Reprinted story from Data Center Dynamics (March 27, 2025)

Hanwha Vision

Data Center

Security: The Primary Stakeholder, But Not The Only One

How cross-departmental collaboration strengthens surveillance, eliminating blind spots and ensuring data centers don't become fortresses with open doors.

For data center owners and operators, technology is, naturally, the most significant investment they make. As artificial intelligence (AI) becomes increasingly valuable for day-to-day activities, these tech investments become increasingly sophisticated and complex, making security an even greater priority for the industry, and a key focus for Hanwha Vision.

As a global leader in visual solutions, Hanwha Vision is a trusted partner for data center operators worldwide.

Allen DiGerolami, business development manager for video surveillance in data centers at Hanwha Vision America, brings his expertise to ensure robust security across the industry.

Devising a data center security plan

Data center security is complex. Numerous factors feed into the feasibility of surveillance systems used, some directly in an operator's control and others beyond it. Despite the growing focus on cybersecurity, physical security measures have sometimes been overlooked. However, recent industry trends and regulatory changes have pushed operators to rethink their approach.

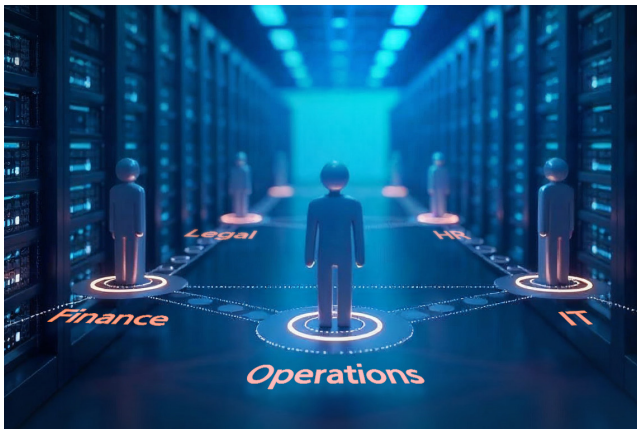
When designing a data center, architects and engineers must also consider the needs of the anchor tenant, as facilities are typically built to accommodate what tenants are willing to invest in. This means security measures often vary depending on the tenant's risk tolerance and budget.

For multi-tenant and colocation data centers, service-level agreements (SLAs) ensure clarity on security measures and responsibilities. With multiple clients sharing space, colocation facilities must provide both visibility and security without compromising tenant privacy. From a network perspective, increasing the number of cameras can also overload infrastructure, making latency a pivotal concern for mission-critical operations.

Beyond operational needs, compliance requirements dictate many security decisions, influencing both infrastructure investments and customer selection. DiGerolami explains:

> "For example, the National Defense Authorization Act (NDAA) and Department of Defense (DoD) regulations mandate perimeter fencing for government contracts. Additionally, large corporations often request advanced security measures such as Light Detection and Ranging (LiDAR) and infrared cameras outside the perimeter, adding extra layers of protection before an intruder even reaches the fence."

Cross-departmental collaboration



As data centers work to implement fully protective yet cost-effective security measures, interdepartmental collaboration plays an important role in the successful deployment of surveillance systems. Teams such as legal and HR, finance, operations, and IT must coordinate to ensure that blind spots are identified and addressed, avoiding gaps that can leave data centers vulnerable.

While industry security standards exist, they act as guidelines rather than strict instructions, making knowledge-sharing crucial. Simply choosing the cheapest camera and deploying it "as is" isn't realistic - systems must comply with local regulations, avoid spyware risks, and meet certification standards.

Naturally, security departments lead risk mitigation efforts, but failure to align with other key departments can create challenges in compliance, ethics, and operations.

Legal and HR: Addressing compliance and ethics in surveillance

With the rise of advanced surveillance technologies, legal and HR teams play an increasingly vital role in shaping policies around facial recognition, biometric data use, and inclusive video labelling (e.g., race, gender, and distinguishing characteristics.) Their involvement ensures that privacy regulations, ethical concerns, and employee rights are fully considered before deploying surveillance solutions.

