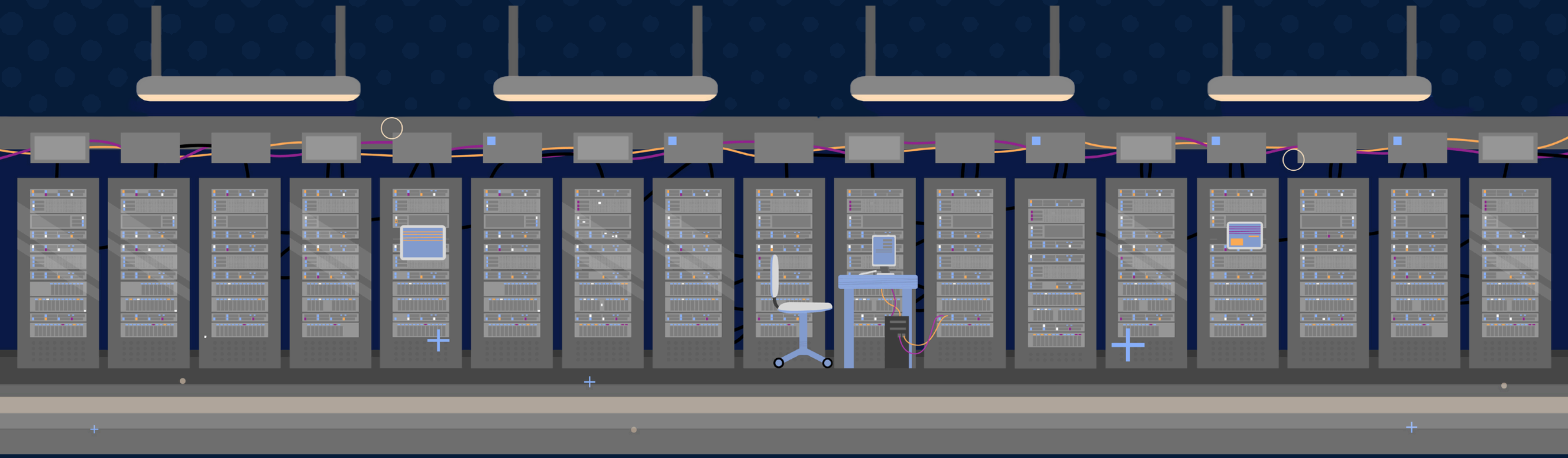
Are Your PLCs a Backdoor to Your Network?

Many PLCs are nearing the end of their lifecycle. Is your system prepared to handle the transition? Act now before vulnerabilities expose your network to cyber threats.

inflexion point

Outdated PLCs Could Cost You Millions

If your PLC is on this list, your network may be vulnerable to a cyberattack. These breaches don't just cause delays; they cripple production, disrupt entire operations, and result in millions of dollars in losses.



High-Risk PLCs Reaching End-of-Life

If your facility depends on PLCs from many leading brands, you may be relying on systems that are approaching the end of their lifecycle. These outdated technologies are no longer supported, increasing the risk of security vulnerabilities and operational disruptions. Proactively plan your migration strategy now to mitigate potential risks and ensure uninterrupted performance.

Two Paths You Can Take

The Risks of Waiting vs. The Benefits of Acting Now

Fix It Later

Delaying upgrades may seem easier, but the risks grow daily, leaving your network exposed to costly attacks.

Fix It Now

Stregthen your network, automate modern processes, and prevent future breaches with immediate action.

inflexion point

Why Teams Hesitate

Upgrading outdated systems is often delayed due to a combination of operational and financial concerns. Here are the most common reasons teams hesitate:

- **Plant Downtime:** An upgrade requires shutting down equipment, leading to operational delays and affecting production schedules.
- **Loss of Production/Revenue:** Every minute of downtime equates to a loss in production and revenue, making it difficult to justify scheduling upgrades.
- **Network Isn't Connected to the Internet:** Some teams believe their systems are safe because they operate in isolated environments, but internal threats and offline vulnerabilities still exist.
- **Perceived Low-Risk Vulnerabilities:** Vulnerabilities might have a low Common Vulnerability Scoring System (CVSS) rating, making them appear less urgent.
- **Cost of Onsite Remediation:** Bringing in specialized technicians to perform upgrades and fixes can be expensive and logistically challenging, adding to the reluctance.

Why Upgrade Now?

Despite these challenges, the benefits of upgrading far outweigh the risks of inaction. Here’s why companies should prioritize updates:

- **Protect Against Known Vulnerabilities:** Even low-CVE vulnerabilities can be exploited, and upgrading ensures your system is safeguarded against known risks.
- **Reduce the Risk of Production Loss:** A secure system reduces the chances of a cyberattack that could lead to catastrophic production downtimes and financial losses.
- **Demonstrate Security to Shareholders:** Proactively upgrading shows your commitment to security, which improves confidence among shareholders and stakeholders.
- **Maintain Public/Client Trust:** Clients and partners value businesses that prioritize security, and avoiding breaches helps sustain trust and credibility.

inflexion point

Secure Your Future, Upgrade Today!

The longer you wait, the more your systems are at risk. Protect your operations, maintain client trust, and demonstrate your commitment to security. Don't wait for a breach to act—ensure your network's safety with proactive upgrades.

Protect Your Operations, Protect Your Customers, and Protect Your Brand.

www.inflexionpoint.ai