SJA SECURITY JOURNAL AMERICAS

Issue 47 | April 2026
SecurityJournalAmericas.com

Information, Analysis and Insights for Manufacturers, Installers and Senior Security Professionals

PLUS

**Utilities**

**Data** Centers

**Security** Screening

**Special** Report

**SCHOOL & CAMPUS SECURITY**

*Produced in partnership with Allegion* *p39*

SALIENT™

**Head to Head** Exclusive

# OPERATIONAL *intelligence*

*p12*

**Stacey Steiger, Vice President of Product and Marketing, Salient Systems explores how AI is the diagnostic, predictive and informative solution of tomorrow**

# Cyber is hardened - physical is next

**Data center security must evolve beyond the network, says Nikki Williams, North American Regional Marketing Manager at ICT with insights from Sarah Thompson, ICT, Teresa Wu, IDEMIA Public Security and Ceres Silva, IDEMIA**

For the past decade, data centers have aggressively strengthened their cybersecurity. Zero Trust architectures, AI-driven threat detection, micro-segmentation and advanced monitoring have become standard in enterprise environments.

However, while digital infrastructure has matured, many data centers still rely on perimeter-based physical security models that assume trust once someone is inside the facility. In today's threat landscape, that assumption is increasingly risky.

Identity compromise remains one of the most common paths attackers use to gain initial access. Once credentials are stolen, shared or misused, traditional perimeter defenses offer little protection, whether in a network or inside a building. The reality is simple: if identity is the primary attack digitally, it must be treated as the primary control point physically.

## The expanding threat landscape

Modern data centers face simultaneous risks from multiple directions:

- Physical threats such as unauthorized access, sabotage, insider compromise and theft of equipment
- Cyber-threats including DDoS attacks, ransomware and malware
- Environmental hazards like power outages, equipment failures and natural disasters
- Legal and compliance exposure resulting from breaches and operational failures

According to IBM's Cost of a Data Breach Report, the global average cost of a breach exceeds $4 million, a figure that reflects direct and indirect impacts including downtime, breach response and customer churn.

> **"While digital infrastructure has matured, many data centers still rely on perimeter-based physical security models."**

Uptime pressures continue to escalate as data centers operate under strict availability expectations and service-level commitments. Even brief disruptions can have outsized operational, financial and reputational consequences.

Any one of these risks can lead to downtime, data loss, regulatory penalties and erosion of trust.

As a result, security integrators are no longer simply deploying doors and cameras. They are designing layered security environments that must withstand both internal and external threats while preserving continuous operations, auditability and resilience.

## Security architecture for data centers

Truly securing a data center today requires an integrated strategy with three coordinated domains:

**Physical security:** Physical security measures ensure that only authorized personnel can gain access to the data center. This includes biometric authentication, key card readers and multi-factor authentication (MFA) to verify identity at every meaningful boundary

As Zero Trust adoption accelerates digitally, physical access must meet the same standard: no implicit trust, continuous verification and role-based authorization

**Network and data security:** Network security acts as a fortress, employing multiple layers of defense to protect against cyber-threats. Data security focuses on maintaining the confidentiality, integrity and availability of the data in the facility

**Operational security:** Operational security encompasses the procedures and policies that ensure the secure operation of the data center, from regular security audits to disaster recovery planning and incident response

Without strong operational governance, even the best technology falls short.

Together, these three pillars create a cohesive defense strategy. But to align with Zero Trust principles, physical security must now operate with the same rigor as network security.

## A unified approach

If cyber teams apply "never trust, always verify" to networks, physical security must follow suit. That means moving beyond basic badge access and implementing layered controls that continuously validate identity and intent.

"Security in a data center can't operate in silos," said Sarah Thompson, Chief Product Officer at ICT. "The organizations that are best positioned for today's threat landscape are the ones that unify access control, monitoring and operational workflows into a single architecture where identity, events and policy are continuously connected."

> **"Security integrators are no longer simply deploying doors and cameras. They are designing layered security environments."**

For security integrators, this shift requires designing data center environments with multiple coordinated layers of protection. When these systems are brought together through a full-stack security platform delivering a single pane of glass to operators, organizations gain the visibility and control needed to enforce identity-driven security policies across the entire facility.

**Perimeter security: the first trust boundary**

A secure perimeter remains the first line of defense. Measures such as fencing, controlled access gates,

lighting and surveillance cameras deter unauthorized entry.

Modern systems should also include: intrusion detection; real-time perimeter breach alerts; and integrated monitoring for rapid response.

An effective perimeter doesn't just delay attackers, it creates immediate visibility into threats before they move deeper into the facility.

**Advanced access control systems: identity at every door**

Access control is no longer about opening doors. It's about enforcing identity-based authorization aligned with role and risk.

Modern data center access control must support: door interlocking to prevent tailgating into restricted zones; door lockdown functionality to secure individual doors or entire facilities during emergencies; integrated biometric authentication (fingerprint or facial recognition); key card readers and mobile credentials; multi-factor authentication (MFA); and flexible, role-based access policies.

"In data center environments, biometric authentication helps address insider risk and credential sharing by tying physical access directly to a person's unique biological traits rather than transferable credentials like cards or PINs," said Teresa Wu, Vice President of Smart Credentials and Smart Integrate at IDEMIA.

"When biometrics are incorporated into multi-factor authentication, organizations gain stronger identity assurance at the physical layer. Every access event is tied to a verified individual, creating clear audit trails and reducing the likelihood of insider-facilitated breaches."

Advances in biometric performance are also expanding how these technologies are deployed in high-security environments. According to Ceres Silva, Solutions Sales Director at IDEMIA, improvements in facial recognition accuracy and system reliability are increasing confidence in biometric-based access control for critical infrastructure.

"As biometric technology continues to mature, some highly sensitive facilities are beginning to rely more heavily on facial recognition as part of their access strategy," Silva said. "At the same time, combining biometrics with other authentication methods, such as PINs, access cards or additional biometric modalities, creates a layered defense that significantly reduces the risk of unauthorized access."

> "Protecting environmental stability is increasingly critical to uptime and service delivery."

**Surveillance and continuous monitoring**

Continuous monitoring is critical for both deterrence and investigation. Integrated surveillance systems should provide: real-time monitoring of sensitive zones; detailed logging of access events; and video retention for post-incident analysis. When access control and video systems are unified, forensic investigations become faster and more accurate, strengthening compliance and resilience.

**Environmental controls: protecting uptime**

Data centers rely on stable environmental conditions. Modern security platforms increasingly integrate with building automation systems to monitor and manage: temperature and humidity; fire detection and suppression; and ventilation and cooling infrastructure.

With the growing prevalence of high-density computing and AI workloads, protecting environmental stability is increasingly critical to uptime and service delivery.

**Redundancy and resilience: designing for failure**

Downtime is costly. Physical security systems must remain operational even during power failures or maintenance events.

Effective solutions support: backup power systems to maintain access control functionality during outages; parallel access systems to ensure seamless operation during upgrades; and automated server failover to replicate security data in real time across redundant hardware, eliminating single points of failure.

## Why this matters

The conversation has shifted. Integrators who can design environments that unify physical, network and operational security are no longer installers. They are trusted advisors shaping resilience. The next generation of resilient data centers will not treat physical and digital risks separately. They will design trust across every layer. ■

This column was created in collaboration with the Security Industry Association (SIA) Women in Security Forum IlluminateHER Subcommittee, to help elevate the voices in the security industry.