SIA
SECURITY INDUSTRY ASSOCIATION

SECURING DATA CENTERS

A Guide to Trends and Strategies for the Physical Security of Data Center Facilities

PRODUCED WITH SUPPORT FROM

MOTOROLA SOLUTIONS

PAVION™
CONNECT AND PROTECT

PLUGOUT

Report Price
$99

Employees of SIA corporate members can obtain this report as a free download thanks to your firms' membership. Non-members can purchase this report online.

Contents

Author

Amy Dunton, Co-Chair
SIA Perimeter Security Subcommittee, and
managing partner, Sulton Security

Abstract

The global data center market is expanding at an unprecedented pace. In 2025, the world will generate 181 zettabytes of data—an increase of 23% year over year. That translates to 2.5 quintillion bytes created every day: 29 terabytes every second. This explosive demand for storage and processing fuels the industry's relentless focus on power and cooling. Yet while those conversations dominate, physical security remains in the back seat—even though it is equally critical to resilience. At the same time, the surge in demand is reshaping the market with hyperscale growth, colocation competition and enterprise expansion.

With rapid growth comes new complexity: outdated specifications, siloed security systems and partners experienced in other markets yet unfamiliar with the unique demands of data centers—all of which threaten the resilience of critical digital infrastructure. This paper examines the challenges shaping physical security for data centers today, with a focus on integration, interoperability and life-cycle management. Drawing from manufacturers, integrators, and end users, it highlights not only emerging technologies but also the persistent risks of treating security as an afterthought. The result is a forward looking roadmap to deliver resilient security that enables, rather than hinders, growth.

PRODUCED WITH SUPPORT FROM

MOTOROLA SOLUTIONS

PAVION™ CONNECT AND PROTECT

PLUGOUT

Introduction: The Evolving Risk Landscape

Despite decades of incidents and billions invested in cyber resilience, physical protections at many data centers remain constrained to just 5% or less of overall build budgets, and sometimes even less than 1% for major data center companies when building at scale. Physical security protections are too often cut in late-stage value engineering, copied from outdated specifications or deployed without regard to integration across perimeter, access control and surveillance.[1]

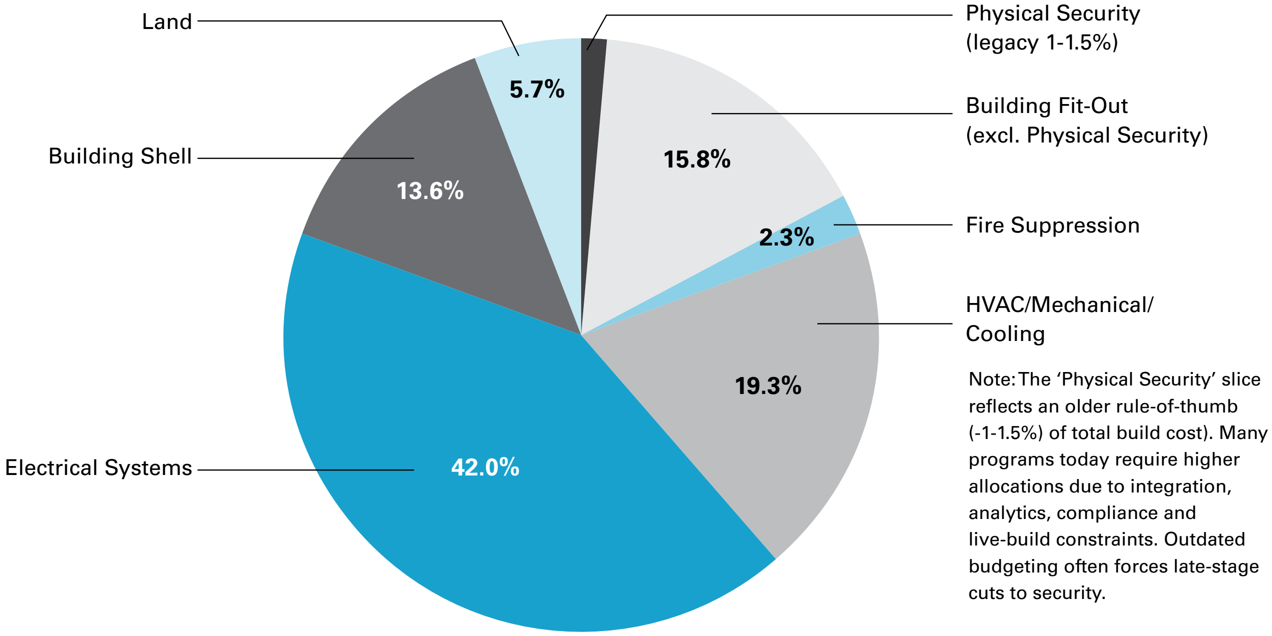
The results are predictable: costly redesigns, operational blind spots and increased liability.

