MODERN INFRASTRUCTURE AND MULTICLOUD

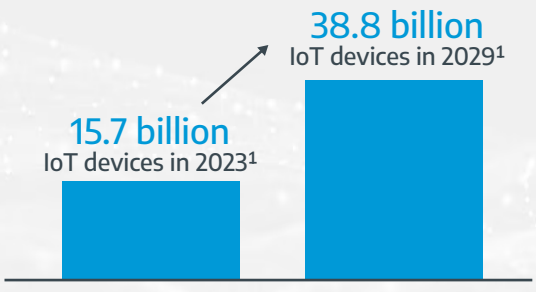
Securing the Industrial Internet of Things

The Rise of IIoT and Why It Matters for Security

As industries including manufacturing, healthcare, telecom, energy and more, are increasingly relying on connected machines and devices to become more productive and efficient than ever before, cybersecurity threats targeting them are also on the rise. New tools and expert guidance can help organizations minimize the risks and maximize the returns.

Billions of Devices

Networking and telecommunications company Ericsson estimates that the number of Internet of Things (IoT) devices will more than double by 2029.[1]



Medical devices, factory machines, and security cameras are just a few of the Industrial Internet of Things (IIoT) devices that gather critical data at the edge and deliver value.

Attacks on Industry

Industries employing IIoT equipment are among the most targeted sectors for cyberattacks, as observed by IBM's X-Force team.[3]

Three IIoT-driven industries among the top ten most-attacked sectors:

- Manufacturing[3]
- Energy[3]
- Healthcare[3]

Understand the threat landscape to make informed decisions for reducing risk.

25.7%
Manufacturing's share of attacks[3]

69.6%
Percentage of attacks targeting critical infrastructure[3]

84%
Percentage of critical infrastructure incidents preventable with Zero Trust, diligent patch management, and other best practices.[3]

Securing Operational Technology

How organizations are rising to meet IIoT security challenges:

- Advanced networking infrastructure
- Industry-specific inline firewalls
- Micro-segmentation
- Secure remote management
- Zero Trust practices

And more, implemented with the help of trusted partners.

3 steps for assessing OT and IIoT

1. Pre-planning

Connection experts lead virtual briefings to define organizational objectives for OT and cybersecurity assessments.

2. On-site visits

Non-invasive assessment uses deep packet inspection for both IT and OT protocols without impacting operations. Assessments also include deep-dive inventories of networking system software, drivers, firmware, storage, and more.

3. Out briefings and recommendations

Comprehensive reports and follow-up meetings enable stakeholders to review risks and prioritize recommendations. For example, Connection's Manufacturing OT Cybersecurity Assessments deliver deep-dive reports and recommendations for securing operational technology (OT), including IIoT devices and machines.

How Connection Can Help

Explore our Resources
Connection.com/cybersecurity

Contact an Expert
1.800.998.0067

Sources:

[1]Ericsson, IoT Connections Outlook
[2]McKinsey & Company, What is the Internet of Things (IoT)?
[3]IBM, X-Force Threat Intelligence Index 2024

Connection® we solve IT®