Operations: AI-driven video surveillance

While on-site security guards manage physical access control, their ability to detect and intervene in real time is often limited. Security breaches aren't always dramatic events like a drone attack or a vehicle ramming a gate. Rather, the more subtle threats, such as missing equipment or unauthorized movement within the facility, require continuous monitoring.

To meet SLAs and proactively mitigate risks, AI-powered cameras can supplement traditionally manned surveillance systems and physical human security. These AI-powered cameras can help by filtering out background noise and focusing on specific individuals or vehicles. DiGerolami says:

> "For example, in Northern Virginia or Canada, a perimeter camera's motion sensor is going to trigger every time a tree sways, overloading bandwidth and generating false alerts. With AI, you can train the system to ignore environmental movements and track only people or vehicles."

IT: AI integrations in security systems

Integrating AI into data center security shifts the focus from reactive responsive to proactive threat prevention. Through APIs, all security elements - including door swipes, biometric scanners, palm readers, and fingerprint readers - should function in sync with cameras as sensors. DiGerolami says:

> "With API integration, cameras can activate only when a door is swiped by an authorized pass."

However, not all high-tech solutions are universally compatible-mismatched technologies can lead to delays, inefficiencies, and integration issues.

Industry trends in surveillance

As demand for power soars and resources dwindle amid the climate crisis and sustainability mandates, data center operators face tightening investment constraints. Departments involved in security are being tasked with streamlining and improving efficiency, driving innovation in surveillance strategies and infrastructure.

In Northern Virginia, for example, DiGerolami has observed a growing trend toward multi-story data centers rather than the traditional horizontal expansion. This shift reflects the industry's need to maximize space and operational efficiency in high-demand regions where land is occupied and costly.

At the same time, regulatory changes are evolving at an accelerated pace, with decisions on critical issues, such as drone mitigation, now reaching Congress for review. These rapid developments are pushing data center operators to stay ahead of compliance requirements while enhancing security measures.

> "As of last year, it's been estimated that 50 percent of data centers had perimeter fencing, and of those, approximately 10 percent or less had an active fence line, DiGerolami explains.
>
> However, Digerolami notes,"that the industry is shifting toward actively monitored fence lines to enhance perimeter security."

Hanwha Vision is at the forefront of this transformation, with DiGerolami emphasizing the importance of a holistic approach:

> "Hanwha Vision integrates with all active fence lines and collaborates with partners on entryways, doors, and access points. My involvement goes beyond cameras - it's about delivering a full security solution rather than just a product. By building a team that brings all security components together, we significantly increase the chances of success."

Inside the data center itself, operators have been testing facial recognition technologies where permitted by civil codes and state regulations.
One promising approach involves using 360° fisheye cameras positioned in data center aisles that activate only when a designated security line is crossed.

This concept extends to an "intelligent handoff" system, where cameras act as sensors, tracking specific individuals as they move across the facility. In turn, this eliminates unnecessary distractions, such as flashing server lights, and enhances real-time security monitoring. DiGerolami adds:

> "You can even install microdomes or hidden cameras inside specific areas or racks to track access - who opens which doors, what technicians are doing, and any unauthorized changes."

These AI-enabled tracking capabilities make it easier for data center operators to retrieve footage, analyze incidents, and intervene much more quickly and easily.

DiGerolami highlights Hanwha Vision's bi-spectrum thermal camera, which features dual-channel surveillance-combining optical and thermal imaging. This hybrid approach improves visibility in low-light conditions, providing an added layer of security for data centers operating 24/7 in diverse environments.

> "The goal is to create a fully unified environment where nothing slips through the cracks, he explains. If an incident does occur, the security system ensures the breach is tracked through every layer of protection within the data center."

4K AI camera

Thermal AI camera

Conclusion

While AI-enabled equipment requires a significant initial investment, it ultimately allows operators to do more with less-enhancing security, optimizing resources, and reducing reliance on extensive hardware.

However, the success of these systems depends not only on the technology itself but also on cross-departmental collaboration. Security, IT, legal, and operations teams must work together to ensure compliance, maximize system effectiveness, and create a resilient security framework.

Expand your knowledge >

Hanwha Vision