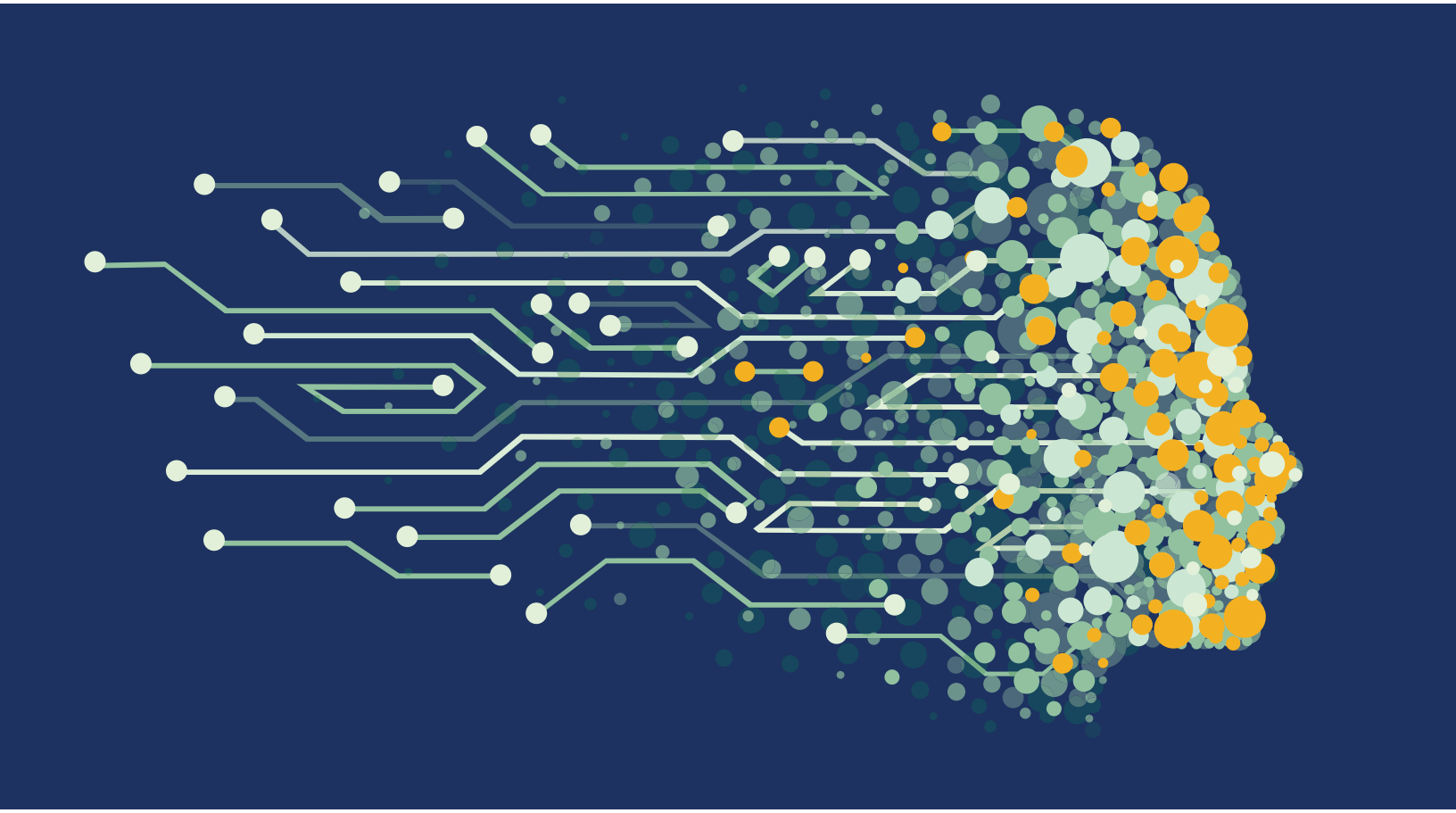
2024 SECURITY MEGATRENDS™

THE ANNUAL VISION FOR THE SECURITY INDUSTRY



SIA
SECURITY INDUSTRY ASSOCIATION

JAMES ROTHSTEIN
SIA Chair of the Board

Megatrends Advisors
BILL BOZEMAN
Founder, Bozeman Strategic Solutions

TARA DUNNING
Vice President, Global Security Strategy and Sales, Communications & Security Solutions, Wesco

KASIA HANSON
Global Senior Director, Physical and Cybersecurity Ecosystems, Intel

JOHN E. MACK III
EVP and Co-Head of Investment Banking, Imperial Capital

BRIAN RUTTENBUR
Senior Vice President, Investor Relations, SmartRent

STEVE VAN TILL
Founder and CEO. Brivo

ERIC YUNAG
Vice President of Innovation, Convergint

DON ERICKSON
SIA CEO
derickson@securityindustry.org

GEOFF KOHL
SIA Senior Director of Marketing
Author and Editor, 2024 SECURITY MEGATRENDS Report
gkohl@securityindustry.org

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

MARC BENSON
Associate Director of Membership
mbenson@securityindustry.org

MICHELLE WANDRES
Production Design

MATT MARAIST
SIA Senior Manager of Graphics and Videography
mmaraist@securityindustry.org

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

2024 SECURITY
MEGATRENDS™

AN EVOLVING INDUSTRY THAT STAYS MISSION FOCUSED

At SIA, we may represent the security industry, but the boundaries of our industry's value are disappearing as we evolve. This change is visible in this year's ranking of the 2024 Security Megatrends, where AI-related trends held the top four slots and where the return on investment (ROI) of security holds the fifth.

Our industry is deeply focused on adding value—from thinking creatively about how security technologies can provide value to office property owners who are seeking to make their buildings more efficient as they adapt to a long-term trend of mobile work to supporting small businesses like retailers who need their security investments to serve to not only protect their operations, but also give them the insights they need on their retail performance.

In surveying our members as part of the research for the 2024 Security Megatrends report, 93% said they expected to see generative artificial intelligence (AI) like ChatGPT make an impact upon their business strategies within the next 5 years, and over 89% said that they had AI projects active in their research and development (R&D) pipelines. This is profound given that OpenAI's ChatGPT project was only introduced to the world a year ago. SIA responded to this hyperfocus on AI by immediately establishing the SIA Artificial Intelligence Advisory Board, a group comprised of industry leaders with a mission to educate our members about relevant trends, applications and regulations.

At the 2023 Securing New Ground conference, held in October in New York City, the discussion from top business leaders who took the stage was not just about how they were securing their business clients. Rather, the conversations focused on how they were working with end-user clients to identify ways in which their solutions and services were able to deliver business value—data, insights and increased operational performance—for their clients in nonsecurity use cases.

That commitment to adding value is at the core of how our industry thinks and moves. We have always given our clients the comfort of knowing that their people, property and assets are protected. As every great business leader knows, the value of their people is of the most importance, and that still holds true in a world that relies more on AI. Protecting people will always be the greatest value we can provide, but as an industry, we are insatiable in our quest for progress, and will never stop as we unlock new value for our customers, clients and partners.

To our members: Thank you for your input in shaping these megatrends and then allowing us to share them as the 2024 Security Megatrends. These are the trends that we believe are not only impacting our industry, but also touching the broader tech industry and the world at large.

Sincerely,
James Rothstein
Chair, SIA Board of Directors

THANK YOU

SIA GREATLY APPRECIATES THE SUPPORT OF ITS 2023 SNG SPONSORS

MEDIA PARTNERS

SNG™

SECURINGNEWGROUND®

THE BUSINESS OF SECURITY

SAVE THE DATE

OCTOBER 8-9, 2024 | NYC

SIA
SECURITY INDUSTRY ASSOCIATION

HOW WE DEFINED AND RESEARCHED THE 2024 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 further surveyed 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.

Simultaneous to the surveys at SNG and the SIA membership, our group of SIA Megatrends advisors—including Steve Van Till of Brivo, Brian Ruttenbur of Smart Rent, Tara Dunning of Wesco, Kasia Hanson of Intel, Eric Yunag of Convergint, Bill Bozeman of Bozeman Strategic Solutions and John Mack of Imperial Capital—provided focused feedback on the megatrends via in-depth conversations and collaborative editing. The earch 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 poll-driven session during the 2023 SNG conference (hosted by Van Till, Dunning and Hanson) provided additional feedback related to the Security Megatrends and helped generate some of the chart data included in this report. Lastly, as we authored this report, we tried to not only reflect the vendor/integrator/service provider side of the industry but include again a brief reflection on how each trend may impact the security practitioner or chief security officer (CSO).

