

*Cybersecurity* is no longer just an IT issue -  
**it's a  
production-  
critical factor!**

# **Legacy systems can't cope**

Old PLCs and legacy systems leave significant gaps in production security, failing to meet modern cybersecurity demands.

# **Increased connectivity**

More machines, sensors, and controllers are connected – and more vulnerable to attacks.

# Cyberattacks are on the rise

In Germany alone, cyberattacks caused €179 billion in damages in 2024.

65% of companies now see them as an existential threat (Source: Bitkom / BfV).

# **Rising regulatory pressure**

With the Cyber Resilience Act (CRA), cybersecurity compliance is no longer optional, but a legal requirement.

# **OT cybersecurity is not just an IT concern**

Scalable, integrated solutions are essential to grow alongside the production environment.

# **IEC 62443-compliant OT devices safeguard critical assets**

Industrial controllers meeting IEC 62443 standards can protect legacy PLC systems and enhance security.

# **Vulnerability Management**

Choose suppliers with proactive vulnerability management to prioritize patching critical security gaps.

# **Regular software updates and patches**

Frequent updates are crucial to fix vulnerabilities, prevent exploits, and ensure ongoing protection.

# **VPN access, firewalls, and network scanners**

Industrial controllers with  
cybersecurity apps strengthen  
defenses and reduce  
vulnerabilities.

# **Intrusion detection and prevention systems**

Active monitoring identifies and prevents potential intrusions, enhancing protection.

# How will YOU tackle cybersecurity challenges now?

What steps will you take to improve security in your production environments?

