WEBPORT SECURITY

A Defense-in-Depth approach to keeping you safe.

By leveraging the right devices and following the correct security procedures, OEMs and end users can remotely oversee operations, perform real-time diagnostics, and keep maintenance costs low.

WebPort Security

Converging manufacturing and enterprise networks allow manufacturing insights to enable better business decisions. The ever-merging world economy is driving businesses to compete on a global level. WebPort allows manufacturers to make critical operational improvements and gain a competitive edge by allowing remote access to their control systems.

Often times the potential gains of network convergence are haunted by the hidden security challenges traditionally found in any IT infrastructure. Network convergence adopters take on the formidable task of determining network ownership and blending cultural differences between IT and OT security deployments. WebPort was developed to alleviate IT and OT concerns. WebPort provides a secure approach to unite both parties to enable better business decisions.

"A non functioning, isolated drive can result in a significant loss of revenue. With cloud technology, when this drive issues a warning or fault, the information is easily propagated to create a work ticket for a support engineer. Within minutes, a cloud-based, asset-monitoring application has an expert looking at the fault and taking corrective actions." - Rockwell Automation

WebPort Security Features

Data Encryption:
With the help of Microsoft Azure, WebPort Connects encrypts all of your data to maximize your security and privacy.

Virtual Private Network (VPN):
As part of a contemporary solution, VPNs ensure confidentiality, sender authentication, and message integrity. WebPort uses already existing IT infrastructure to establish a secure connection.

Network Address Translation (NAT):
Regulates the network traffic coming into and leaving a private network. NAT restricts network access to only authorized connections.

User Authentication:
Only authenticated users can access WebPort. WebPort supports multiple authorized users, along with custom roles that are set to limit user access. User roles can be monitored and audited for full transparency.

Defense-in-Depth

WebPort's security was developed in line with the Defense-in-Depth approach used by both Cisco and Rockwell Automation. Our goal is to help OEMs build layers of security into their machinery and end users' facilities. A Defense-in-Depth security strategy layers technical and non-technical protection to detect and thwart both internal and external unauthorized activities.

No single security technology can fully protect any industrial controls system. Beyond the WebPort standalone device, our Defense-in-Depth security strategy includes policies, procedures, and other technology-related security processes that guard OEMs from the security threats of any modern solution. By deploying a layered defense, the protection of all of the layers guard against the unseen vulnerabilities of any single security approach. WebPort helps OEMs reduce their susceptibility to any accidental or unauthorized activities that impact the safety, integrity or confidentiality of their systems.

1. **Data Encryption**
   Keeps your data private and secure.
2. **Network Security**
   Firewalls, intrusion detection/prevention systems (IDS/IPS), port security, routers, switches and other networking implementations.
3. **Application Security**
   WebPort allows the administrator to authorize user roles, white/black lists and permissions.
4. **Device Hardening**
   Update firmware, patches and antivirus software on network devices.
5. **Physical Security**
   Limit physical access of devices, cabling, control panels, control rooms, and any other areas of high importance.
6. **Best Practices & Policies**
   Help monitor, identify, isolate and counter network security threats.

Security Best Practices

- Keep all control system PCs updated with contemporary antivirus and anti-malware protection.
- Control network access through access lists and port-blocking devices.
- Test all updates before implementation.
- Schedule all network updates and maintenance during factory downtimes.
- Have a password policy that enforces password history, maximum password age, length and requirements.
- Limit all guest accounts on clients and servers.
- Develop recovery policies and test backup regularly.
- Evaluate firewall configurations to ensure non-essential traffic is blocked.
- Obtain all product-specific electronic content (firmware, software, updates, etc) directly from trusted sources.

Spectrum Controls
1705 132nd Ave NE
Bellevue, WA 98005

+1 (425) 746-9481
www.WebPortConnects.com
www.SpectrumControls.com
Spectrum@SpectrumControls.com

SPECTRUM CONTROLS

Rockwell Automation
Encompass™ Product Partner
Global