Through SIA's research and the vetting, validation and additional research that occurs during and after SNG, here we have, hopefully, not only captured the industry's driving forces in the 2024 Security Megatrends report, but also provided you insights and action items to facilitate a successful future in the security industry.

Geoff Kohl
Editor, 2024 Security Megatrends report
Sr. Director of Marketing, SIA

2024 SECURITY MEGATRENDS

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.

GLOBAL TENSIONS

From global tensions that play out in the form of cyber espionage to ones involving tanks, terror attacks and remote drone strikes, global tensions are a constant mark on the radar of business and security. Security and business leaders have to think ahead: How will this conflict affect my overseas or traveling team members? What will this mean for our sourcing, shipping and market sector growth?

CLOUD MODEL FOR TECHNOLOGY DELIVERY

Cloud services were long a Security Megatrend, but today cloud is just part of how technology services are deployed, with even most of the software-and-server companies now offering their solutions as cloud-delivered solutions. And while cloud leaders like Ken Francis of Eagle Eye Networks told the audience at SNG 2023 that the security industry still has a long way to go in terms of transforming its offerings as cloud-based services, we think this now has become such a core option to technology delivery that we're calling it a "foundational trend."

CHANGING ECONOMIC CONDITIONS

After a relatively long period of steady economic growth that benefited from consistently "normal" (read: low) inflation and low interest rates, today's business leaders are facing more volatility and uncertainty, increased inflation and higher interest rates. Anyone who thought we'd snap out of that period of economic uncertainty came to be sorely disappointed, and today this volatility is just fundamental to today's economic conditions.

SUPPLY CHAIN ASSURANCE

When supply chains of all types ground to a near halt during the COVID-19 pandemic, supply chain assurance earned the attention it has always deserved. As Wesco's Bill Geary said at SNG 2023, "[The focus on the] supply chain is growing and has a prominence in the C-suite that it never had before. Companies are looking at it in a different way, and that focus will be a driver."

FOUNDATIONAL

CYBERSECURITY

Cybersecurity has long reigned supreme among the megatrends, but today it's 100% foundational. Security executives who are not thinking about cybersecurity, planning for a cyber incident and building their internal resources are missing the obvious. In November 2023, the "Cyberav3ngers" working for Iran's Revolutionary Guard Corps breached the networks of multiple U.S. water/wastewater utilities, and this kind of breach barely registered any media attention—that's how accustomed the world has become to cyberattacks, and that's why security leaders must be steadfast in their attention to this concern. Convergence of cybersecurity and physical security continues to progress, and to help support the industry with cyberscurity and convergence resources, SIA operates a Cybersecurity Advisory Board, dedicated to providing insights and resources in this foundational area.

WORKFORCE DEVELOPMENT

Hiring is difficult; unemployment remains low, and roles across the security industry—from guards to technicians to systems architects—require even more skills than ever before. Companies need to focus on core activities like working with local universities, colleges and trade schools, and the industry needs to continue to bond together through groups like the Foundation for Advancing Security Talent (FAST) to demonstrate career paths and help market the industry as a great destination for a rewarding and fulfilling technical career.

SUSTAINABILITY

Designing solutions and systems for increased energy efficiency is becoming the norm, even if an environmental, social and governance approach to business hasn't become a standard. Companies are also seeking to reduce waste, reduce energy costs of production and operation and connect sustainability with their bottom lines. Sustainability isn't just about your carbon footprint and natural resources—it's also about sustainable economic growth and your social sustainability, including at the human level. As ASSA ABLOY Director of Sustainable Builiding Solutions Amy Musanti remarked to the 2023 SNG audience, "If it's important to our customer, it's important to us." As part of this foundational trend SIA created an ESG Advisory Board in fall 2023 to provide guidance for members navigating this aspect of their businesses.

33%

Share of SIA surveyed members who expect sustainability initiatives to make a strong impact on their business or product strategy within the next 5 years

TRENDS

TRENDS WE LOVE SO MUCH THAT THEY ARE JUST STRUCTURAL TO THE BUSINESS OF SECURITY

MEGATREND 1

THE SECURITY OF AI

MEGATREND MOVEMENT

With AI rising to the No. 1 spot for 2024 and cybersecurity moving into a "foundational trend" spot, the security of AI is somewhat of a blend of AI and cybersecurity (and a lot more than that).

If AI is the overarching megatrend, claiming the four top trend spots, the specific AI megatrend that has to preface them all is the security of AI—this is the security industry, after all, and we always lead with protection and trust.

With the ongoing adoption of AI into businesses of all sizes, the need to prioritize cybersecurity for the protection of data, IP and corporate integrity has never been greater. A comprehensive and proactive security posture for AI should enable an organization to devise, develop and deploy machine learning models from day one in a secure environment, with real-time awareness that's easy to access, understand and act upon.

There is an opportunity for integrators and manufacturers to understand AI impacts on their business and their customers. What are the customer's AI policies, plans, investments and ecosystem? AI security tools and platforms should protect organizations with smaller budgets who must turn to open-source marketplaces for machine learning models or ready-to-use AI components by allowing them to use these products with safety and security from the start. Without tools to monitor the health and security of AI models in use, it's only a matter of when, not if, a company will experience a security breach.

DEFINING THE SECURITY OF AI

The security of AI is defined by these three topics and questions:

1. Trust of AI. How do we trust AI as it begins to automate more of our business and life experiences?

2. Ethical Application of AI. How do we ensure that AI is applied ethically and fairly? Do we have consent to use the data to which we are applying AI?

3. Cybersecurity of AI. How do we ensure the AI algorithms and even the hardware running the AI do not become corrupted, poisoned or attacked?

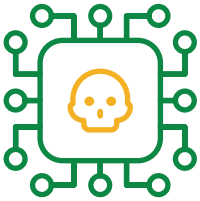
IMPACT TO THE SECURITY PRACTITIONER

For the practitioner, AI is an enormous opportunity, but for a security practitioner, any additional technology system also becomes one more threat vector.

Because AI is built on data, ingests data and makes sense of data, to control the security of AI, practitioners will need to start by getting control of their data—understand where it exists, what the privacy concerns are, etc.—and build corporate policies about how they use that data. That work will be transformative to the control of AI as a practitioner.

Practitioners will also be required to evaluate the cybersecurity practices of their AI vendors and the integrators and service providers that touch those systems and will always need to be able to be transparent to their boards and senior leaders about how they are applying AI.

Establishing a framework for safe and ethical use of data helps to protect your business and customers and facilitates the adoption of new technologies by streamlining decision making. That transparency and clarity can provide peace of mind—both internally and to customers.



30%

Expected percentage of AI cyberattacks that will leverage training-data poisoning, AI model theft or adversarial samples

Source: Gartner

34%

Number of companies/organizations which are already using or implementing AI application security tools

Source: Gartner

54%

Number of security technology firms which said that public perception of some AI technologies (e.g., facial recognition) was limiting their further expansion into AI applications

"PREVENTING ADVERSARIAL AI ATTACK TYPES SUCH AS DATA POISONING AND PROMPT INJECTION, WHILE PREVENTING AND MITIGATING SUPPLY CHAIN ATTACKS LIKE RANSOMWARE AND BACKDOORS ARE KEY FACTORS IN FACILITATING A COMPREHENSIVE SECURITY POSTURE FOR AI."

– INTEL/HIDDEN LAYER REPORT, "THE FUTURE OF RISK IS UPON US."

"ADVERSARIAL DATA POISONING IS AN EFFECTIVE ATTACK AGAINST MACHINE LEARNING AND THREATENS MODEL INTEGRITY BY INTRODUCING POISONED DATA INTO THE TRAINING DATASET. SO FAR, IT HAS BEEN STUDIED MOSTLY FOR CLASSIFICATION, EVEN THOUGH REGRESSION LEARNING IS USED IN MANY MISSION-CRITICAL SYSTEMS (SUCH AS DOSAGE OF MEDICATION, CONTROL OF CYBER-PHYSICAL SYSTEMS AND MANAGING POWER SUPPLY)."

– FRAUNHOFER INSTITUTE FOR APPLIED AND INTEGRATED SECURITY, "DATA POISONING ATTACKS ON REGRESSION LEARNING AND CORRESPONDING DEFENSES," 2020

MEGATREND 2

AI: VISUAL INTELLIGENCE, NOT VIDEO SURVEILLANCE

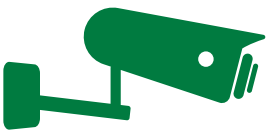
MEGATREND MOVEMENT

AI: Visual Intelligence, Not Video Surveillance is something of a synthesis of two trends: 2023's No. 10 Megatrend, The Proliferation of Sensors, and that year's No. 2 trend, AI.

