SECURITHINGS

2026 ISC West Customer Roundtable Recap

We brought over 50 industry leaders from Physical Security together to discuss trends, focus areas, opportunities and challenges. What follows is a summary of what they shared with each other.

Each year at ISC West, SecuriThings convenes its annual Customer Roundtable—bringing together dozens of physical security leaders from some of the world's most complex and highly regulated environments. This year, approximately 50 practitioners gathered to share candid perspectives on what's working, what continues to challenge teams, and where the industry is headed next. The level of leadership represented is notable, with physical security leaders from companies totaling over $2.5 trillion in annual revenue.

What emerged from the discussion was not a collection of isolated anecdotes, but a remarkably consistent narrative. Across industries and geographies, physical security teams are undergoing the same fundamental transformation: moving away from manual, reactive operations toward automated, IT-aligned, and increasingly AI-driven models. The conversations made clear that this shift is no longer theoretical—it is actively underway, and in many cases, already delivering measurable results.

The Breaking Point of Manual Operations

A dominant theme throughout the roundtable was the growing impossibility of managing modern physical security environments using legacy, manual processes.

Many organizations described sprawling device fleets—tens of thousands of cameras and access control systems—paired with mounting pressure from cybersecurity teams to remediate vulnerabilities quickly. In these environments, traditional approaches simply cannot keep pace. Routine tasks like credential rotations, firmware updates, and configuration changes often take weeks or even months when handled manually.

> ***"For the sixty percent of devices we've automated, cybersecurity remediation takes us sixty minutes. The other forty percent of devices takes us forty five to sixty days."***

The gap between manual and automated operations has become impossible to ignore. Where automation is in place, remediation timelines shrink dramatically—from months to hours. Where it is not, organizations remain stuck in extended cycles of exposure, unable to keep up with the pace of risk.

The consensus was clear: automation is no longer a forward-looking aspiration. It is a baseline requirement for operating at scale.

Physical Security Resembling an IT Function

Closely tied to the rise of automation is a broader organizational shift: the integration of physical security into the IT domain.

Roundtable participants repeatedly emphasized the benefits of treating physical security infrastructure—cameras, readers, and associated systems—as IT-managed assets. This shift brings with it established best practices around governance, accountability, and tooling. It also introduces a level of operational rigor that has historically been absent in many physical security programs.

One of the most impactful changes has been the move from periodic, audit-driven security models to continuous, real-time operations. Instead of identifying issues once or twice a year, organizations now have the ability to detect and remediate vulnerabilities as they arise. This "always-on" approach fundamentally changes the security posture, enabling teams to move from reactive to proactive.

Equally important, aligning with IT helps resolve long-standing ambiguity around ownership. Physical security, cybersecurity, and IT teams have traditionally operated in silos, often leading to confusion and finger-pointing. With shared platforms and unified data, those boundaries are beginning to dissolve, replaced by a more collaborative and accountable operating model.

Visibility: The Foundation for Everything Else

If automation and IT alignment are the pillars of modern security operations, visibility is the foundation they rest on.

A striking number of participants acknowledged that, until recently, they lacked a complete and accurate picture of their own environments. Device inventories were often maintained in spreadsheets that quickly became outdated. In some cases, organizations discovered that their actual device counts were significantly higher than expected. In others, devices had gone years without updates simply because they were not being tracked.

This lack of visibility creates cascading challenges. Without an accurate inventory, it is nearly impossible to assess risk, prioritize remediation, or measure compliance. Conversely, once centralized visibility is established, organizations gain a powerful new capability: the ability to operate with real-time awareness.

Teams can walk into a site with up-to-date information on device status, identify issues before they escalate, and hold stakeholders accountable with data rather than assumptions. In many ways, visibility is the inflection point—once achieved, it unlocks everything that follows.

"We had a mile long spreadsheet... and it was not highly accurate... I couldn't trust the information that was on there."

Automation as a Force Multiplier

As organizations build on that foundation, automation is emerging as the primary driver of scale. Rather than expanding headcount to keep up with growing device fleets, many teams are using automation to extend their reach. Routine tasks are increasingly handled by systems that can operate continuously and consistently, freeing human operators to focus on higher-value activities.

This shift is also changing the skill profile of physical security teams. Instead of relying solely on specialized expertise, organizations are enabling broader groups of employees to interact with systems using simplified workflows and, increasingly, natural language interfaces. Tasks that once required deep technical knowledge can now be executed by more junior staff, reducing reliance on external consultants and lowering operational costs.

