SECURITY MEGATRENDS™ 2026

THE ANNUAL VISION FOR THE SECURITY INDUSTRY

SECURITY INDUSTRY ASSOCIATION

SNG™

SECURINGNEWGROUND®

THE BUSINESS OF SECURITY

SAVE THE DATE

OCTOBER 20-21, 2026 | NYC

SIA
SECURITY INDUSTRY ASSOCIATION

THANK YOU

SIA THANKS ITS 2025 SNG SPONSORS

Genetec™

ALLEGION

ASSA ABLOY

AXIS COMMUNICATIONS

cento SEARCH | FIRE & SECURITY

convergint

dormakaba

EAGLE EYE NETWORKS

EGIS CAPITAL PARTNERS

Genea

Hanwha Vision

HID

Honeywell

Houlihan Lokey

IDIS One Solution. One Company.

Imperial Capital

i-PRO

ISC

LVT

M.C. DEAN BUILDING INTELLIGENCE

milestone

MOTOROLA SOLUTIONS

RAYMOND JAMES

SAGE integration

UNLIMITED TECHNOLOGY

VERKADA

VIVOTEK A Delta Group Company

wachter

wesco

Media Partners:

SDM

SECURITY BUSINESS

securityinformed.com

SJA SECURITY JOURNAL AMERICAS

Security Sales & Integration

SECURITY SYSTEMS NEWS

sourceSecurity.com

©2025, Security Industry Association. All rights reserved.

SECURITY 2026
MEGATRENDS™

HOW WE DEFINED AND RESEARCHED THE 2026 SIA SECURITY MEGATRENDS

Each year at Securing New Ground (SNG), senior-level industry leaders and financial partners gather, trends are discussed, connections are formed and ideas are shared openly. In advance of SNG, as part of our annual membership survey, SIA asked hundreds of executives from SIA member companies what factors were shaping their business decisions and what trends they were watching. We then spoke with numerous SIA members, along with current and recent speakers and attendees of SNG, about which previous trends were still relevant, which trends were no longer as impactful to the industry and which trends could be identified to be added to our report.

Securing New Ground, our annual executive conference, serves as the rallying point for the Security Megatrends project.

In advance of the event, numerous discussions are held with core advisors about the trends, which remain relevant, what has changed and what new trends are affecting the industry's direction. This group of SIA Security Megatrends advisors provides hours of focused feedback on the megatrends via in-depth conversations and collaborative editing. The value of insights from these leaders and luminaries cannot be overstated (thank you, Steve Van Till, Tara Dunning, Eric Yunag and Devin Love). I also want to thank so many individual SIA members who I engaged with on conversations about trends in their sector that aligned directly with Security Megatrends under consideration. In that area, I want to thank Ken Francis, CEO of Actuate, and the entire SIA Executive Advisory Board (EAB) that he chairs. This group's reports on integrator trends and industry expansion are valuable additional reading. I'd also like to thank EAB member Scott Elkins of Zeus Fire & Security for his perspective.

In addition to the member survey research and the focused conversations, the selection of these trends relies on the speakers, panel and audience members of SNG, because the conference is the ultimate proving ground for deep-dive discussions on what we can do as an industry to pave a successful future. A special session during the 2026 SNG conference from Steve, Tara, Devin and Eric provided additional feedback related to the Security Megatrends and helped generate key trends in this report. Lastly, as we authored this report, we tried to reflect not only the vendor/integrator/service provider side of the industry, but also reflections on how each trend may impact the security practitioner or CSO.

Geoff Kohl
Editor, 2026 Security Megatrends report
Sr. Director of Marketing, SIA

SCOTT DUNN
SIA Chair of the Board

Megatrends Advisors

TARA DUNNING
Vice President, Converging Technology, Wescoo

DEVIN LOVE
Vice President, Global Software Platforms, Allegion

STEVE VAN TILL
President and CEO, Brivo

ERIC YUNAG
EVP, Products and Services, Convergint

STAFF

DON ERICKSON
SIA CEO
derickson@securityindustry.org

GEOFF KOHL
SIA Senior Director of Marketing
Author and Editor, 2026 SECURITY MEGATRENDS Report
gkohl@securityindustry.org

KARA KLEIN
Associate Director of Marketing and Media Relations
kklein@securityindustry.org

KEVIN MURPHY
SIA Senior Director of Member Services
kmurphy@securityindustry.org

Copyright 2025 Security Industry Association. Reproduction prohibited without prior permission.

Security Industry Association
8455 Colesville Road
Suite 1200
Silver Spring, MD 20910
Main: 301-804-4700
Fax: 301-804-4701
securityindustry.org

SIA
SECURITY INDUSTRY ASSOCIATION

SNG™
SECURING NEW GROUND®

Building a Better Future—Together!

Thank you for engaging with this year's Security Megatrends report. We are proud to produce this report as a benefit for all Security Industry Association members and as a resource to help guide the security industry at large. These insights are designed to inform, inspire, and prepare us for the opportunities and challenges ahead.

Among the trends shaping our future, the shift from the traditional channel model to the value chain (Megatrend 3 in this year's list) is the most transformative. The channel was built for transactions; the value chain is built for collaboration and outcomes. When our industry aligns around the needs and outcomes of the end-user security practitioner, every stakeholder thrives—manufacturers, integrators, service providers, and practitioners alike. This evolution ensures security is not just delivered—it is co-created, driving resilience, innovation, and shared success.

Together, we will build a future where security delivers measurable business value and empowers every professional to excel. The future is bright—and built together.

Sincerely,
Scott Dunn
Chair, SIA Board of Directors

SECURITY 2026 MEGATRENDS™

©2025, Security Industry Association. All rights reserved.

FOUNDATIONAL TRENDS

These trends, some previously long recognized as Security Megatrends, are now so much part of the fabric of the world that they are viewed no longer as future-looking megatrends, but instead as common concerns that all business leaders must manage as they operate within the security industry.

ARTIFICIAL INTELLIGENCE

CYBERSECURITY

GLOBAL TENSIONS

CLOUD MODEL FOR TECHNOLOGY DELIVERY

CHANGING ECONOMIC CONDITIONS

SUPPLY CHAIN ASSURANCE

SUSTAINABILITY

WORKFORCE DEVELOPMENT

EXECUTIVE TAKEAWAYS

FROM SNG

"Right now in security, data is a whole new business emerging on top of the 'old' business of security. The right pieces come together to deliver it as a business model. Data doesn't do anything in and of itself without getting insights out of it. Data drives opportunity, and it's a great new business model."