AI has reached the apex of the megatrends, and the camera has become the ultimate sensor. Now AI is permanently changing the value proposition of video surveillance. It's now "visual intelligence," not video surveillance.

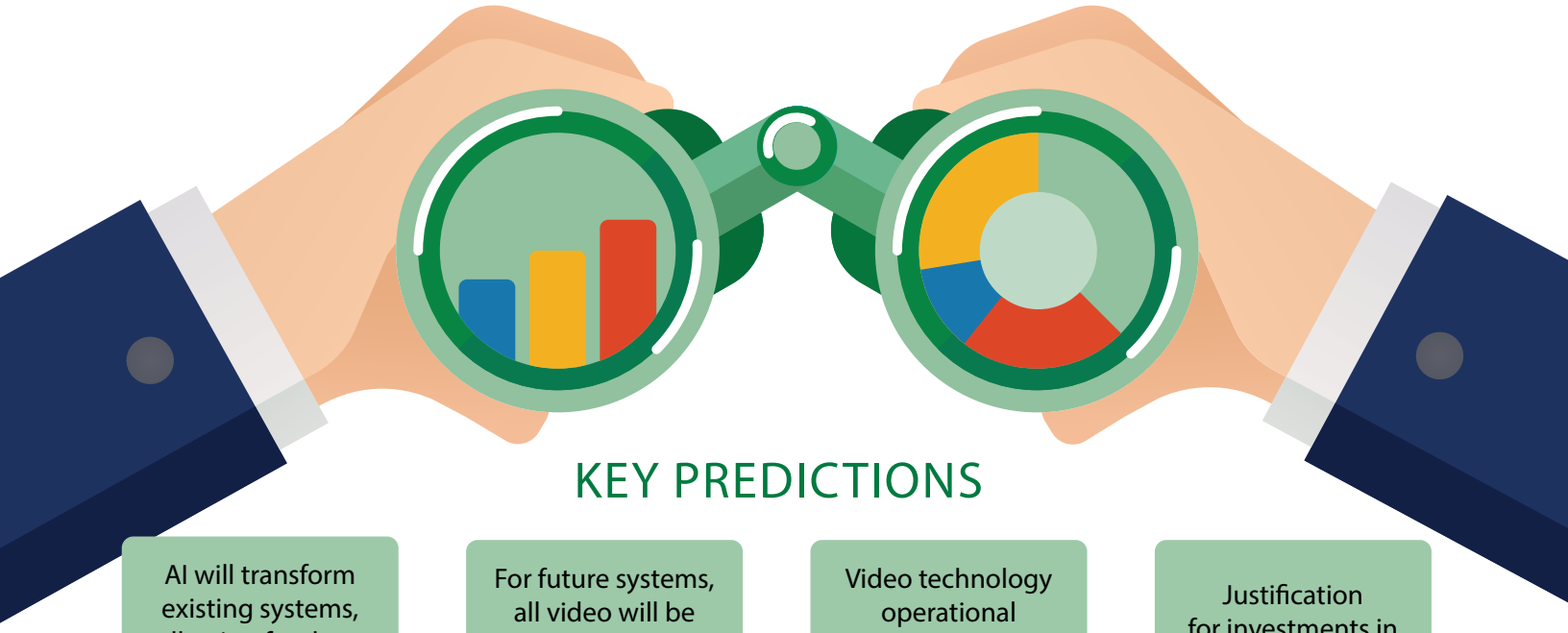
The camera is rapidly becoming the "everything tool" in our industry—moving beyond its early capacity as a recording device and creating the opportunity for exponential value. More than a camera, these devices are a platform for multiple sensors (audio, chemical, temperature, etc.). AI and analytics applied to these cameras' sensors will make the cameras 10, 100 or maybe even 1,000 times more valuable to end user, particularly when you compare yesterday's norm of unmonitored cameras to today's camera where the system does the monitoring 24/7 and alerts in real time, on the optical sensor as well as the other supported sensors.

The capabilities of visual intelligence are evolving, and businesses are beginning to create a visual intelligence infrastructure. The security industry's fundamental challenge is whether we will lead in this growth area as video surveillance becomes visual intelligence: Will our industry's product makers, installation/integration channels and security practitioners be the ones driving the ship to leverage these systems for business process automation and improvements related to customer, visitor and employee experiences?



THE INTERNET OF THINGS: MOSTLY CAMERAS?

The Internet of Things (IoT) was once perceived to be a vast network of sensors. As it turns out, many of those sensors will be cameras. By the end of 2023, 16.7 billion connected IoT devices are projected. That is expected to grow to 29 billion by 2027.



KEY PREDICTIONS

AI will transform existing systems, allowing for deep search of recorded content.

For future systems, all video will be analyzed in real time, not just stored.

Video technology operational ownership will not be exclusive to the security team.

Justification for investments in camera technology will be easier

IMPACT ON THE SECURITY INTEGRATOR

As the camera evolves and becomes the ultimate sensor, it will help expand the integrator's opportunity to deliver value to the end user that extends beyond the traditional security use cases. The rate of innovation is challenging the entire ecosystem to rise to the consultative requirements and enact policies and regulations that leverage AI and large language models (LLMs) responsibly.

The camera's expanding role creates opportunity and disruption. Integrators that adapt and expand their depth and breadth in functional consulting can reap the rewards and maximize the value of their customers' investment in surveillance systems. On the other hand, those that stay narrowly focused may be edged out of higher-value projects.

Just like the manufacturing community, integrators must take a hard look at the use cases that leverage AI and set boundaries around applications they will not consider in their practices. This may mean passing on business, but building a practice on solutions that become regulated out of existence will yield short returns and the potential for reputational harm.

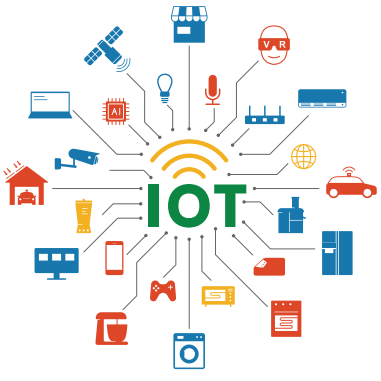
78 million

Number of security cameras shipped globally in 2022

Source: OMDIA/SIA

16.7 billion

Number of connected IoT devices expected by end of 2023 Source: IOT Analytics



MEGATREND 3

GENERATIVE AI

MEGATREND MOVEMENT

Generative AI is brand new to the Megatrends for 2024, but this trend is an expansion of the overall AI trend that was ranked No. 2 in our 2023 report.

ChatGPT debuted at the end of November 2022 (sadly, too late for the 2023 edition of Security Megatrends that came out a few days later) as a text-prompt-only AI programmed with data that was two years old, but by February, news media were proclaiming that it had already broken the Gartner hype cycle for technology, and its interface and functionality improved rapidly during 2023.

In the time since, the world at large has become familiar with large language models and generative AI and has had it write poems for family gatherings and, yes, author essays for students. Today, scores of AI-powered image generators exist, and AI applications like Google Bard and even ChatGPT can help programmers write code.

As these technologies improve and adoption expands, the security industry is likely to change in three primary areas:

1. LLM applications (like ChatGPT) will be applied to security systems data
2. Generative AI will be used for content creation
3. Generative AI applications will be applied to solving business operational challenges

"GENERATIVE AI IS POISED TO REVOLUTIONIZE THE SECURITY LANDSCAPE BY DYNAMICALLY ADAPTING TO EVOLVING THREATS, AUGMENTING HUMAN DECISION MAKING AND PROVIDING AN AGILE DEFENSE THAT ANTICIPATES AND RESPONDS TO THE EVER-CHANGING SECURITY CHALLENGES OF THE FUTURE. IT WILL BE LIKE GENIE WHICH WILL DO EVERYTHING SECURITY LEADERS WANT, AND MOST IMPORTANTLY IT WILL ALSO SHOW THEM WHAT THEY SHOULD BE DOING SO THAT THEY ARE NOT BLINDSIDED BY ANY POTENTIAL THREATS."

– JASVIR GILL, CEO, ALERT ENTERPRISE

1 LLM AND GENERATIVE AI APPLIED TO SECURITY

Whether it's text chat or voice conversations, LLM-style generative AI applied to security solutions will unlock data and insights, provide training and illuminate policies and procedures within security departments. "We have a lot of times when people have to make a decision pretty quickly about the right thing to do," explained Brivo CEO Steve Van Till at Securing New Ground 2023. "Generative AI can be an active assist to people in these examples of critical roles.

