Belden

12 reasons for NAC in OT

Awareness is key to protection

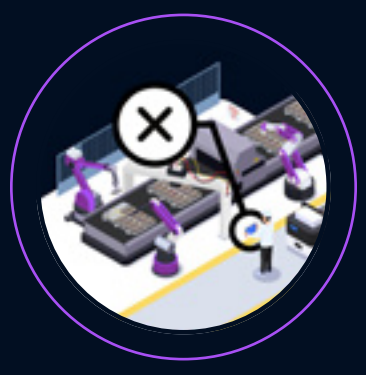
Comprehensive network overview and segmentation of all connected assets support the creation of security zones.

Plant availability is the top priority

A NAC system should not specify fixed implementation strategies, but must allow sufficient freedom to maximize the radius of action of a NAC. At the same time, a NAC must not conflict with consistently high plant availability to ensure business continuity.

Sustainable safety strategy implementation

Flexible, future-proof software solutions are essential for heterogeneous IT/OT networks. A NAC system achieves high sustainability without extensive hardware upgrades.



Unwanted devices stay out

In a hardened OT environment consisting of various OT-specific end devices (e.g. robots, PLC), cybersecurity solutions have to prevent unknown end devices from obtaining a connection that could negatively influence the production plant.

Keeping unwanted devices out

In a hardened OT environment, cybersecurity solutions must prevent unknown devices from connecting and potentially disrupting production.

Meeting legal requirements

Regulatory standards like ISO62443/ISO27001/ ISO9001 require reliable enforcement of corporate policies across the network. Third-party information can help isolate detected threats automatically.

Controlled access to network areas

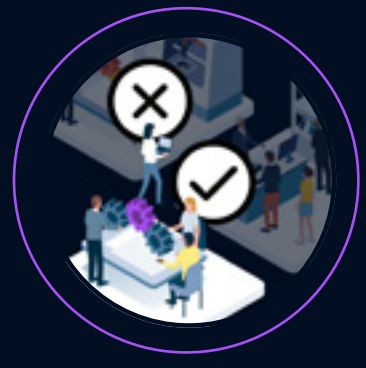
External companies need time-limited access to specific network areas for defined devices. Any access beyond this should be automatically blocked.

Ensuring compliance

OT assets must meet compliance requirements even if they can‘t be protected by conventional technologies. Immediate alerts and responses are necessary in case of compromise.

Time-limited access to specific network areas

An external company (e.g. technical service provider) requires time-bounded access to very specific network areas for defined end devices (e.g., notebooks, control devices). Any access beyond this should be automatically prevented.



Granular access control

Unauthorized devices, such as private routers or unmanaged switches, must be automatically excluded from network communication or given limited access.

Quick device localization

When a handheld scanner or programming device is lost, quick access to its communication history is crucial for initiating targeted measures promptly.

Reducing administrative effort

Security solutions like Belden‘s macmon NAC minimize administrative expenses despite increasing network threats to maintain high acceptance within the company.

macmon nac

Overview Control and Security in the Network