—**Tim Palmquist,** vice president, Americas, Milestone Systems, on how data is the new oil

"Ideally those level 1, 2, 3 alarms and incidents are being managed by the systems so we can do a better job managing bigger incidents and paying attention to critical things."

—**Sobie Velasquez,** vice president, physical security technology, Morgan Stanley, on what AI promises corporate security leaders

"The security data by itself can be valuable, but what becomes more so is when you bring it into other data from the organization or external data and be able to make decisions and do risk assessments."

—**Hans Kahler,** chief operating officer, Eagle Eye Networks, on opportunity to build new business models that leverage the value of data

"Technology for technology's sake isn't the point. We're moving to be more business enablers and advisors—taking these shiny new objects and applying them to our current products, looking at future products and being able to pace them as innovation evolves."

—**Ewa Pigna,** chief technology officer, Honeywell, on how CTOs stay focused on business

©2025, Security Industry Association. All rights reserved.

EXECUTIVE TAKEAWAYS

FROM SNG

"We're stewards of the industry and keep the customer first.
It's a customer-first perspective, which seems to now be true across the industry, not just at Convergint."

—**Ann Fandozzi,** CEO, Convergint, on how firms navigate challenging situations like tariffs so as to not pass disruption on to customers or burden them with surprise costs

"What's a problem we're trying to solve for our customer? Anchor it in a real-life use case and get the customer actively participating in the development cycle. We have technology in our titles, but focusing on just the tech is focusing on the wrong thing. Focus on the real problems customers have and how you can use technology to achieve your goals and solve those problems."

–**Christian Morin,** vice president, product engineering, Genetec

"We do the opposite of what everyone else might do. That separates us. We do the counterintuitive thing—be different in a good way."

—**Brian Sloan,** CEO, Wachter, on remaining innovative in business

"We're looking for enhancements within our existing products. We're looking for utilization of AI within our existing databases. We're looking for automation within our existing tools we already have. We don't want new tools and don't necessarily need new tools. We have enough tools. We want to hear there's a light at the end of the tunnel when it comes to the tools we have. And we need more conversation about what we're actually doing within the products we already have."

—**Bobby Louissaint,** head of technical partnership engagement, GSST, Meta, on why outcomes are more meaningful for practitioners than simply embracing new technology

"Know your customer. What's the sector? What's their size and scale? What past performance is going to be relevant and resonate? Bring the innovation and be able to think around the corner."

—**Cheryl Steele,** former chief security officer for Starbucks, on how global security solution providers can best serve security practitioners

©2025, Security Industry Association. All rights reserved.

MEGATREND 1

SOFTWARE EATS THE WORLD. WILL AI EAT SOFTWARE?

> **“If you’re not in the game of making software, you’re not going to be in the game.”**
>
> —ERIC DEAN, CHIEF TECHNOLOGY OFFICER (CTO), M.C. DEAN

The security industry has witnessed a dramatic shift over the past decade: hardware, once the dominant force, has ceded ground to software. Historically, system identity was tied to physical components—cameras, network video recorders (NVRs), access panels and readers. Today, the conversation has flipped. End users increasingly identify their systems by software brands, not hardware manufacturers. This evolution reflects a broader truth: the user experience is shaped by software interfaces, not the devices behind them.

As software gained dominance, cloud-based delivery accelerated the trend. SaaS solutions have steadily eaten into the market for on-premises platforms, driven by the need for remote access, outsourced technical support and vendor-managed updates. While adoption varies—only 7% of organizations report that 75% of their application stack is SaaS—the trajectory is clear. Newer companies lean heavily toward cloud-first strategies, and even legacy platforms are being redeveloped for hybrid or cloud-native delivery. Advances in bandwidth, compression and scalable storage have reduced friction, even for data-heavy applications like video surveillance.

Now, artificial intelligence introduces a new layer of disruption. Industry leaders call AI a “mass extinction event for software,” as agentic AI begins replicating functionality once hard-coded into applications. Headlines such as “Anthropic Says Its AI Can Clone Enterprise Apps Like Slack” underscore the potential for AI-native solutions to replace traditional software models. While tight hardware-software integration currently provides a moat for security vendors, AI will reshape workflows, automate reporting and enhance analytics. The question is no longer hypothetical: AI may not “eat” security software, but it will dramatically influence software—how soon and how deeply remains the critical debate.

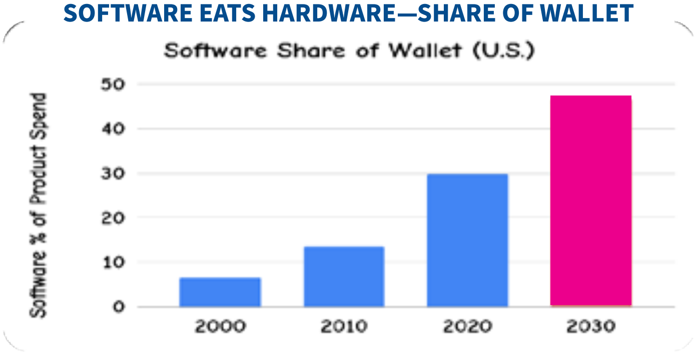
©2025, Security Industry Association. All rights reserved.

> **“AI is a mass extinction event for software.”**
>
> —BESSEMER VENTURE PARTNERS

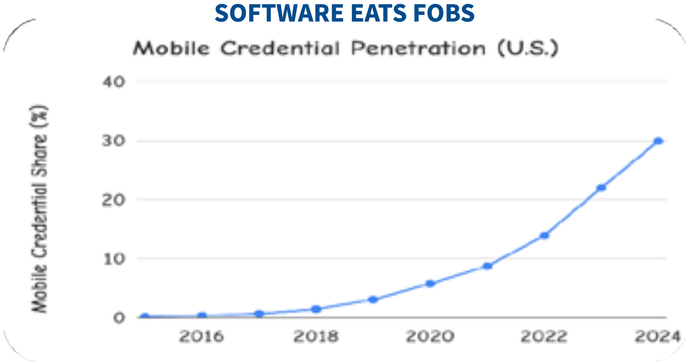
Software Startups Outpace Hardware Startups

There are nearly five times as many software startups as hardware startups—when measured across all industries. According to startup research website Startup Blink, of all startup businesses, an estimated 33% are software focused vs only 6–7% being focused on hardware. According to data shared at SNG 2025, the percentage of software startups is even higher in the security sector.