- Unlock data: [Security: "Export all video clips in which someone was in the north stairwell last night between midnight and 5 a.m."]
- Unlock insights: [Security: "Show all unusual activity in the north stairwell."]
- Personnel training: [Security: "Train me on how to file an incident report."]
- Speed response: [Security: "Show me a recommended security response for a verbal threat made to an employee by a customer."]

The industry is already seeing early examples of LLM applications (similar to ChatGPT) applied to security and is likely to see a new wave of innovation coming from security command and control providers as they leverage these tools to improve the interface and functionality of their systems.

2 GENERATIVE AI: THE BLESSING VS. THE CURSE

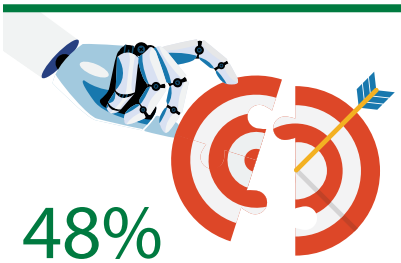
The blessing: Synthetic data. One of the common complaints of video analytic developers is that machine learning often requires many examples to be able to effectively train an AI. Want to teach an AI what a slip-and-fall looks like? You have to show real slip-and-fall incidents, and AI/machine learning experts note that there just isn't a big database of security video footage with specific incident classified and tagged that is accessible to them. Companies like Nvidia are already developing digital twin-style virtual reality worlds to help train AI for robotics and claims its virtual reality environment "augments costly, laborious human-labeled real-world data, which can be error prone and incomplete, with the ability to create large and diverse physically accurate data tailored to the needs of AV and robotics developers." There's early speculation that synthetic data could be the "golden unicorn" that AI developers need to train AI for visual intelligence systems like those for video security applications, solving the problem of there simply not being enough test data.

The curse: Deepfakes. As generative AI moves beyond 2D artistic image creation, it steps into the world of being able to convincingly create fake video clips. The Israel-Hamas and Russia-Ukraine conflicts have demonstrated the proclivity for faked video clips as a tool to attempt to shape public opinion, and this strategy is likely to eventually be applied in the form of fake security incidents that could cause brand reputation.

3 GENERATIVE AI: BROAD APPLICATIONS FOR BUSINESS

Generative AI and other AI tools are becoming part of how you operate your business, and businesses that are not beginning to adopt AI right now will be falling behind. Today, AI chatbots are now commonplace for real-time customer service, but you can now feed in large data sets to use AI to find insights from that data or identify areas for potential operational efficiency improvements.

To find these efficiency opportunities, users will need clearly defined processes and a corresponding data set. For companies that have the processes and the data and which are currently applying a lot of personnel hours to effect/actuate that process, it's likely they can apply AI to solve that problem. Examples are using AI to improve alarm monitoring, better match staffing levels for contract officers with incident occurrences, combine data from intrusion and access systems to identify aberrant behavior or even combine project locations, project types, technician skills and service truck GPS data to determine more efficient routing and use of field techs.



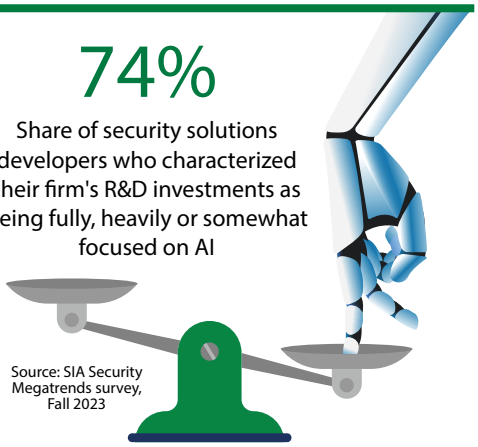
48%

Percentage of security solution developers who expect generative AI to have strong impact to their strategy within the next 5 years

Source: SIA Security Megatrends survey, Fall 20232

74%

Share of security solutions developers who characterized their firm's R&D investments as being fully, heavily or somewhat focused on AI



Source: SIA Security Megatrends survey, Fall 2023

IMPACT ON THE SECURITY PRACTITIONER

Generative AI applied to the interface of security systems can mean more efficient control of security systems and the possibility to apply generative AI to guide security officers on operating procedures, while allowing officers to query systems to elicit hidden insight to data.

MEGATREND 4

REGULATION OF AI

MEGATREND MOVEMENT

Entirely new for the 2024 report, this trend rides on the wave of substantial legislative activity happening in the U.S. and the EU.

AI is the key to dramatic change in the future of the security industry, and accompanying that change will likely be a wave of regulations that establish a framework on AI.

Coupled closely with Megatrend No. 1, the Security of AI, this trend of regulation is the mechanism to ensure trust and transparency.

The security industry, and all industries using artificial intelligence, should expect widespread regulation of AI applications in the coming years, but many believe having a framework could actually speed up development of AI technology.

Regulation of AI is coming, so the AI landscape of tomorrow is likely one that involves more compliance, more data privacy and likely even more openness/transparency about the algorithms themselves and how they are applied.

"THE JURY IS STILL OUT ABOUT WHETHER YOU CAN REGULATE THIS TECHNOLOGY [AI] OR NOT. THERE'S A RISK THIS E.U. TEXT ENDS UP BEING PREHISTORICAL."

—ANDREA RENDA, SENIOR RESEARCH FELLOW AT THE CENTER FOR EUROPEAN POLICY STUDIES, AS QUOTED IN THE NEW YORK TIMES

"AI HAS BECOME ONE OF THE HOTTEST POLICY TOPICS DISCUSSED IN WASHINGTON AND GLOBALLY. THE EUROPEAN UNION IS ENACTING SWEEPING REGULATIONS ON AI SYSTEMS THAT HAVE BEEN YEARS IN THE MAKING, WHILE MORE THAN 50 RELATED BILLS WERE INTRODUCED IN THE U.S. CONGRESS IN 2023. IN OCTOBER, THE BIDEN ADMINISTRATION RELEASED THE MOST SIGNIFICANT EXECUTIVE ORDER YET ON AI, WHILE SEVERAL U.S. STATES HAVE LAUNCHED TASK FORCES TO EXAMINE USE OF RELATED TECHNOLOGIES IN GOVERNMENT. IT'S LIKELY THAT IN 2024 WE WILL SEE STATE LEGISLATIVE MEASURES UNDER CONSIDERATION, AND THERE IS A HIGH LIKELIHOOD OVER TIME THAT ONE OR MORE STATES WILL ACT TO BROADLY REGULATE AI AHEAD OF POSSIBLE ACTION AT THE NATIONAL LEVEL."

— JAKE PARKER, SENIOR DIRECTOR OF GOVERNMENT RELATIONS, SIA

REGULATIONS TO WATCH

President Biden: President Biden's executive order from Oct. 30, 2023, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," provides an early framework.

OMB: The U.S. Office of Management and Budget's proposed memorandum, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," about implementation of President Biden's executive order.

Individual U.S. States: There is the potential that individual U.S. states may implement regulations creating a problematic patchwork of laws on AI. We are likely to see state-level creation of AI regulations before comprehensive federal regulations are put into effect. As an example, the California Consumer Privacy Act was the first in the United States to provide data privacy regulation, and it was done before federal regulations or other states, and it nearly coincided with the EU's General Data Protection Regulation.

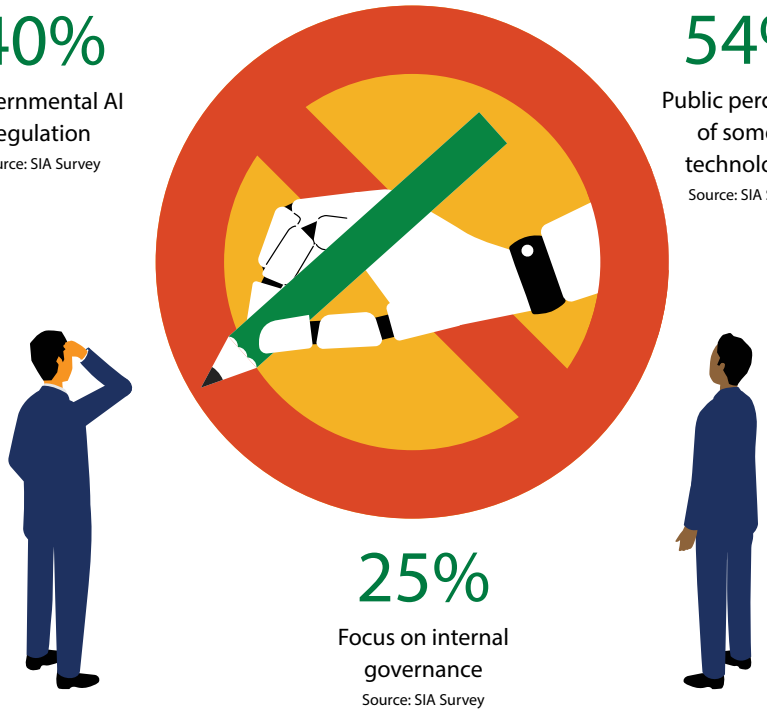
EU: The European Union's European Commission and Parliament's AI act. The European Parliament states that the goal is "to make sure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly. AI systems should be overseen by people, rather than by automation, to prevent harmful outcomes. Parliament also sought to establish a technology-neutral, uniform definition for AI that could be applied to future AI systems." The EU's AI Act was passed on Dec. 8, 2023, but some aspects of the policy would not take effect for 12 to 24 months.