At the same time, participants emphasized that automation does not eliminate the need for human oversight. If anything, it elevates it. Defining parameters, managing exceptions, and ensuring systems behave as intended are becoming core competencies. The model is not human versus machine, but human plus machine—each playing a distinct and complementary role.

A More Sophisticated Approach to Compliance

The implications of automation extend directly into how organizations think about compliance and risk management.

Historically, compliance has been treated as a periodic checkpoint—something to be measured and addressed at specific intervals. The roundtable made clear that this model is rapidly being replaced by continuous compliance, where systems are constantly monitored and remediated.

This shift has led to significant improvements in compliance rates, with some organizations moving from partial coverage to near-complete adherence without increasing headcount. However, the conversation also highlighted the importance of nuance.

Not all systems are equal, and not all processes should be fully automated. In highly sensitive environments, particularly those involving industrial controls, many teams are intentionally maintaining manual oversight to avoid unintended disruptions. This reflects a more mature, risk-based approach—automating where it drives clear value, while preserving control where the stakes are highest.

Breaking Down the Physical-Digital Divide

Another recurring theme was the breakdown of traditional silos between physical and digital security.

As threats become more sophisticated, the distinction between cyber and physical risk is increasingly irrelevant. Organizations are responding by adopting unified security strategies that integrate data, tools, and workflows across domains.

In practice, this often means leveraging existing enterprise systems rather than building isolated solutions. Ticketing platforms, identity management systems, and cybersecurity tools are being extended to include physical security use cases. At the same time, shared dashboards and "single pane of glass" views are giving multiple stakeholders access to the same underlying data.

The result is not just improved security outcomes, but a more cohesive organization—one where teams are aligned around common goals rather than operating in parallel.

"We're not just a cost center anymore . . . so the question we're asking ourselves is how do we enable the business, do more with the infrastructure."

Security as a Driver of Business Value

Perhaps the most significant mindset shift discussed at the roundtable was the evolving role of physical security within the business.

No longer confined to a purely protective function, security is increasingly being recognized as a source of operational insight and competitive advantage. The same systems that monitor facilities for safety can also generate valuable data about how those facilities are used.

Participants shared examples ranging from optimizing the flow of people through physical spaces to improving logistics operations and identifying inefficiencies. In each case, security infrastructure becomes a sensor network—capturing data that can inform decisions far beyond traditional security use cases.

This evolution has important implications. As security becomes more tightly linked to business outcomes, investments in reliability, uptime, and data quality take on new significance. Security is no longer just about preventing loss; it is about enabling performance.

The Road Ahead: AI and the Simplification of Complexity

Looking forward, the group expressed strong alignment around the role of AI—particularly agentic AI—in shaping the next phase of this transformation.

The promise is twofold. First, AI has the potential to simplify the inherent complexity of modern security environments, allowing users to interact with systems using natural language and automate increasingly sophisticated workflows. Second, it opens the door to more advanced analytics, including anomaly detection and predictive insights.

Early use cases are already emerging, from identifying underperforming devices to uncovering patterns that would be difficult for humans to detect at scale. Over time, these capabilities are expected to further elevate the role of physical security, enabling teams to move beyond operations and into strategic decision-making.

"Agentic security is a non negotiable... we need to leverage AI... to automate and autonomously update and secure our systems."

A Defining Moment for the Industry

Taken together, the insights from this year's SecuriThings Customer Roundtable point to a defining moment for the physical security industry.

The transition to automated, IT-aligned, and data-driven operations is no longer optional—it is inevitable. Organizations that embrace this shift are not only improving their security posture, but also unlocking new efficiencies and sources of value. Those that do not risk falling further behind, constrained by processes that cannot scale to meet modern demands.

Perhaps most importantly, the conversation highlighted a broader redefinition of what physical security can be. No longer operating in the background, it is emerging as a strategic function—one that sits at the intersection of safety, technology, and business performance.

And if the voices in that room are any indication, this transformation is only just beginning.

About SecuriThings

SecuriThings is the leading provider of physical security device management and remediation that supports enterprise-level compliance and operational requirements. Built for scale and the diversity of modern environments, SecuriThings provides continuous control across device types and locations, bridging the gap between IT management expectations and traditional manual or siloed technologies in physical security.

By making uptime, security and compliance part of everyday operations, SecuriThings has become the trusted platform of large organizations including for dozens of Fortune 500 companies across multiple industries.