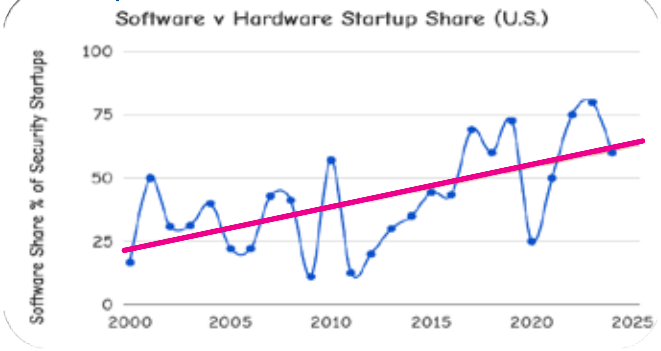
SOFTWARE EATS HARDWARE—SHARE OF WALLET



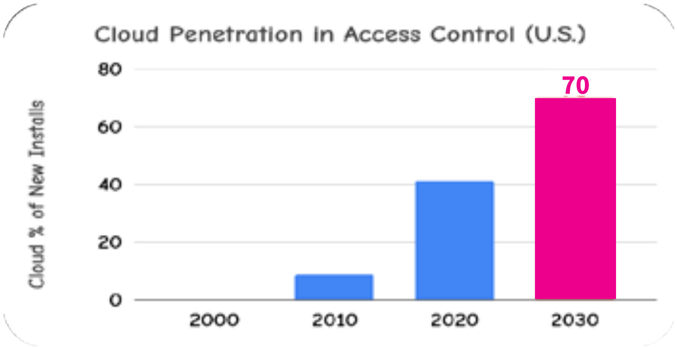
SOFTWARE EATS FOBS



STARTUPS INCREASINGLY FOCUSED ON SOFTWARE, NOT DEVICES/GADGETS ACROSS THE TECHNOLOGY MARKET



SOFTWARE MEANS CLOUD



SOURCE: Steve Van Till, SNG 2025

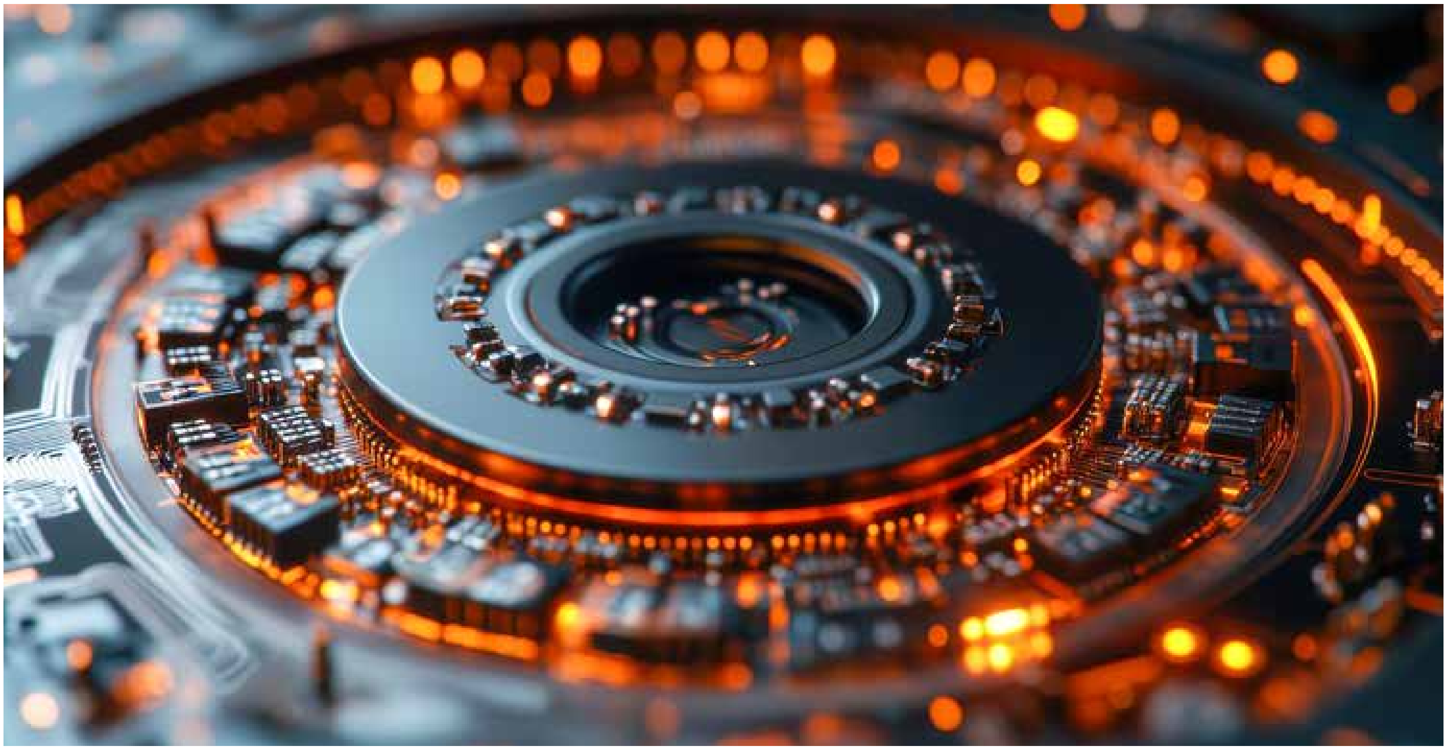
KEY TAKEAWAYS

- Software has overtaken hardware as the dominant interface in security systems.
- Cloud-based SaaS continues to erode on-premises dominance, driven by flexibility and remote access.
- AI introduces a new disruption, with agentic models replicating traditional software functionality.
- Hardware-software integration of the security industry offers protection, but AI will reshape future design.
- Opportunities exist for AI-driven automation in reporting, access reviews and video analysis.

©2025, Security Industry Association. All rights reserved.

MEGATREND 2

THE SECURITY HARDWARE LAYER IS REINVENTED



> **“Data normalization between products needs to be a standard.”**
>
> —BOBBY LOUISSAINT, HEAD OF TECHNICAL PARTNERSHIP ENGAGEMENT, GSST, META

As software and cloud solutions have dominated the security landscape, hardware providers are reinventing their role to avoid becoming commoditized peripherals. Hardware remains the lifeblood of the industry—producing the critical data that software and AI depend on to deliver value—which means hardware must evolve beyond simple sensing to become intelligent, integrated and indispensable.