Biometrics and Facial Recognition: As seen in SIA's recent guides to facial recognition laws and biometric information privacy laws, regulation has been occurring at the state and even municipal levels, and this is likely to continue. While these aren't AI laws themselves, they may incorporate some of the data sets that AI systems will access.

WHICH OF THE FOLLOWING FACTORS ARE LIMITING YOUR EXPANSION INTO AI?

40%
Governmental AI regulation
Source: SIA Survey

54%
Public perception of some AI technologies
Source: SIA Survey



25%
Focus on internal governance
Source: SIA Survey

IMPACT ON THE SECURITY PRACTITIONER

The security practitioner will need to be steadfast in awareness of legislation governing AI applications. The ability to manage compliance to regulations of all types—including rules that shape data privacy and AI and biometrics deployments—will become a necessary skill set within a security practitioner team.

However, many practitioners have indicated to SIA that they have been reticent to implement some AI applications that involve facial recognition, due in some part to the fact that the legal framework wasn't clearly defined at a federal level. Once AI regulatory guidance and implementation policies existing at the U.S. federal level or from the European Union, this may give practitioners in these regions enough confidence to being to expand their implementation of AI.

MEGATREND 5

EXPANSION AND EVOLUTION OF SECURITY'S ROI

MEGATREND MOVEMENT

While a new trend for 2024, this trend is also an evolution of the 2023 trend about the "Elimination of Industry Boundaries."

In 2023, one of the new Megatrends was the "Elimination of Industry Boundaries." In last year's report, that was largely focused on how our industry was expanding into adjacencies (think Vivint and solar or ADT making deals with State Farm). It also covered how access control companies were providing building usage data as a form of "proptech."

Today this trend includes all of the former megatrend but also includes how security solution offerings are offering business value beyond the core security need. In that sense, this is really the parent trend to how AI is converting video surveillance into visual intelligence.

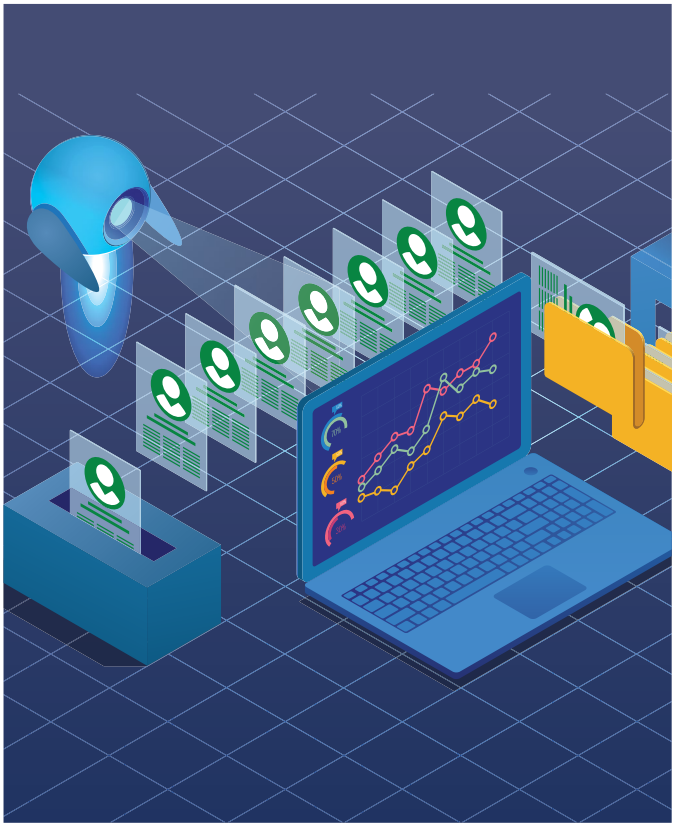
When security systems and solutions produce return on investment (ROI) outside of the core security outcomes, these solutions become more indispensable to the practitioners/business owners. The indispensability is becoming very visible in the access control sector, where access control vendors are seeing a rapid increase in integrations/partnerships with their platforms as building owners strive to unlock data insights out of their real estate.

"IT'S EASIER TO MAKE THE REQUEST FOR FUNDING IF YOU CAN MAKE THE CASE FOR ROI."

—HELEN NEGRE, CHIEF CYBERSECURITY OFFICER, SIEMENS

VISUALIZE IT

Security leaders can find value in data visualization by using tools like Microsoft's Power BI and Salesforce's Tableau. Consultant Sean Ahrens shares the example of how he correlated a heat map of camera and call box coverages to demonstrate consistency in device coverage and show where there were gaps. A similar project using data visualization showed where campus devices were needing preventative maintenance or were close to the end of their functional lives – all allowing wise investments of limited security funding. "Our industry must now show trends and prove its value," said Ahrens. "It's about making informed decisions based on data."



EXAMPLES OF ROI

SIA has focused on demonstrating what we call the "Return on Security" through a series of events and webinars produced with members. Some examples that are already being seen in the industry include the following (not an exhaustive list, by any means):

- Heat mapping, customer flow, assessing customer density and queue lengths for retail-type environments
- Providing building usage stats through access control data (see also the Real Estate Reoptimization megatrend)
- Detecting illegal dumping
- Studying road traffic and using the data to create great transportation efficiency
- Validating employee working hours with badge entry scans
- Owner/managers using camera system to remotely view an office/store/facility to check operations or the presentability of the store
- Creating building efficiency by connecting lighting and HVAC controls with access control entry points and motion detection sensors

IMPACT ON THE SECURITY PRACTITIONER

If any trend on this list has strong impact to the security practitioner, it is this one. Historically, security practitioners were challenged to demonstrate value to the C-suite. They had to show that security investments were justified by correlating the reduction of costly security and safety incidents – the old pitch that "security shows its value when nothing (bad) happens." Security practitioners have always been heroes due to their focus on protecting people and assets, but now that security practitioners are able to show operational ROI that benefits other departments, the security practitioner has yet another opportunity to be a business hero.

MEGATREND 6

SAAS RESHAPES INTEGRATION BUSINESS MODEL

MEGATREND MOVEMENT

Security as a Service was ranked No. 7 in the 2023 Megatrends, and this Megatrend is an evolution of that trend, albeit more focused now on the changes of the integrator's business model. SaaS' rise in importance underscores the impact of this change, which is forcing business disruption among integrators and solutions developers.

With the market in a strong shift to cloud-based security as a service (SaaS) and managed services delivery models, this means sweeping changes for the business of integrators and for the industry as a whole. The primary "construction" model of building out hardware, wiring and on-premises solutions will yield steadily to a model in which security solutions are sold as subscriptions tied to business outcomes for the business client.

Integrators will need to rewrite their business models to incentivize delivery of these solutions, will need to rethink how they contract with their clients to create recurring revenue streams and will need to evaluate their role and who they will partner with for delivery of SaaS solutions, particularly for advanced AI solutions that are sold as a managed service model. And yes, the integrator will need to navigate this evolution while also still having to support legacy systems for some of their clients.

This change to cloud delivery of most services has already swept through the IT business world, and that change that IT value-added resellers (VARs) have already experienced serves as the template for change in the security solutions sector. In the IT VAR world, this has led to many VARs becoming tightly connected to just a couple vendor's offerings, almost becoming an extension of those vendors' ecosystems.

PRIMARY SUPPORT MODEL CHANGE

As security-as-a-service and AI offerings continue to rise in prominence, most integrators will feel the impact as the primary point of support moves away from the integrator and to the SaaS or AI provider. The solution provider will inevitably gain more direct contact with the customer, rather than always relying on the integrator as the first stop for support. Companies operating in the cloud space are now attaching that service/support to their subscriptions.

THE INTEGRATOR'S CORE VALUE

In the face of this shift to AI, SaaS and IoT offerings, integrators should recognize their strengths and play to these strengths.

First, despite sweeping technology shifts, integrators have real relationships with their clients and contacts and can position themselves in the consultative value of helping clients select among the major SaaS/AI/IoT service providers.

