Reimagining Building System Cybersecurity
Enhancing Data Center Outcomes

Data centers rely on connected building and critical infrastructure systems to support continuous operations. As facilities expand, workloads grow, and systems become more connected, operators must manage increasing cyber exposure alongside workforce constraints and evolving regulatory and customer requirements.

Publicly reported cyberattack and ransomware outages averaged about 25 days of downtime.[1]

49% of vulnerabilities disclosed in the first half of 2025 that could affect OT environments were rated high or critical.[2]

Breaches affecting OT environments cost approximately EUR 4 million; 23% of affected organizations reported damage to OT systems or equipment.[3]

Will current practices stand up to evolving pressures?

How a traditional approach may increase risk:

- **Limited understanding of OT cybersecurity posture and gaps across connected infrastructure:** Critical gaps may go undetected, leaving building and infrastructure systems exposed and making it difficult to focus resources on the highest-priority risks.
- **Incomplete visibility into connected IT and OT assets, vulnerabilities, and remediation priorities:** Unknown assets and unprioritized vulnerabilities create security blind spots, slow remediation, and allow weaknesses to persist across connected systems.
- **Inconsistent, infrequent, and reactive OT patch and update management:** Delayed updates can leave OT systems exposed to known vulnerabilities, while patching that is not carefully planned and coordinated may disrupt critical operations.

SIEMENS

Transition from reactive OT cybersecurity to proactive OT cyber risk management

You have goals. Siemens helps you achieve them. With our outcome-based approach, we partner with you to develop a customized service program that improves facility operations and supports your key business objectives.

Improving OT cybersecurity through digital services

- **Assess:** Understand your OT cybersecurity posture and identify gaps across connected infrastructure
- **Identify:** Gain visibility into connected IT and OT assets, known vulnerabilities, and remediation priorities
- **Protect:** Keep eligible building systems securely updated through validated, controlled software updates

Outcomes enabled:

Customer Scenario

Customer objective: A large data center sought to secure its connected building systems and reduce the risk of cyber incidents affecting critical infrastructure and continuous operations.

Siemens solution: Siemens conducted a Cybersecurity Gap Assessment to evaluate the data center's OT cybersecurity posture and identify opportunities to strengthen protections for its connected building systems. Asset and Vulnerability Reporting helped identify connected building system assets and known vulnerabilities, while OT Patch Management supported validated, controlled updates for eligible systems.

Outcomes: The facility team could use these findings to prioritize remediation, improve visibility into vulnerabilities, and plan updates around operational requirements, supporting cyber resilience and compliance readiness.

Contact Us

Discover how Siemens cybersecurity services can help assess OT risk, identify vulnerabilities, and support controlled updates to eligible building systems. For more information, visit siemens.com.

1. Uptime Intelligence
2. IBM X-Force
3. IBM X-Force

SIEMENS