Manufacturers are embedding software and AI-lite analytics directly into devices, transforming them from passive endpoints into active contributors within a system of systems. Cameras, for example, are no longer just video sensors—they now combine audio, motion detection and environmental monitoring. This multi sensor approach satisfies AI’s hunger for rich, contextual data. Standards-based architectures, open APIs and unified data models are critical to unlocking this potential, enabling interoperability and seamless integration.

The future favors hardware that delivers actionable insights, supports digital twins and interacts dynamically with buildings. Point solutions will lose relevance, while powered sensors and edge devices become essential for AI-driven security ecosystems. Ultimately, hardware’s value will be measured by its ability to feed clean, normalized data into platforms that enable automation, analytics and intelligent decision making.

©2025, Security Industry Association. All rights reserved.

“If AI is the brain, the hardware that wins is hardware that gets information across the blood-brain barrier between hardware and AI.”

—DEVIN LOVE, VICE PRESIDENT, GLOBAL SOFTWARE PLATFORMS, ALLEGION

What Hardware Requires to Elevate Its Value and Deliver Better Outcomes

Clearly defined and available hardware APIs

System of systems interaction

Standards-based architecture and data models

Data aggregated into unified platforms

Data availability delivers higher hardware value.

KEY TAKEAWAYS

- Hardware is reinventing itself with embedded software and AI-lite analytics.
- Devices must deliver rich, multi-sensor data to satisfy AI’s growing needs.
- Standards, APIs and unified data models unlock hardware’s full potential.
- Point solutions will decline; integrated systems of systems will dominate.
- Hardware’s future value lies in enabling AI-driven automation and insights.

©2025, Security Industry Association. All rights reserved.

MEGATREND 3

SECURITY SOLUTIONS LOSE THEIR BOUNDARIES

Security is no longer confined to physical protection—it is expanding into a holistic ecosystem that integrates building systems, IT infrastructure and operational technologies. This megatrend, highlighted at SNG 2025 as "Expanding the Boundaries of Security Solutions," reflects a shift from traditional video surveillance toward visual intelligence and enterprise-wide value creation.

Buyers now seek multi-use technologies that deliver operational insights alongside security benefits. This convergence spans software, cameras, sensors, access control, fire safety, HVAC, lighting and utilities—creating unified platforms that enable intelligent control across cyber and physical domains.

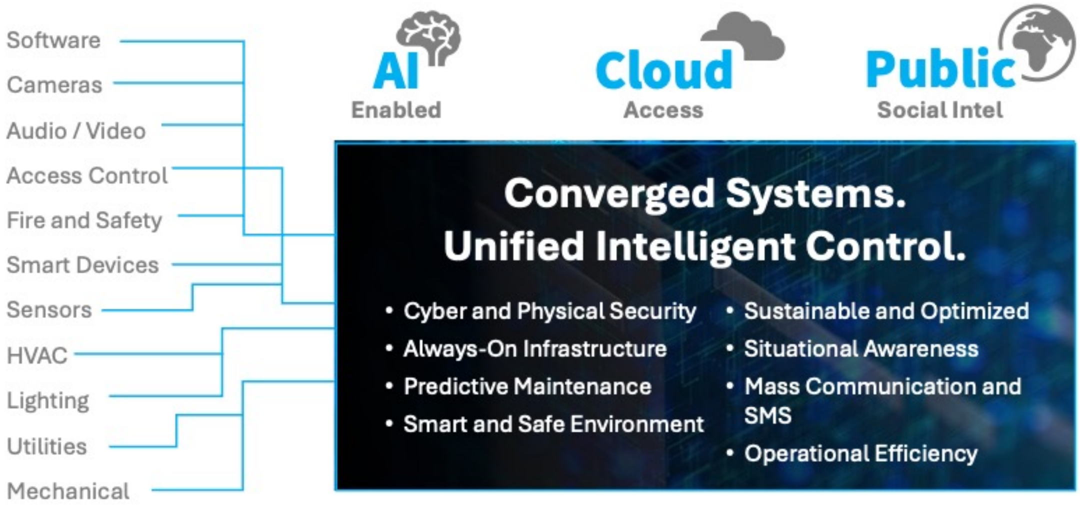
The benefits are transformative: predictive maintenance, situational awareness, mass communication, operational efficiency and sustainability. Real-world examples include integrated responses in data centers, where cameras validate alerts from environmental sensors, and campus environments where AV systems, lighting and access control collaborate for emergency response. These integrations redefine security's role, positioning it as a driver of resilience and efficiency.

Organizational structures are evolving too. Some firms consolidate building and security technologies under one group, while others create tech-focused teams within security departments to unlock added value. The boundaries of security are dissolving—and with them, the perception of security as a siloed function.

> **"Our industry's boundaries are rapidly vanishing. Convergence across all technology stacks allows us to provide unified insights and control across the business ecosystem, which leads to safer, more efficient, more sustainable and more resilient enterprises."**
>
> —TARA DUNNING, VICE PRESIDENT, CONVERGING TECHNOLOGY, WESCO

©2025, Security Industry Association. All rights reserved.

The Converged Enterprise Technology Stack



Software
Cameras
Audio / Video
Access Control
Fire and Safety
Smart Devices
Sensors
HVAC
Lighting
Utilities
Mechanical

AI Enabled

Cloud Access

Public Social Intel

Converged Systems.
Unified Intelligent Control.

- Cyber and Physical Security
- Always-On Infrastructure
- Predictive Maintenance
- Smart and Safe Environment
- Sustainable and Optimized
- Situational Awareness
- Mass Communication and SMS
- Operational Efficiency

Real-World Example:
Securing the Critical Infrastructure of Data Centers and Network Closets

- Sensors plus cameras enable rapid validation of alerts and rapid response
- Lighting, alerting and access controls can work together to mitigate immediate risks
- ecurity and operational data combine for enhanced fault detection and diagnostics
- Cabinet-open alert validated by camera feed
- Environmental sensors (temperature, humidity) tied to security alerts
- Enabling faster fault detection and diagnostics
- Remote access and lockdown capabilities

Real-World Example:
Safety and Efficiency at Scale in Campus Environments
(Education, Corporate, Health Care)

- AV, public address and access control systems can provide multilayered response
- Sound masking systems deactivate during emergency notifications
- Lighting systems can illuminate unauthorized occupants
- scenario: Perimeter security integrated with AV and public address
- Threats trigger automated alerts and building lockdown
- Enabling real-time collaboration and safety messaging
- Provides context and information in situations like crowd control or emergency response

KEY TAKEAWAYS

- Security solutions now span building, IT and operational systems.
- Buyers demand multi-use technologies delivering enterprise-wide value.
- Convergence enables predictive maintenance, situational awareness and efficiency.
- Integrated responses improve safety in critical infrastructure and campus environments.
- Security teams are reorganizing to manage tech-driven ecosystems.