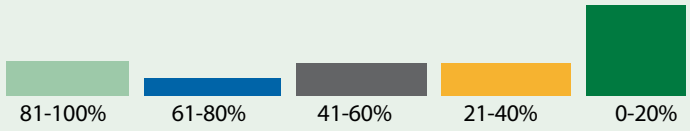
Secondly, integrators have thousands of trucks and field locations and can put people on ladders and can connect those IoT devices anywhere at any time, and that boots on the ground presence is something that even the largest cloud-service providers do not have and would have difficulty building at scale.

Third, there is sometimes a lack of understanding from AI and cloud providers in understanding the importance of the exacting demands of camera installation and configuration (pixels per foot, lighting, etc.) to make field deployment of these AI systems perfect. Integrators are uniquely equipped with this technical knowledge.

As nonsecurity use cases emerge in a connected world, and as cameras become visual intelligence solutions rather than video surveillance devices, there is likely no business type better positioned to usher in the delivery of these smart devices than the security integrator. This is a huge opportunity. Integrators have the opportunity to deliver value and grow as the market expands, but they also must be strongly prepared to sell nonsecurity use cases and sell business ROI of the solutions, rather than relying on selling devices as risk-reduction solutions.

CHANGE AHEAD

Approximately what percentage of your firm's revenues are based on recurring revenue service models?



"AI REPRESENTS A TREMENDOUS, LONG-TERM OPPORTUNITY FOR THE INTEGRATOR. THIS WILL BE A MACRO TECHNOLOGY REFRESH ACROSS SYSTEMS THAT WILL ULTIMATELY FAR EXCEED THE BUSINESS IMPACT THAT VIDEO EXPERIENCED IN THE MOVE FROM ANALOG TO IP. THE TECH STACK NECESSARY TO DELIVER AI ENABLED OUTCOMES IS FUNDAMENTALLY DIFFERENT THAN MANY TRADITIONAL SECURITY ARCHITECTURES. MANUFACTURES AND INTEGRATORS WHO EMBRACE INTELLIGENT EDGE DEVICES, CLOUD APPLICATIONS AND AUTOMATION WILL BE ABLE TO DELIVER NEW VALUE TO CUSTOMERS AND OUTPERFORM THEIR PEERS."

— ERIC YUNAG, VP OF INNOVATION, CONVERGINT

PICKING THE RIGHT PARTNER

As technologies have progressed, most integration business experts tend to agree: It's not practical or possible to support scores of different vendors' solution lines. Instead, integrators focused on excelling in the managed services business environment will need to become deeply invested in one or two vendors and their lines, truly becoming a partner in the delivery of those solutions set, rather than operating as a reseller and installer of many products.

This narrowing of focus will put a requirement on the integrator to pick the right SaaS or AI provider—one that will helps sustain their integration business. Integrators ready to make this shift will have to ask questions like:

- Does the solution provider have a strongly documented product/technology development road map to ensure continued relevance and market competitiveness?
- Does the solution provider treat integrators as partners rather than simply relying on an integrator as reseller and installer?
- Does the cloud solution provider allow the integrator to share in recurring revenue?
- Is there a model for the integrator to provide value-added services to the customer?
- Is the solution provider committed to leveraging integrators as part of their long-term business model?
- Is there value that you as the integrator can provide and monetize in the support, set up and performance measurement of AI-enabled and cloud systems?

As integrators ask questions like these, they will need to retain a strong focus on the sale of solutions that are margin accretive. Integrators need to focus on creating recurring revenue streams that have strong margins, versus relying on low-margin recurring revenue like hardware support that requires a truck roll expense.

MEGATREND 7

IMPACT OF THE MEGATECH COMPANIES

MEGATREND MOVEMENT

This trend is entirely new for the 2024 Megatrends report, but is introduced following significant megatech ecosystem changes that have facilitated the storage of government-issued IDs and building access privileges into the "wallet" systems of some of the top tech companies, and steady growth in partners for building access control.

According to estimates, there are nearly 1.5 billion iPhones in active use around the world today. And depending on the wildly different claims of market research firms, somewhere between 30% and 80% of Apple phone users in the U.S. are also actively using the Apple Watch. Google said in a 2022 blog post that there were over three billion active monthly Android devices and in 2021, they were said to have activated over a billion new Android phones. Meta has nearly 4 billion active users across its products (Facebook, Messenger, WhatsApp, Instagram). Microsoft has well over 300 million paid users of Office and is said to have over 1 billion people using its products or services worldwide. Amazon is said to have over 310 million customers around the world and is believed to have sold more than 4.1 billion items in 2022.

With those kind of numbers behind them, it's easy to understand how quickly these so-called megatech firms can disrupt entire industries overnight, and the security industry will not be ignored. From the enormous impact that Apple, Google and Samsung NFC and wallet type solutions can have on the door access sector to Amazon's ability to make instant waves with its Amazon One solution that uses palm vein biometrics for retail payments, entrance/access control and other identity-based applications.

The sheer active user bases of these megatech companies and their ability to deliver hardware and cloud solutions (often using the latest AI) immediately to a loyal userbase is what allows them to create incredible disruption.

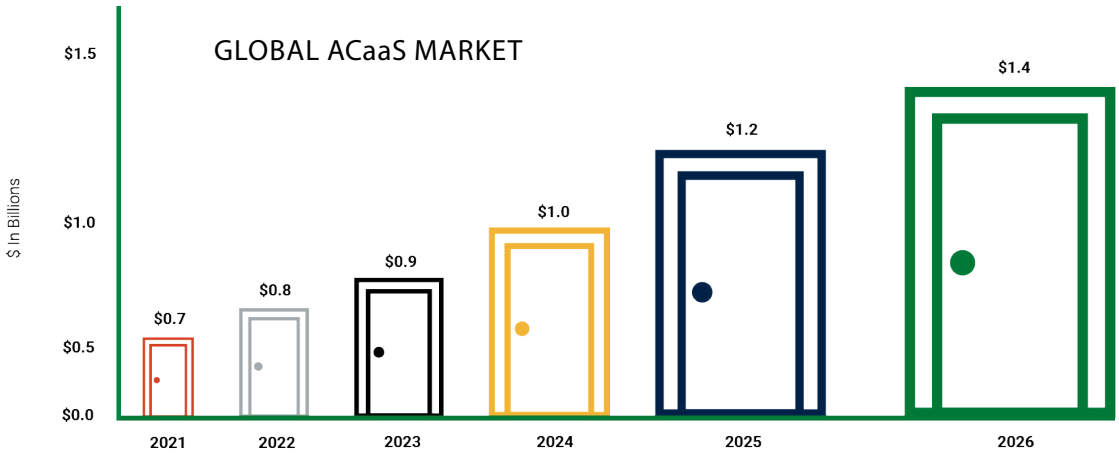
CHANGING USER EXPECTATIONS

The reality is that the megatech firms also have the ability to change user expectations. As Rob Lydic of Wavelynx points out, the user expectation we face today is that your average homeowner can go to Home Depot, pick out a high-quality smart lock, and within the hour, have the lock installed, WiFi connected, remote access enabled, iPhone or Android control enabled, access privileges configured and multiple users enrolled. The end user is expecting plug-and-play integration with minimal configuration effort and a really good user experience.

16%

Expected CAGR of the global ACaaS market between 2021 and 2026

Source: Omdia



"THE AMOUNT OF DISRUPTION POTENTIAL IS ASTOUNDING. APPLE AND GOOGLE WILL SHAKE THE CORE OF THE ACCESS CONTROL INDUSTRY IN THE VERY NEAR FUTURE. THEY CAN BECOME THE DEFAULT CREDENTIAL IN THE NEXT 18 MONTHS."

