Critical infrastructure and industrial control systems face increasingly costly attacks that endanger human and environmental safety, operational integrity, and intellectual property. Recent revelations regarding physical damage from cyber attacks against the energy and manufacturing sectors demonstrate that the threat is real.¹ ² Remote locations such as power substations and corporate networks can serve as attack gateways leading to control networks.

While control networks are vulnerable to cyber and physical attacks, operations technology (OT) teams are understandably resistant to deploy cybersecurity products within these networks because traditional IT active discovery and threat-response techniques may take down fragile critical systems. The concern over deploying cybersecurity products in control networks and the difficulties in deploying them in substations has resulted in a lack of visibility into threats in these networks.

The physical and geographical scale and complexity of control networks such as mining operations, refineries, and manufacturing plants pose an additional challenge. When a security product is deployed, management and integration then become the next large hurdle to overcome. While IT staffs handle many deployment and administrative tasks, it’s not uncommon for OT engineers to be given responsibility for cybersecurity as well, increasing operator burden.

Advanced Cybersecurity for Industrial Environments

Like all other networks today, industrial control networks require advanced threat protection. But the solution must not interfere with safe, reliable service delivery. The new Cisco® ASA with FirePOWER™ Services next-generation firewalls meet these needs by delivering integrated threat defense, low total cost of ownership, and simplified security management without affecting safe, reliable service delivery.

These ASA models are available in both desktop (5506-X and 5506W-X) and 1-rack-unit (1RU) rack-mount (5508-X and 5516-X) form factors for carpeted spaces and as a DIN-rail, ruggedized appliance (5506H-X) for substations and other extreme-condition locations.

Leading Cybersecurity, Manageability, and Cost of Ownership

Cisco ASA with FirePOWER Services delivers security for the real world, from the corporate network to the control center, to the substation or shop floor. The solution integrates precise application visibility and control with leading advanced malware protection and next-generation intrusion detection and prevention capabilities.

The on-device and optional centralized management options both provide exceptional threat visibility, contextual information, and analytics across the distributed enterprise. The threat-correlation feature highlights risks and assists with the prioritization of monitoring and remediation, reducing operator burden.

Cisco ASA with FirePOWER Services for industrial control networks provides cost-effective cybersecurity. It lowers your total cost of ownership by tightly integrating multiple leading threat-defense technologies along with the Cisco AnyConnect® VPN into a single device, thereby reducing hardware costs and reducing space and power requirements.

Next Steps

Get started by contacting a Cisco partner in your region:
Locate a Cisco Partner.