Reimagining Building System Security
Enhancing Data Center Outcomes

As data centers expand and operations become more complex, teams must protect critical areas, manage access for employees, contractors, and visitors, and respond quickly to security incidents and system failures across 24/7 operations. Workforce constraints, aging and siloed systems, and evolving customer and regulatory requirements add pressure—all while data centers must protect critical infrastructure and support secure, uninterrupted operations.

Nearly two-thirds of data center operators report difficulty finding or retaining staff.[1]

57% of end users cited aging or outdated physical security or IT infrastructure as a primary organizational challenge.[2]

60% of respondents replacing legacy security technology said integrating new capabilities was their main motivation. [3]

Will current practices stand up to evolving pressures?

How a traditional approach may increase risk:

- **Limited centralized visibility into security system health, coverage, performance, and events:** Periodic checks and separate alerts can obscure device issues, coverage gaps, recurring problems, and changing conditions across data center facilities.
- **Manual, fragmented access rights governance, alarm management, workflows, reviews, and documentation:** Separate systems and labor-intensive processes can delay credential changes, hinder event prioritization, and create inconsistent records for employees, contractors, vendors, and visitors.
- **Reactive maintenance, siloed systems, and limited lifecycle planning and modernization:** Faults may go unaddressed until failure, while disconnected systems slow response and deferred modernization allows vulnerabilities and obsolescence to persist.

SIEMENS

Transition from static, reactive security to continuous security 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 physical security through digital services

- Gain centralized visibility into security system health, coverage, performance, and events
- Strengthen access governance and coordinate physical, IT, and OT security workflows
- Improve system reliability through proactive services and phased modernization

Outcomes enabled:

Customer Scenario

Customer objective: A large data center operator needed to improve physical security system reliability across multiple facilities while reducing manual work, outdated access rights, false alarms, and video coverage gaps.

Siemens solution: Siemens provided Access Rights Review, Video Health Insights and Management, Camera Health Reporting, and False Alarm Detection & Diagnosis to identify issues, support remote resolution, and direct targeted onsite maintenance.

Positive results: The organization strengthened access governance, improved system reliability, and reduced manual effort—helping protect critical infrastructure, support compliance readiness, and maintain continuous operations.

Contact Us

Discover how Siemens can help you enhance performance, boost staff efficiency, and proactively address system issues. For more information, please visit siemens.com

1. Uptime Institute, Global Data Center Survey 2025
2. Genetec, 2025 State of Physical Security Report
3. Genetec, 2026 State of Physical Security Report

SIEMENS