©2025, Security Industry Association. All rights reserved.

MEGATREND 4

THE VALUE CHAIN REPLACES THE CHANNEL MODEL

The traditional channel model in the security industry was built on a linear path: manufacturers produced products, distributors handled logistics, integrators installed and maintained systems and practitioners used them. This structure prioritized efficiency in moving products to market but often created friction when roles overlapped—such as manufacturers selling directly to end users.

Today, that model is being replaced by the Value Chain, a framework that centers on customer outcomes rather than product delivery. Instead of pushing products through a pipeline, the value chain aligns hardware, software, AI/data, services and operations around solving end-user challenges. This shift transforms the industry from transactional to collaborative, where success is measured by resilience, integration and business impact rather than unit sales.

In the value chain, "sell-through becomes build-with"—manufacturers, integrators and service providers work together to co-create solutions tailored to enterprise needs. Efficiency gives way to adaptability, and competition evolves into partnership. For security leaders, this means vendors must deliver holistic solutions that integrate physical security with IT, operations and business objectives. The result is a more dynamic ecosystem where innovation thrives and customer value drives every decision.

> **"Being able to solve customer problems with all partners is incredibly exciting. It's also the challenge. There's a Venn diagram of complexity—who owns the customer relationship? How can we pass value down through the channel, through the integrator, and can we still solve the problem for the end user? We have a responsibility to solve customer problems, and we have to do it together."**
>
> —BRET HOLBROOK, SENIOR VICE PRESIDENT, DORMAKABA USA

©2025, Security Industry Association. All rights reserved.

Channel Model to Value Chain

Sell-Through
becomes
Build-With

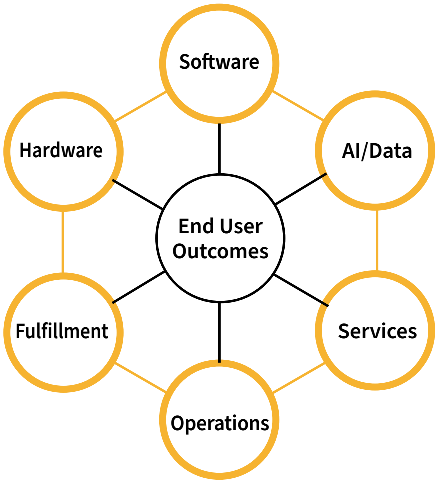
A Product Push
becomes an
Outcome Pull

Efficiency
becomes
Resilience

Competition
becomes
Collaboration

> **"The channel was a model built for transactions—not transformation. In a value chain model, the future of security is built together."**
>
> —ERIC YUNAG, EXECUTIVE VICE PRESIDENT, PRODUCTS AND SERVICES, CONVERGINT

The Value Chain Model: Focused on End-User Outcomes



KEY TAKEAWAYS

- The traditional channel model is giving way to a customer-centric value chain.
- Focus shifts from product delivery to end-user outcomes and resilience.
- Collaboration replaces competition; stakeholders co-create solutions.
- Hardware, software, AI and services converge to deliver integrated value.
- Success is measured by impact, not just efficiency or product sales.

©2025, Security Industry Association. All rights reserved.

MEGATREND 5

POSTHUMAN AUTOMATION OF SECURITY

Yes, this Megatrend is intentionally provocative. And no, we don't really expect all humans will be removed from security. What we do believe is that the security industry is entering a new era where automation and agentic AI redefine how systems operate and decisions are made.

Historically, security technology focused on detection and response, but advancements in AI now enable a shift toward prevention—an aspiration long held by practitioners. Agentic AI introduces capabilities that go beyond simple automation, allowing systems to interpret data, make decisions and execute actions without human intervention.

This transformation is already visible. AI-driven platforms are replacing labor-intensive tasks such as monitoring video feeds, ranking alarms and managing visitor access. Predictions suggest that AI will eventually handle universal scene analysis and automate processes traditionally managed by humans, including badge issuance and access permissions. While concerns about job displacement persist—highlighted by reports of AI-related layoffs—the reality is more nuanced. Rather than a mass extinction of roles, AI is expected to augment human capabilities, enabling professionals to focus on high-priority issues and strategic risk management.

The opportunity lies in leveraging AI for incremental gains: automating security reports, reviewing footage and interrogating data for trends and incident response. Practitioners seek tools that reduce friction and unlock hidden value, aligning with the principle of "aggregation of marginal gains."

Embracing this change proactively will ensure AI empowers rather than replaces the security workforce.

> **"The idea of post human security automation—which calls out the core of the transformation we're all contemplating with AI—begs the question of trust and reliability, to be sure, but more importantly underscores the reality of current labor trends leading to the decimation of the lowest rungs on the ladder, including the majority of roles in a traditional monitoring center or SOC."**
>
> –STEVE VAN TILL, PRESIDENT AND CEO, BRIVO

©2025, Security Industry Association. All rights reserved.

“This industry is ripe for being able to use the force multiplying benefits of agentic AI. It can handle lower-priority requests and automate them, and allow humans to focus on high-priority issues coming in.”

– STEVE LINDSEY, CO-FOUNDER, LVT

“The old benchmark used to be that ‘One day we’ll pass the Turing test,’ but we’ve already passed it 2 years ago and are moving on. AI can now do video things way better than a human can.”

– SHIKHAR SHRESTHA, CEO AND CO-FOUNDER, AMBIENT AI

Adapt or Extinct?

To ensure that AI isn’t a mass extinction event for your role, leverage AI to the best of your ability and embrace change head on, rather than wait.

Potential opportunities to develop agents for security:

- Automating security reports
- Automating user access permission reviews
- Automating review of security footage
- Automating learning for security professionals that matches their knowledge levels and gaps

What Practitioners Need From AI

Interrogation of Data

Assessments, trends and incident response

Reshaping Personnel Security Awareness Content Creation

Training

Appropriate Use of AI Within Security Services

that doesn't create security risk exposure

Ability to Solve Small Problems

A path to achieving greater insight and operational efficiency

KEY TAKEAWAYS

- Agentic AI shifts security from detection to prevention.
- Automation reduces human involvement in routine tasks like monitoring and access control.
- AI disruption is real but will augment, not eliminate, professional roles.
- Opportunities include automated reporting, video review and data-driven insights.
- Success depends on embracing AI strategically to enhance efficiency and resilience.