Speed-to-market pressures compound these issues. Entire campuses are now delivered in overlapping construction phases; operators bring a building or data hall online while adjacent areas remain active work zones. This raises risk: live racks and guard activity sit next to heavy construction, creating safety, access and incident-response challenges. Integrators must sequence bring-ups in days rather than weeks, with little tolerance for missteps.

Finally, pace and scale have drawn in a wave of experienced partners from other verticals—architects, engineers, general contractors, subcontractors and integrators who excel elsewhere but may be new to data center norms. Without the right education and common requirements, assumptions from retail or warehousing are transplanted into environments with materially different uptime, compliance and tenant requirements.

This white paper is not another checklist. It consolidates perspectives from operators, integrators and manufacturers to expose systemic gaps and to highlight where innovation is changing the equation—from artificial intelligence (AI) analytics that slash nuisance alarms to governance models that elevate security into earlier design decisions.

Illustrative Data Center Build Budget Allocation
(Carving out a legacy 1-1.5% 'Physical Security' slice)

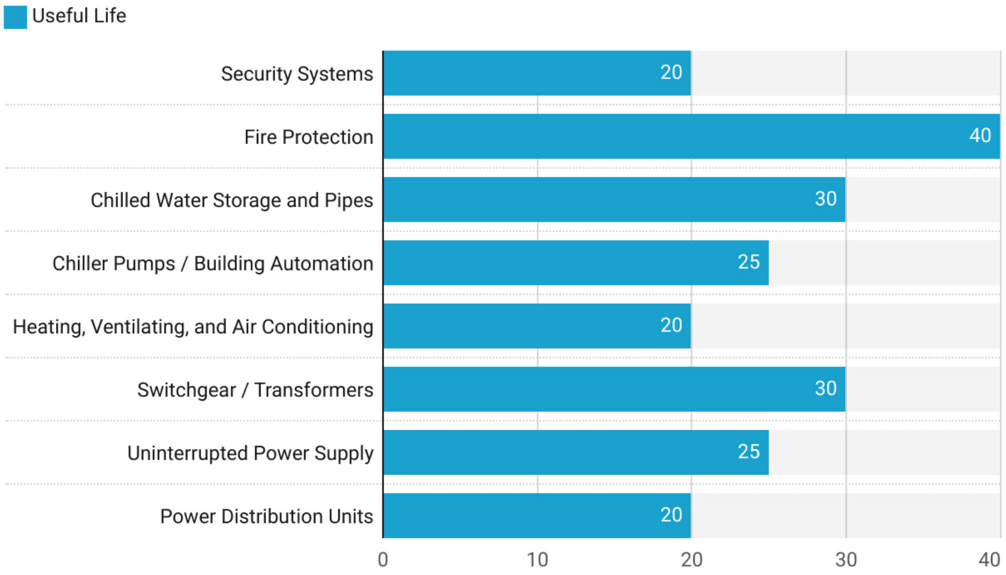


Note: The 'Physical Security' slice reflects an older rule-of-thumb (-1-1.5%) of total build cost). Many programs today require higher allocations due to integration, analytics, compliance and live-build constraints. Outdated budgeting often forces late-stage cuts to security.

[1] In this paper, "surveillance" refers broadly to monitoring functions, which may include but are not limited to video security systems (e.g., cameras, analytics and supporting sensors).

Useful Life of Data Center Equipment Components

Useful Life in Years



(Useful Life in Years)

Source: Market.us Scoop

The Current State of Data Center Physical Security

Physical security has historically trailed power, cooling and network infrastructure in attention and funding. With budgets hovering near 5% of total build costs, security is often the first line item cut under pressure. Those cuts rarely disappear—they reappear as retrofits and operational pain. However, cutting security can often bring audit and compliance risk, so security budgets of data centers are not cut as frequently as in other industries.

Specifications are frequently recycled from other industries or from older generations of data centers. In practice, this yields predictable failures: cameras mounted 18 feet high expected to perform facial recognition, license plate recognition specified at angles that are optically impossible and access control readers that force multitenant sites to deploy "reader farms" because they cannot interoperate. Operators report discovering, post-warranty, that key solution components are missing or installed incorrectly—with little recourse to recover costs.