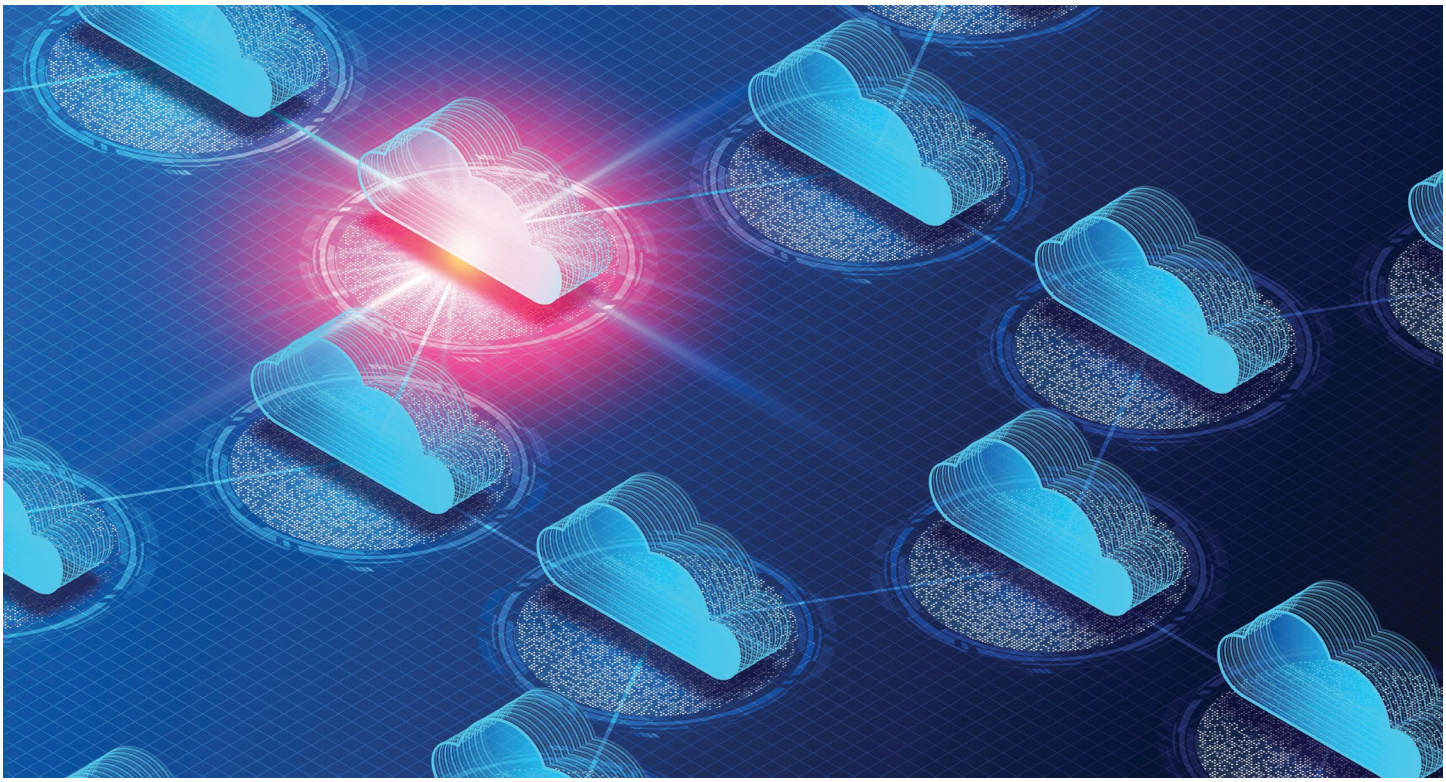
— ERIC YUNAG, VICE PRESIDENT OF TECHNOLOGY AND INNOVATION, CONVERGINT

IMPACT ON THE SECURITY PRACTITIONER

The megatech firms are raising the bar for the end users' customer experiences and are potentially making the integration of services/technologies more seamless for end users (just as has come to be expected in the world of consumer technology).

MEGATREND 8

MEGACLOUD CONSOLIDATION



MEGATREND MOVEMENT

While tangentially related to the megatrend of Security as a Service (ranked, No. 7 in 2023), this is truly a new Megatrend for the 2024 report.

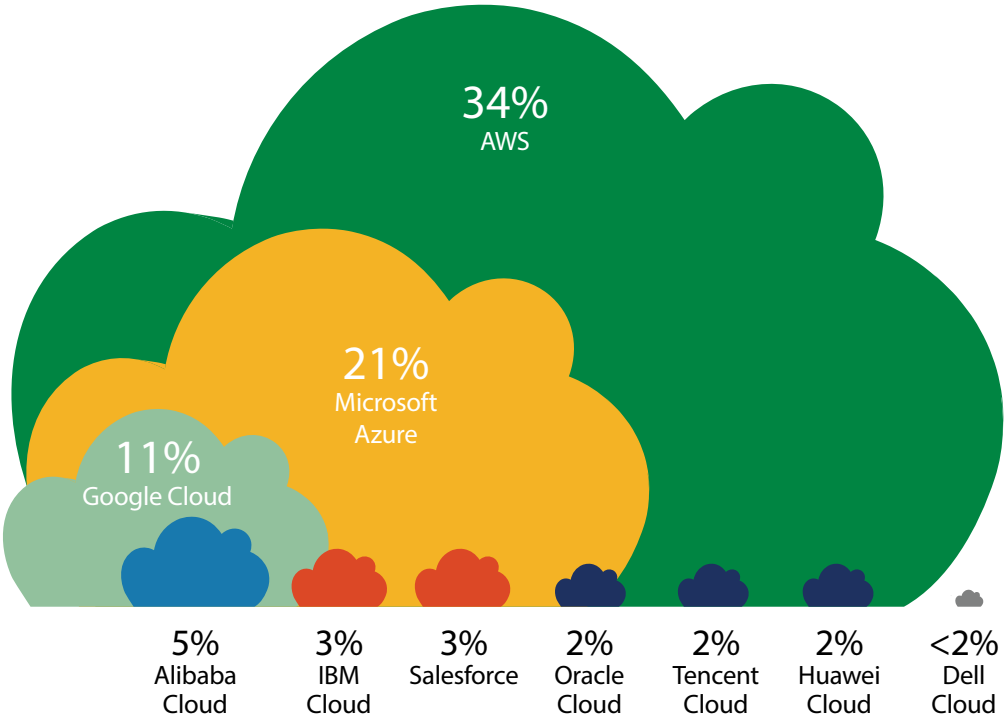
This trend reads like a riddle: It is a cloudy day, but there are only a few clouds in the sky.

This megatrend of cloud consolidation and the amassing of greater power and influence by the dominant cloud providers is closely related to Megatrend #7 and the Impact of the Megatech Companies. However, given our industry's move to security as a service, our advisors opinions and our survey results indicated it was worth calling out by itself.

Just a few companies dominate cloud hosting, creating a state of oligopoly Amazon Web Services (AWS), Google Cloud and Microsoft Azure together have two-thirds of the market). For many leaders who are thinking about the future of the security industry, that consolidation creates some unease. The cloud hosting providers continue to inject themselves more and more directly into the customer experience, rather than just being an invisible cloud back end. What we might think of as a major solution in our industry (like a combined security management access and video platform with good market share) is just a niche application to these companies with their billions of SaaS partners running on their clouds. Furthermore, as menus of services from these providers (like the AWS Service Catalog) grow, many executives are asking: Will these cloud companies continue to support you if your solution now competes with one of their services?

There are also concerns that some of your customers may have standardized on solutions running on one cloud provider, so if your cloud backbone is AWS based but your prospective client has standardized on Azure or GCP, you may be out of the running before you can even share the particular value that your SaaS solution delivers.

TOP 10 CLOUD PROVIDERS ESTIMATED MARKET SHARE



Source: Technology Magazine, 2023

PERSPECTIVE

The global security industry is in the midst of a profound transformation, transitioning from a hardware-centric model to a software-centric paradigm. With the emergence of cloud computing, mobile technology and artificial intelligence, the industry has evolved beyond its traditional role of providing safety and security. It has become an enterprise software industry that drives operational efficiencies and generates revenue on top of our core value proposition. This shift has attracted major players in the tech industry, such as Apple, Google, Microsoft and Amazon, who are disrupting established norms and introducing innovative concepts like Mobile Wallets, scaled credentialing and expansive ecosystems, which integrate our industry into a broader value proposition and in some cases, is making core disciplines of our industry a feature."

—Lee Odess, Access Control Executive Brief

"AS PUBLIC CLOUDS CONTINUE TO RAISE THEIR PRICES, YOU'LL SEE SKINNIER MARGINS."

—KEN FRANCIS, PRESIDENT, EAGLE EYE NETWORKS, AT SNG 2023

IMPACTS TO THE PRACTITIONER

While cloud consolidation and greater power amassing in the hands of the cloud providers may create unease for executives who are creating SaaS security solutions and for integrators who have to select their partners, for security practitioner teams, the near-term benefit is likely to be benefits of greater integration among SaaS services since the data from multiple systems could be living within just a couple cloud environments. It can also mean more consistent user experiences as SaaS developers build within these three dominant providers in the U.S.

As greater consolidation occurs, this could lead to more power for the dominant cloud companies to raise their prices. While higher cloud service pricing may first squeeze margins for the SaaS companies offering security as a service, eventually cost increases will find their way to the practitioner's desk, who will have few options to fight price increases, since all SaaS providers will be dependent on the same dominant cloud providers.

