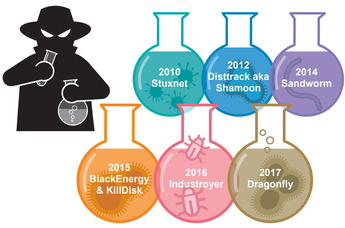
MOXA
Reliable Networks Sincere Service

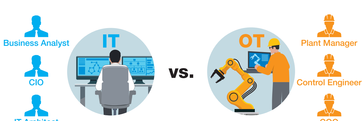
Do You Think Your Industrial Networks Are Secure?

Cyber Attacks Frequently Target Industrial Networks



Both IT and OT Personnel Have to Take Responsibility for Industrial Cybersecurity

The Approach Taken to Protect Enterprise Networks Does not Work for Industrial Networks



No. 1 Priority	Confidentiality	Availability
Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Target	Windows computers, servers	Industrial legacy devices, barcode readers
Environmental Conditions	Air-conditioned	Extreme temperatures, vibrations and shocks

A comprehensive understanding of industrial cybersecurity allows you to take a holistic approach to protect your networks.

Things You Should Know

When implementing industrial cybersecurity

1

Industrial control systems cannot endure downtime even for a few seconds.

2

The legacy devices used on industrial networks often do not have extensive security features, which creates weaknesses and potential vulnerabilities.

3

Industrial control systems often contain a wide variety of operating systems and devices from different vendors. When it comes to security measures, there is no unified way to enhance security.

Moxa takes a holistic approach to cybersecurity for industrial networks. We offer rugged products that have enhanced security features and network management software that allows you to view the security status of your network.

For more information, please visit our website: www.moxa.com/security