Specifications are frequently recycled from other industries or from older generations of data centers. In practice, this yields predictable failures, including:

- Cameras mounted 18 feet high but expected to deliver facial recognition
- License plate recognition specified at angles that are optically impossible
- Access control readers that force multitenant sites to deploy "reader farms" because they cannot interoperate
- Rough-ins and headend locations placed incorrectly, requiring costly rework
- Perimeter systems that are not operational before the data center itself goes live—forcing owners to rely on temporary measures until corrected
- Post-warranty discoveries that key solution components are missing or installed incorrectly—leaving operators with little recourse to recover costs

Security is often just a nominal percentage of build budgets—making it the first place cuts are made, and the last place issues are discovered.

Design accountability is fragmented. Perimeter elements (e.g., fencing, gates, bollards) are usually scoped under construction divisions, while access control, video, visitor management and alarms are handled by security. Without an integration owner, systems arrive in silos. Even where detailed specs exist—often 70+ pages with exact model and part numbers—visibility into what subs actually order can be limited; substitutions go unnoticed until a failure.

Global scale adds complexity. Practitioners report that truly "global" integrator coverage is uncommon. Even national consistency is difficult. The pragmatic answer, many operators note, is a roster of multiple integrators—often five or more—who are aligned to common standards and governance, rather than a sole-source model that cannot keep up with speed and geography.

Market and Technology Trends Shaping the Future

Artificial intelligence and advanced analytics are resetting expectations. End users report that AI-driven analytics can reduce nuisance alarms by as much as 90%, reaching high accuracy after a brief learning period. As analytics mature, they move beyond detection to classification—distinguishing benign activity from credible threats and pushing only actionable events to operators.

Integration is widening from "video + access" to include radios/voice, intrusion, radar, thermal, and environmental sensors. The outcome is not alerts for their own sake, but coordinated responses: policy-driven actions that trigger doors, cameras, and communications together. Equally, version control matters—mismatched software baselines routinely break otherwise sound integrations.

Procurement is evolving. "As-a-service" models shift capital expenditures to operational expenditures, embed refresh cycles and help operators avoid lock-in to aging platforms. Performance-based specifications are replacing manufacturer-named specs, opening the door for innovators—provided they can meet scale and interoperability requirements.

Don't confuse meeting the performance spec with meeting the need.
A gate meets impact rating but can't be supervised from the headend; a reader meets range but lacks supported drivers; cameras meet resolution but won't integrate with the video management system; sensors alarm, but events can't flow to the security information and event management system. Specify outcomes and integration so "compliant" also means deployable, supportable and operable at scale.

End users report that AI-driven analytics have reduced nuisance alarms by as much as 90%, reaching near-perfect accuracy after a learning period.

Sustainability pressures—energy efficiency, reduced guard reliance, modular deployments—now shape physical security roadmaps. A main driver for adopting emerging technologies is reducing reliance on on-site guards: operators are prioritizing capabilities that replace static posts with automated, verifiable detection and remote response (analytics-enabled video, sensor fusion, intelligent intercoms, robotics and managed global security operations centers), preserving or improving detection and response while redeploying guard hours to higher-value tasks. Globalization raises a final trend: few partners can truly deliver consistent implementation across regions. Many operators prefer hybrid approaches—global standards and governance paired with strong local execution—so they can achieve consistency without sacrificing regional agility.

Strategic Considerations for Manufacturers and Integrators

Start with the market, not the product.

The data center sector is not a place to copy-and-paste approaches from enterprise, retail, education, or warehousing. That can look like bringing a butter knife to a cybersecurity fight. Uptime, speed-to-market, multitenant complexity, version discipline and global–local delivery patterns make this environment fundamentally different. Manufacturers and integrators who thrive here begin by understanding the operating model they're entering—how campuses are phased, how standards are governed, how tenants drive requirements and how accountability travels from design through commissioning and operations.

> **If your strategy starts with "what we sell" instead of "how data centers are built and run," you're already behind.**

What "market understanding" means in practice

- **Uptime and phasing realities:** Live buildouts ("part 1.1" online while adjacent areas are still under construction) change risk, sequencing and commissioning methods.
- **Multitenant and colo nuance:** Reader standards, badging models and visitor workflows must coexist without "reader farms" or proprietary lock-in.
- **Global standards, local execution:** Expect hybrid delivery—central standards and governance, executed by multiple regional integrators.
- **Version control as a discipline:** Small firmware or software mismatches routinely break integrations—plan for baselining and regression tests.
- **Governance and acceptance:** Performance-based specifications, witness tests and measurable outcomes are increasingly the norm.

