assigns authorized devices to the correct segment (VLAN) automatically. This enabled a more efficient process that contributes to the cyber hygiene of the plant.

“The deployment of macmon NAC was a very smooth and quick process. There was no downtime related to it, no misconfigurations, no bizarre behavior or bugs.”

Joel Naumoff

Vice President of Cybersecurity | Belden Inc.

Final statement

by the Belden IT

Based on the extensive experience with the successful implementation at the Richmond facility, Belden started deploying macmon NAC globally across more than 70 sites and aims to finish this project by the end of 2024.

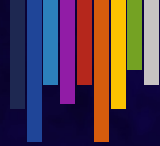
A COMBINED SOLUTION

A combined solution with macmon NAC offers everything to build a reliable industrial network or improve the existing network architecture for increased industrial cybersecurity.



HIRSCHMANN
A BELDEN BRAND





“We never had a tool in the history of Belden that shows us everything that is plugged in. Having this capability is super powerful!”

Ryan Buckner
IT Infrastructure | Belden Inc



With macmon NAC, Belden was able to make its industrial cybersecurity future-proof: **It's automated, efficient, and robust.**

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