©2025, Security Industry Association. All rights reserved.

MEGATREND 6

END-TO-END SOLUTIONS AND ONE-LOGO APPROACHES

The security industry is witnessing a significant shift as vendors move beyond their traditional single-product categories to deliver comprehensive, end-to-end solutions. Historically, manufacturers specialized in narrow segments—video surveillance, access control or networking—but today, boundaries are dissolving. Companies like Axis Communications, Hanwha, Motorola Solutions and i-PRO have expanded from video into offerings for access control and even communications, while Verkada rapidly evolved from cameras to access, alarms and air quality monitoring. Even IT-focused firms like Ubiquiti have entered the security space, adding video and access solutions to their networking portfolios. And there are countless more examples of solution manufacturers transforming their product lines.

This evolution is driven by customer demand for simplicity and integration. Small and midmarket buyers increasingly prefer unified platforms that reduce complexity and eliminate the need to manage multiple vendors. For some, the appeal of a "one-logo" approach mirrors IT strategies where organizations standardize on a single provider, such as Microsoft, to streamline operations and support.

For security integrators, this trend has profound implications. To remain competitive, an integrator must offer at least one end-to-end solution in their portfolio. Buyers expect vendors and partners to deliver holistic systems that combine situational awareness, security and operational efficiency—without the heavy lifting of multiplatform integration. The future belongs to those who can provide seamless, scalable solutions under one brand.

©2025, Security Industry Association. All rights reserved.

> **“How are you going to make my life easier as a CSO? That is what I’m looking for from a vendor. I’m looking for a tool that will help the entire enterprise, not just physical security.”**
>
> —DAVID FORTINO, HEAD OF CORPORATE SECURITY, NEW YORK BLOOD CENTER ENTERPRISES

From One to Many

In Megatrend 3, we pronounced that security solutions are losing their boundaries—becoming more relevant as systems that capture and process data, be that for security or operational management. In this megatrend, we pronounce that traditional single-line product vendors are losing their boundaries, too, and are moving toward end-to-end solution models through R&D or acquisition.

Traditional Single-Line Vendor Examples

Video software vendor
Video hardware vendor

Access hardware vendor
Access software vendor

Communications vendor
Security operations center platform vendor

Intrusion hardware vendor
Intrusion monitoring software vendor

versus

End-to-End Solutions

1. No integration required
2. Compatibility across different product sectors
3. Locked to a single vendor
4. May offer limited customization and features

KEY TAKEAWAYS

- Single-product vendors are expanding into adjacent categories through research and development and acquisitions.
- End-to-end solutions appeal to buyers seeking simplicity and integrated functionality.
- One-logo strategies reduce complexity and mirror IT standardization trends.
- Security integrators must include at least one comprehensive solution in their offerings.
- Unified platforms deliver security and operational efficiency without multivendor challenges.

©2025, Security Industry Association. All rights reserved.

MEGATREND 7

THE UNIFICATION OF THE SECURITY EXPERIENCE LAYER

The security industry is moving toward a unified experience layer—a transformation that goes beyond integrating systems to fundamentally change how security is managed and experienced. Historically, platforms for access control, video surveillance and intrusion operated in silos, creating fragmented workflows and leaving valuable data underutilized. Today, the push for unified platforms and data aggregation is reshaping this landscape.

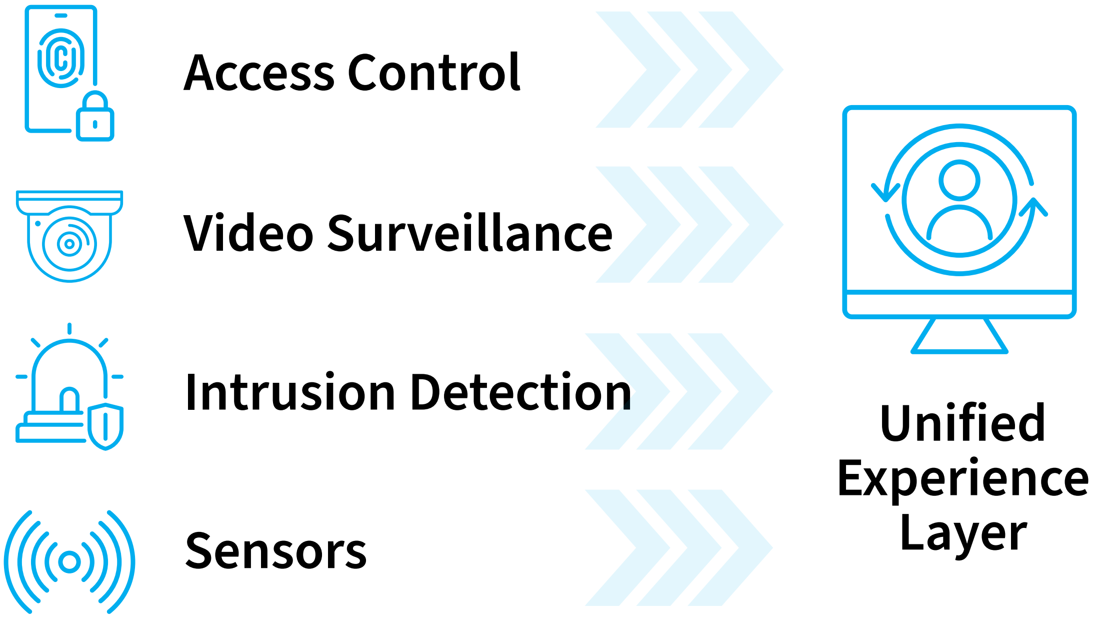
Unification begins with the data layer. Security systems generate massive amounts of information—video feeds, access logs, sensor alerts—but much of it remains untapped. By consolidating these data streams into a single architecture or overlay platform, organizations can surface actionable insights, automate responses and improve decision making. This evolution accelerates progress toward AI-driven outcomes, enabling predictive analytics and intelligent automation.

For smaller organizations, unified experience layers democratize advanced capabilities once reserved for enterprises with deep resources. Whether through end-to-end solutions or software overlays, the goal is not a “single pane of glass” but a smarter, more intuitive interface that enhances both operational efficiency and user experience. Ultimately, unification transforms security from a reactive function into a proactive, integrated component of business resilience.