Additional Resource

SIA's recent Vertical Insight Symposium on Data Centers provides market strategy and input from Allegion, SAGE Integration and Wesco, and is available as an on-demand recording.

ALLEGION™ SAGE Integration wesco

Interoperability is non-negotiable

Operators expect **API-first** systems that integrate across perimeter, access, video, voice, intrusion, radar/thermal and environmental sensors. Products that cannot participate in a larger ecosystem will be sidelined—regardless of feature depth.

Prove you can deliver at scale

New entrants frequently underestimate: products must be able to pass application security, review global stock keeping units (SKUs), logistics, spares and return material authorizations (RMAs) and the field engineering bench required for 24/7 response. Commitments must match capacity—overpromising at scale erodes trust quickly and is hard to recover.

Structure your organization for the vertical

Data centers don't map neatly to regional sales hierarchies. Winning teams:

- Assign **global account "quarterbacks"** with authority over standards and success metrics
- Use **regional delivery teams** for site execution and sustainment
- Align **compensation to account outcomes**, not territorial wins (to avoid internal friction that the customer feels)

Compete on life cycle, not line items

Treat programs as **multiyear partnerships**. Expect 6–12+ month vendor reviews, pilots and integration tests before standard inclusion. Build offers that include life-cycle refresh, health checks, version management and upgrade paths—not just initial install.

Guard against value engineering traps

Performance-based specs help, but only if substitutions are controlled. "Low-cost equivalents" that break interoperability or durability create downstream risk for tenants and operators—and will cost more in retrofits and reputation.

CHECKLIST

Are you ready for the data center market?

□ Have we mapped our **integration points** (APIs, events, identity, voice) to the operator's ecosystem?

□ Can we keep **all sites aligned** on the same version and prove, through testing, that **updates won't break existing functions**—at the pace operators demand?

□ Do we have **global SKUs/logistics** and a realistic **RMA/field response** plan?

□ Is our team **organized around accounts**, with a dedicated data center practice and clear handoffs to regions?

□ Do our offers include **life-cycle commitments** (e.g., health, refresh, roadmap alignment), not just one-time delivery?

□ Can we pass **performance-based acceptance** (e.g., witness tests, measurable outcomes) without vendor-specific carve-outs?

Interoperability and scale readiness beat features in a demo—every time.

Strategic Considerations for Practitioners (Operators and Security Leaders)

Embed security early. Bringing security in after civil, structural and mechanical, electric and plumbing decisions guarantees avoidable compromises. Early security participation aligns perimeter, access and surveillance with site plans, utilities and traffic flows—reducing change orders and improving outcomes.

Adopt a multi-integrator strategy governed by standards. Given speed and geography, a single partner rarely suffices. Documented standards, approved product lists and certification paths enable multiple integrators to execute consistently. Maintain a living baseline and a strict process for exceptions and version control.

Align construction phasing with security risk. The new norm—lighting up partial spaces while adjacent areas are still under construction—demands controls for live-build environments: zoned access, temporary surveillance coverage, clear demarcations between "live" and "construction" and rapid incident-response playbooks.

Strengthen accountability in procurement. Require visibility into suborders against specifications, including serials, firmware baselines and commissioning checklists. Tie acceptance to demonstrated performance, not just installation. Where possible, use performance-based specs with measurable outcomes and witness tests.

Coordinate with law enforcement and first responders. Preplanned access protocols, radio interop and scenario exercises prevent delays in emergencies. Integrate public-safety requirements into site design (e.g., apparatus access, egress routes, water use constraints).

Invest in people and process. A widening skills gap affects every role—from end-user security teams to integrators in the field. Build internal training, vendor certification requirements and on-call escalation paths. Clarify responsibilities between security and construction for Div. 32 (site) and security scope to avoid the "everyone and no one" problem.

Looking Ahead:
Emerging Challenges and Opportunities

Cyber-physical convergence will define the next decade. Just-in-time identity management, physical-logical event correlation and risk scoring will inform access decisions and incident response in real time. The boundary between "IT security" and "physical security" will continue to blur.

Adaptive, software-defined security is coming into view. Policies, not point devices, will orchestrate responses; infrastructure will become more modular, with analytics and automation absorbing routine decisions and escalating only the exceptions.

Governance must keep pace. Innovative architectures will stall without compliance frameworks that recognize and guide their use. Practitioners caution that models will succeed only when aligned with standards and auditable controls.

