

FURNITURE MANUFACTURER SECURES ITS ICS NETWORK, KEEPING EMPLOYEES SAFE AND OPERATIONS RUNNING WITH CHECK POINT RUGGED APPLIANCES AND CYBER SECURITY MANAGEMENT

Customer Profile

This company is the largest manufacturer of its kind in the U.S.

Challenge

- Secure 50 industrial manufacturing work centers against cyber threats
- Protect thousands of industrial manufacturing and control systems in harsh environment
- Manage a widespread, comprehensive security infrastructure

Solution

- Check Point 1200R Rugged Appliances
- Check Point R80 Cyber Security Management

Benefits

- Prevented security incidents and protected employees from security-related accidents
- Saved hours of management time with consolidated security management in a single pane of glass
- Avoided costs associated with adding security staff, electrical infrastructure, and space

“Check Point 1200R appliances fit our environment perfectly. The DIN rail mounts made them simple and cost effective to deploy. We simply clamped them to equipment DIN rails and they are automatically powered through OT systems. It eliminated the need to build extra space or run expensive electrical cabling.”

—IT Engineer, Furniture Manufacturer

Overview

Leading Furniture Manufacturer

This company is the largest manufacturer of its kind in the U.S. Its primary manufacturing facility includes 4 million square feet of space, employs 2,000 workers, and sources raw materials from around the world. Protecting mission-critical industrial equipment from cyber threats is difficult for many reasons. The company chose Check Point to make it easier.

Business Challenges

The need to secure Industrial Control Systems (ICS)

The company markets more than 40 different product lines. To produce them, the company relies on hundreds of unique industrial machines and control systems, such as Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs). All of these systems and processes must be monitored to ensure optimal manufacturing quality and uptime.



“Emerging threats increasingly aim to disrupt or take over manufacturing processes by gaining access through SCADA and PLC devices,” said the IT Engineer. “As IT and operational technologies (OT) converge, it’s critical to ensure cybersecurity for OT systems, in addition to IT systems.”

Protecting Industrial Control Systems (ICS) in manufacturing floor systems with traditional security measures is difficult. Unlike IT environments, sawdust, temperature swings, vibration, and electromagnetic interference make a factory floor hostile to traditional electronics. Space and power is dedicated to manufacturing systems, making it difficult to fit additional devices for security. In addition, many factory systems were not designed with cybersecurity in mind, so patching or upgrading can be risky—or even impossible. Some systems were imported years ago from Europe, and the vendors no longer exist.

“The IT team needs to secure both IT and OT investments,” said the IT Engineer.

“We were looking for a way to add secure boundaries to our OT environments and protect a wide range of systems.”

Solution

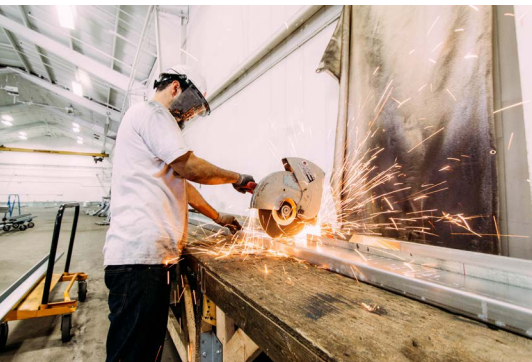
Creating a Safe Boundary

The IT Engineer was familiar with Check Point solutions, and after evaluating several options, the company chose Check Point 1200R Rugged Appliances to secure its work centers. Check Point 1200R appliances deliver proven, integrated security in harsh environments, and they support an extensive range of industrial-specific protocols for comprehensive coverage. The Check Point 1200R appliances also include next-generation firewall, IPS, application control, antivirus, anti-bot for full-featured defense of the ICS systems, as well as network bridges between OT and IT systems.

“Check Point 1200R appliances fit our environment perfectly,” said the IT Engineer.

“The DIN rail mounts made them simple and cost effective to deploy. We simply clamped them to equipment DIN rails and they are automatically powered through OT systems. It eliminated the need to build extra space or run expensive electrical cabling.”

The company also uses Check Point R80 cyber security management to manage 50 Check Point 1200R appliances deployed across multiple work centers around the world. Check Point R80 consolidates systems, policies, and management into a unified console for management simplicity. Having a single policy for users, data, applications, and networks enables granular control to save time and ensure consistency across environments.



“Check Point anti-bot and anti-malware capabilities also help us ensure that employees are protected from accidents that could result from malicious takeover of an industrial device.”

—IT Engineer, Furniture Manufacturer

Results

Protecting Systems and People

Check Point 1200R appliances are deployed between the IT network and OT networks to monitor all traffic going in and out of the company’s manufacturing facilities. The appliances use next-generation firewall and IPS to detect inbound threats to SCADA and control networks.

“We haven’t had any security incidents since implementing R80 and the 1200 rugged appliance,” said the IT Engineer. “Check Point anti-bot and anti-malware capabilities also help us ensure that employees are protected from accidents that could result from malicious takeover of an industrial device.”

No Extra Staff Needed

Check Point R80 cyber security management runs as a virtual machine and gives the team a single pane of glass for administering the entire environment. Team members don’t have to log into each device individually, which saves hours of time. Concurrent administration features enable multiple administrators to be logged in at the same time to increase efficiency. All policy changes can be reviewed before they are installed to further reduce risk.

“We didn’t have to add staff,” said the IT Engineer. “Check Point systems are very administrator-friendly so we don’t have to spend hours a week monitoring them. We watch for threats, but they are almost ‘set-it-and-forget-it’ simple.”

Good Advice

The company now rests assured that critical systems and employees are protected. Check Point 1200R appliances are protecting thousands of devices on its network, and by extension, manufacturing employees.

“We have peace of mind knowing we’re protected,” said the IT Engineer. “My advice to other manufacturing IT teams is to look at Check Point to protect their OT investments. Threats and new exploits are targeting industrial control and other hardware devices—there’s too much at stake to be unprepared.”



For more information, visit:
<https://www.checkpoint.com/products/>