©2025, Security Industry Association. All rights reserved.

> **“The industry is moving from a point solution to a systems solution. Understanding how we as an industry can bring the best in class of access, intrusion, video, visitor management, together in a platform and innovate for the user? How can we bring things together, streamline and reduce friction in the system?”**
>
> —SARAH RODRIGUES, CHIEF PRODUCT OFFICER, ACRE SECURITY

Unification of Data for a Unified Experience Layer



Access Control

Video Surveillance

Intrusion Detection

Sensors

Unified Experience Layer

KEY TAKEAWAYS

- Unified platforms combine access, video and intrusion into a single architecture.
- Data aggregation is essential for delivering actionable insights and automation.
- Unification improves decision making and accelerates AI-driven outcomes.
- Smaller organizations gain access to enterprise-level capabilities through unified solutions.
- The experience layer focuses on usability, efficiency and proactive security management.

©2025, Security Industry Association. All rights reserved.

MEGATREND 8

SECURITY OPERATIONS CENTERS (SOCS) AND MONITORING WILL BE TRANSFORMED AND AUTOMATED

The security industry is experiencing a seismic shift, driven by automation, AI and virtualization. Two areas at the center of this transformation are the traditional security operations center (SOC) model and the alarm monitoring industry. These changes are redefining how organizations manage risk, allocate resources and deliver value.

Part 1.

Transformation of the Security Operations Center

The era of the "showcase" SOC—characterized by massive video walls and rows of operators passively staring at screens—is rapidly drawing to a close. A fundamental disruption is underway, driven not by a desire for grander facilities, but by a relentless push for efficiency through automation and virtualization. This shift is democratizing advanced security capabilities, making global security operations center (GSOC)-level protection accessible to smaller enterprises that could never previously afford a dedicated command center.

The traditional SOC model is being dismantled by the twin forces of virtualization and AI. Organizations no longer feel the need to build physical "war rooms" where teams are co-located. Instead, decentralized, virtual teams are managing global command functions remotely, often supported by outsourced providers. Simultaneously, AI is rendering the "video wall" obsolete. Intelligent analytics now handle the monitoring, freeing human staff from the tedium of watching screens. This allows security personnel to pivot from reactive notification watchers to

©2025, Security Industry Association. All rights reserved.

proactive risk analysts, focusing their energy on anticipating threats rather than responding to routine pings.

Automation

- SOCs increasingly automated, reducing staff needs and enabling outsourcing
- Staff freed from monitoring notifications to focus on anticipating risks
- Less need for video walls as AI enables virtualization

Virtualization and Outsourcing

- Teams no longer need to be co-located for national or global command.
- Rise in outsourced SOC services makes capabilities accessible to smaller enterprises
- Makes GSOC-level functionality affordable for smaller enterprises

Part 2.

Disruption of the Alarm Monitoring Industry

The alarm monitoring sector faces an even more aggressive timeline, with AI predicted to largely replace human monitoring within seven years. The industry is adopting standards-based algorithms to automatically rank alarm priority and automate dispatch communications. This technological leap will likely force market consolidation, as only those capable of heavy investment in AI will survive; however, the payoff is immense: we are moving from "passive detection" to "active deterrence." Instead of just recording an intrusion, AI-driven systems can now execute a complex chain of automated responses—turning on lights, tracking subjects, triggering voice-downs and alerting patrols—instantly transforming a monitoring system into an active defender.

AI-Driven Automation

- AI automating video analysis, alarm prioritization and dispatch
- Largely replaces human monitoring within seven years

Standards-Based Prioritization

- Alarms ranked by algorithms according to industry standards
- Fully automated workflows emerging in alarm monitoring

Shift Toward Active Deterrence

- Automation provides path from passive detection to active deterrence

KEY TAKEAWAYS

The 7-Year Prediction
The clock is ticking for traditional monitoring. A bold industry prediction suggests that within seven years, AI will largely replace human labor for monitoring tasks, automating everything from video analysis to dispatch.

From Detection to Active Deterrence
Monitoring is evolving beyond the simple "Detect" phase. Through automation, systems can now execute the "Deter" phase without human intervention—automatically escalating responses from lighting changes to voice-downs and patrol dispatch.

The Democratization of the GSOC
You no longer need a Fortune 500 budget to have a global security operations center. Virtualization and outsourcing are making high-level command and control capabilities affordable and accessible to smaller enterprises.

©2025, Security Industry Association. All rights reserved.

MEGATREND 9

CORRECTING THE SYSTEMIC UNDERVALUATION OF SECURITY

Despite the security industry dismantling operational boundaries and delivering unprecedented utility, it remains trapped in a "cost center" paradox—offering more value than ever while still fighting for budget; however, a systemic correction is now underway to fix this historical undervaluation. The industry is collectively pivoting toward a "Return on Security" strategy. What was recently considered an innovative pitch—proving security's return on investment beyond risk mitigation—has become the default language for end users, integrators and manufacturers alike.

This shift is visible in pricing and product strategy. Vendors are realizing that adding advanced features without adjusting costs inadvertently signals that their innovation has no worth. Consequently, we are seeing a necessary rise in prices for lower-tier offerings to re-anchor market perceptions. This economic recalibration is critical for the human element of the sector. By establishing security as a value-generating asset rather than a sunk cost, the industry can justify the higher compensation needed to attract top-tier talent, which creates a virtuous cycle: higher perceived value leads to better pay, which secures a higher-quality workforce for the entire ecosystem.

> **"What we've seen is what we can unlock with the speed of information, how quickly we can come to insights, etc. That brings people to security because they see the value of our assets to contribute across the business."**
>
> — CHERYL STEELE, FORMER CHIEF SECURITY OFFICER OF STARBUCKS

©2025, Security Industry Association. All rights reserved.

Correcting the Systemic Undervaluation of Security

Security remains undervalued but is gaining recognition as a strategic asset

"Return on Security" is now a standard investment metric

Pricing strategies are evolving to reflect added value

Higher perceived value improves workforce quality and compensation

Industry-wide shift positions security as a business enabler, not a cost center

KEY TAKEAWAYS

The “Return on Security” Standard

The concept of ‘Return on Security’ has graduated from a niche sales tactic to the industry standard. It is now the baseline requirement for any investment conversation between manufacturers, integrators and buyers.

Changing Pricing Psychology

Stop giving it away. Vendors are recognizing that feature stuffing without price adjustments devalues their technology. Expect to see price increases on base tiers as the industry reasserts the worth of its baseline utility.