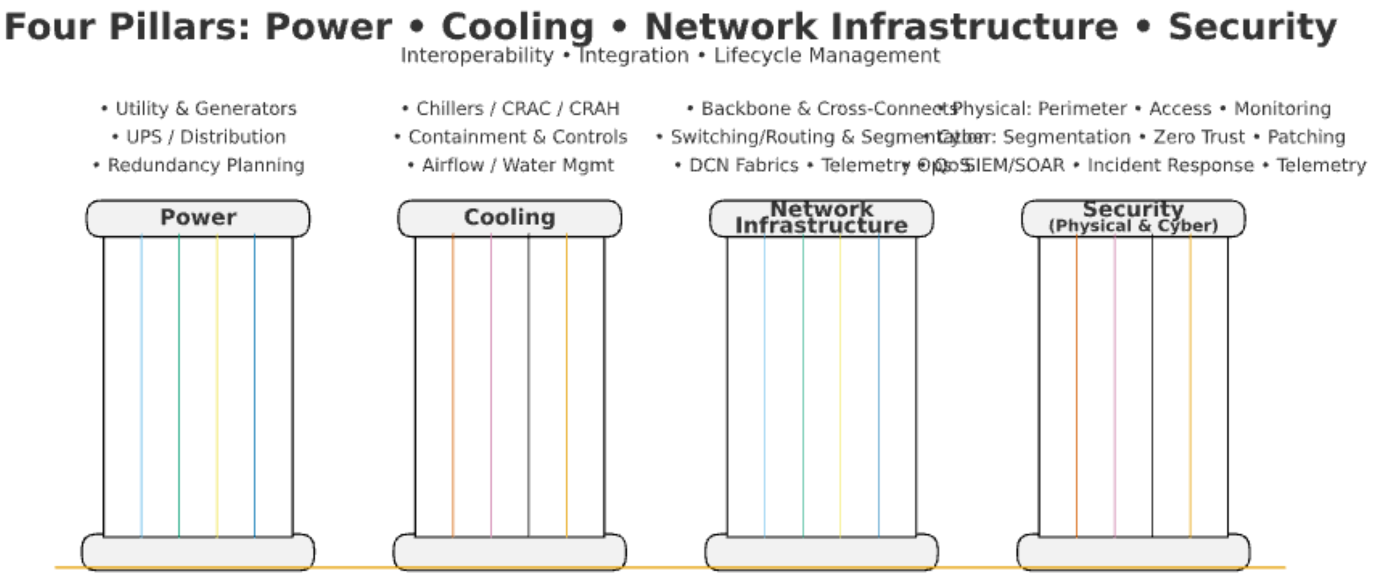
Finally, culture matters. Legacy knowledge, siloed teams and ad-hoc communication slow progress. Roundtables, joint design reviews and shared post-incident learning between end users, integrators and manufacturers raise the floor for everyone—even among competitors. In a market where the consequences of failure are shared, collaboration is not altruism—it it is risk management.

"Adaptive models will only succeed if they align with compliance and governance frameworks—and if teams share lessons rather than guard silos."

Conclusion

Physical security is now inseparable from resilience, trust and competitive differentiation in the data center market. The costs of treating it as an afterthought far outweigh the investment required to embed it early and manage it as a life cycle program.

Manufacturers and integrators should deliver interoperable, API-first solutions, prove scale readiness and structure themselves around global accounts with regional execution. Operators should integrate security into design from day one, govern with standards that enable multiple delivery partners and align construction phasing with security risk. Together, stakeholders can transform physical security from a compliance checkbox into a business enabler—supporting the speed, scale and reliability that the next decade of digital growth will demand.


Four Pillars: Power • Cooling • Network Infrastructure • Security
Interoperability • Integration • Lifecycle Management
• Utility & Generators
• UPS / Distribution
• Redundancy Planning
• Chillers / CRAC / CRAH
• Containment & Controls
• Airflow / Water Mgmt
• Backbone & Cross-Connects
• Switching/Routing & Segmentation
• DCN Fabrics • Telemetry • QoS
• Physical: Perimeter • Access • Monitoring
• Cyber: Segmentation • Zero Trust • Patching
• Ops: SIEM/SOAR • Incident Response • Telemetry
Power
Cooling
Network Infrastructure
Security (Physical & Cyber)

All four pillars must be architected together to meet availability, performance, and risk targets.

PRODUCED WITH SUPPORT FROM

MOTOROLA SOLUTIONS

PAVION™ CONNECT AND PROTECT

PLUGOUT

SIA SECURITY INDUSTRY ASSOCIATION

securityindustry.org