The Workforce Connection

Undervalued contracts lead to undervalued people. Correcting the financial perception of security is the only path to improving compensation, which is essential for attracting the high-quality talent the industry desperately needs.

MEGATREND 10

SECURITY TECHNOLOGY REFRESH CYCLES ACCELERATE

For decades, security technology was treated as a "buy and hold" investment. If a device installed 10 or 15 years ago still worked, it often stayed in place. Past refresh cycles were sporadic—video upgrades came with better image capture, and access control modernized as software moved to the cloud.

The philosophy surrounding security infrastructure is undergoing a radical shift. Historically, security hardware was viewed as a static "set it and forget it" investment. Today, that "run-to-fail" mindset is vanishing, replaced by an accelerated refresh cycle that mirrors the more rapid cadence of the IT world.

Today, the pace has changed dramatically. A major macro-level refresh is underway, driven by cybersecurity demands, AI adoption and IT oversight. Outdated operational technology—security systems, building automation and smart sensors—now represents a serious vulnerability. IT leaders are scrutinizing these devices because unsecured endpoints can enable lateral attacks across networks.

Corporate IT's influence has also reshaped refresh expectations. While IT traditionally operated on a three- to five-year cycle, security is now aligning with similar timelines (although not as fast as common refresh rates on devices like PCs). The rise of AI and automation is accelerating this trend, as organizations seek analytics-driven solutions and edge computing capabilities. New AI functions are fueling innovation, potentially making older hardware obsolete in terms of functionality.

Compliance pressures add urgency. Updated standards that add interoperability and improved cybersecurity are encouraging organizations to replace legacy systems, while edge computing enables smarter, low-latency devices that support automation. Integrators report strong demand despite economic uncertainty, signaling confidence in this transformation.

We are in the early stages of this refresh, but its impact is profound. Security teams must rethink processes and data strategies, paving the way for boundaryless security ecosystems and correcting the historic undervaluation of security. Looking ahead, postquantum readiness will drive the next wave—but for now, AI and cybersecurity are the catalysts for change.

©2025, Security Industry Association. All rights reserved.

> **“We map the tech readiness level to see how close to implementable and securable it is. Can we test it, can we work with it? Is the technology there, and are the tools to work with it there? Is it even possible to work with this technology yet? And then failure modes analysis—what’s the worst thing that could happen right now as you implement a technology? Could it be insecure? Could it create security gaps? Ask these questions as you consider when technology is ready.”**
>
> — PETER BORISKIN, CHIEF TECHNOLOGY OFFICER, AMERICAS, AT ASSA ABLOY OPENING SOLUTIONS, ON DECIDING WHEN TO DECIDE IF A TECHNOLOGY IS READY FOR THE MARKET

The Next Big Refresh

Looking to the future, the next-generation refresh (not this cycle) is projected to be driven by postquantum readiness. But while postquantum and advanced technologies are important, integrators will tell you that many organizations they serve still rely on older platforms, making a broad, macro-level refresh cycle that speeds adoption of AI automation and edge computing the more immediate need.

Cybersecurity is the #1 driver of refresh cycles

AI and automation demand modern hardware and edge computing

Corporate IT now collaborates on security technology decisions

Compliance and new standards accelerate replacement of legacy systems

KEY TAKEAWAYS

The Timeline Shift

A 10-plus-year life cycle for security devices and software is obsolete. Driven by IT influence, security is moving toward a higher refresh rate to keep pace with hardware acceleration and threat landscapes.

The Risk Driver: Cybersecurity

Outdated operational technology is no longer just “old”—it is a liability. IT leaders are mandating refreshes to close the security gaps where unsecured physical devices provide hackers access to the broader corporate network.

The Functional Drivers: AI and Compute at the Edge

The refresh isn't just about safety—it's about capability. The availability of powerful AI chips is pushing compute power to the edge, replacing passive sensors with active automation tools that businesses now demand.

©2025, Security Industry Association. All rights reserved.

Powering Your Business Intelligence

From artificial intelligence to operational security technology, data centers, school security funding, market research and career tools, you can find essential insights into the security industry at securityindustry.org/reports.

The Evolving Security Landscape: The Path to International Expansion

This report, produced by the SIA Executive Advisory Board in collaboration with Novaira Insights, looks at the impact new entrants are having on security.

Operational Security Technology: Principles, Challenges and Outcomes

This report, available in English and Spanish, provides a comprehensive overview of OST, key technology types, challenges and best practices to help with making mission- critical investment decisions.

Guide to AI Use Cases in Security

This report provides guidance on the responsible, effective and human-centric use of AI in security, including key tech, use cases, benefits, implementation considerations and best practices.

SPARC Intelligence Report: Evaluating AI Vendors

This report helps end users accurately evaluate AI-based security solutions by clarifying true AI capabilities and providing clear guidance and decision-making considerations.

Guide to Securing Data Centers

This report outlines the rising complexity and critical importance of physical security in the rapidly expanding data center market, offering a roadmap to resilient, integrated solutions that keep pace with industry growth.

Guide to State and Local Laws on Facial Recognition Technology

This report provides guidance to U.S. state and local laws on facial recognition technology and related legislative trends.

Mexican Physical Security Market Assessment

This research report, produced for SIA by Omdia and available in English and Spanish, provides insights into the equipment, technologies and economic significance of the security industry in Mexico.

Guide to School Security Funding

This guide provides education leaders and partners with a centralized resource on funding opportunities and grants available for K–12 school security solutions.

The Evolving Security Landscape
The Path To International Expansion
SIA
OPERATIONAL SECURITY TECHNOLOGY
Principles, Challenges and How to Achieve Mission-Critical Outcomes Leveraging OST
SIA
Guide to AI Use Cases in Security
SIA
SPARC INTELLIGENCE REPORT:
GUIDANCE FOR EVALUATING AI VENDORS/SERVICE PROVIDERS
SIA
SIA
SECURING DATA CENTERS
A Guide to Trends and Strategies for the Physical Security of Data Center Facilities
Guide to State & Local Laws on Facial Recognition Technology
A Reference Guide to U.S. State and Local Laws on Facial Recognition Technology and Related Legislative Trends
SIA
MEXICAN PHYSICAL SECURITY MARKET ASSESSMENT 2025
SIA
SIA
SIA GUIDE TO SCHOOL SECURITY FUNDING
A guide to federal and state funding sources and programs for school safety and security improvements
securityindustry.org

SIA
SECURITY INDUSTRY ASSOCIATION

securityindustry.org