$597.3 B

Estimated spend in 2023 on all public cloud services

21.7%

Annual estimated growth in spending on those public cloud services in 2023

Source:: Gartner

MEGATREND 9

REAL ESTATE REOPTIMIZATION

MEGATREND MOVEMENT

The Proptech megatrend of 2022's report didn't make the top 10 cut in 2023 but was part of the "Elimination of the Industry's Boundaries" megatrend of 2023 (ranked No. 6). While this trend forecasts pain in this vertical sector, it also holds the promise of some new opportunities for vendors and integrators who can focus on connecting security to efficiency.

There's no denying it: 2023 was a challenging year for the commercial real estate market, particularly for office buildings. The work-from-home and partial mobile work policies meant office buildings continued to receive less usage than in prepandemic years. Meanwhile, interest rates increased steadily and didn't retreat significantly, even after the Federal Reserve stopped raising rates, and that meant office owners couldn't refinance out to lower rates to ease their debt burdens. Office-sharing company WeWork, which was once valued at nearly $50 billion, filed for bankruptcy in November 2023, and major landlords considered best of breed like Brookfield were even defaulting on select properties in key markets as they faced vacancies. Multifamily housing rent growth rates were slowing or plateauing, and commercial office space lease rates were dropping.

This is forcing landlords to reexamine technology expenditures and placing a cooling effect on what had been a very hot proptech market. This will lead to office-to-housing conversion projects and a focus on connecting building systems (including security) to generate operational efficiency—and this trend can create opportunities for the security industry.

"HOW WE USE SPACES IS ALREADY STARTING TO CHANGE AND WILL CONTINUE TO DO SO. MANY COMPANIES ARE FULLY REMOTE, AND OVER HALF OF THE POPULATION IS WORKING OUTSIDE THE OFFICE 50% OF THE TIME OR MORE. THERE'S A RETROFIT OPPORTUNITY TO TAKE THE SPACE A COMPANY HAS AND ADAPT IT TO THAT NEW MODEL LEVERAGING CLOUD AND MOBILE TECHNOLOGY"

JEFF STANEK, PRESIDENT, ACCESS SOLUTIONS, CARRIER FIRE & SECURITY

THE OPPORTUNITY FOR COMMERCIAL OFFICE ENVIRONMENTS

The continued low usage of office environments actually emphasizes the ROI of security (Megatrend No. 5) and gives a chance for solution providers and integrators serving these markets to actually demonstrate the insight value that "security" systems can generate. Commercial office owners/operators are being forced to "reposition" buildings to other uses as the demand (especially in major cities) decreases, which may bring some construction-related projects, such as conversion of office buildings into multifamily condo and apartment properties.

This low usage means it's time for landlords and property managers to double down on a building's operational efficiency. As Michael Wong of Genea shared in an example at CONSULT 2023, "With office buildings empty on Fridays, this is the perfect opportunity to use badge scans to trigger automated changes to HVAC." Salient Systems President Chris Meiter said building owners and their integrator and vendor partners will need to think creatively to identify new sources of operational efficiency. One example he suggested at SNG 2023 was that badge scans can indicate if certain spaces, like conference rooms or particularly low-usage office wings have even been accessed, and if not, property owners can trim costs by removing those spaces from daily cleaning services.

THE OPPORTUNITY FOR MULTIFAMILY PROPERTIES

Multifamily owners and operators are interested in capital expenditures that can generate higher rents and ROI. This includes IoT solutions (including security solutions like mobile-friendly entrance) and community WiFi solutions; both offerings create high ROI for the owner/operators while improving tenant experiences. A continued deficit of housing at the multifamily and single-family markets should continue to drive investments in smart home and automated security technologies.

IMPACT ON THE PRACTITIONER

Security end users should leverage any opportunity to tie in video, access and other sensor-driven systems to building lighting, HVAC and other systems. End users will want to constantly monitor access systems for data on building usage and have the opportunity to share this data with executives to help the business more efficiently apply its real estate assets to its current workforce.

Only 3%

Of New York office buildings would be viable for apartment conversions

Source: 2022 analysis by Moody's

5.75%

Share of office commercial mortgage-backed securities loans that are delinquent, a number which has tripled over the past year

Source: Real estate data provider service Trepp

MEGATREND 10

IT-OT CONVERGENCE

MEGATREND MOVEMENT

While closely related to 2023's No. 1 Megatrend of Cybersecurity for Physical Security, this path of convergence is nonetheless an entirely new megatrend for the 2024 report. It tied closely into megatrend No. 5, "1. Expansion & Evolution of Security's ROI," as this convergence of IT and OT trend is driven by the business need to extract more value from formerly isolated systems.

As information technology (IT) and operational technology (OT) systems rapidly converge, this means edge devices are no longer isolated and that OT systems, which were once truly standalone systems or platforms, are becoming integrated into a company's data environment. IT and OT silos were historically even more siloed than those of IT/cybersecurity and physical security, but those silos will be removed over time as the core business finds value in having these systems which make up the Industrial Internet of Things (IIoT) converged and correlated.

This convergence requires the creation of larger, more complex networks, and this increasing complexity means more risk (cyber and physical), and that means more opportunity for the security industry to provide value. Ransomware threats for these OT systems (like the Colonial Pipeline attack in May 2021) will become even more actionable and impactful.

STANDARDS NEEDED AS IT-OT CONVERGENCE OCCURS

For reasons of interoperability and cybersecurity, there will be an increased need for IT-OT convergence standards.

"I LIKE TO THINK OF IT AND OT AS A CULTURAL CONVERGENCE – BRINGING TOGETHER FORMERLY ISOLATED SYSTEMS AND USING COMMON IT PATHWAYS. OT SYSTEMS HAVE DIFFERENT REQUIREMENTS INCLUDING KPIS, USE CASES, FUNCTIONS AND MAY BE OLDER. SECURING THESE SYSTEMS CAN BE DONE, BUT IT'S WELL KNOWN THAT AGENCIES, ORGANIZATIONS HAVE NOT PRIORITIZED THE SECURITY OF OT DEVICES DUE TO COST, PEOPLE, PROCESS AND LACK OF UNDERSTANDING OF THE RISK."

— KASIA HANSON, MEGATRENDS ADVISOR, AND GLOBAL DIRECTOR, CYBER AND PHYSICAL SECURITY ECOSYSTEMS, INTEL CORPORATION

"THE LINES BETWEEN MASTER SYSTEMS INTEGRATORS AND SECURITY INTEGRATORS WILL CONTINUE TO BLUR. IN A TIGHT LABOR MARKET, NEW PARTNERSHIPS WILL EMERGE TO FILL THE IT AND OT REQUIREMENTS OF CONVERGED SOLUTIONS."

—TARA DUNNING, MEGATRENDS ADVISOR AND VICE PRESIDENT, GLOBAL SECURITY STRATEGY AND SALES, COMMUNICATIONS & SECURITY SOLUTIONS, WESCO

IMPACT ON THE INTEGRATOR

The integrator must support a holistic view of security. It isn't enough to secure the physical environment. From solution design and manufacturer selection to system architecture and the entire technology stack, as systems converge, the attack surface and need to defend IT and OT systems will simultaneously increase. Customers will learn about incredible integrations and AI solutions for powering their businesses into the future. Integrators should balance this excitement with the discipline of acting within ethical boundaries and putting cybersecurity first.

IMPACT TO THE PRACTITIONER

This convergence will change how you operate, because while the convergence generates increased productivity, it also creates greater exposure. Be prepared to respond to cybersecurity attacks on your own. As Brian Harrell said at SNG 2023, "The calvary is not coming to save you. If you think DHS CISA is going to save you from malware, ransomware or other threats, you're wrong. You need to be able to come back to homeostasis as quickly as you can."

To be prepared, develop an internal digital forensics team or a digital forensics skill set within your team so that you can respond to threats. And security practitioners and business leaders will need to force convergence among managers. IT and OT and corporate risk and security will need to have a daily briefing or similar type of regular information sharing session to ensure everyone is on the same page and working in the same direction.

MICRO TRENDS

TRENDS ON OUR RADAR, BOUND TO IMPACT BUSINESS OPERATIONS AND SECURITY PROGRAMS

AUTONOMOUS DEVICES

Autonomous mechanical devices—think robotics and drones—were ranked as ninth on the list of the 2023 SIA Security Megatrends, but in 2024 there was more hesitancy among respondents in the promotion of these technologies. Most survey respondents indicated that there would be steady growth of autonomous devices. Keep an eye on this space as federal rules change that would affect drones and as the robotics solution providers adopt even more sensors and allow these solutions to be even more autonomous than they currently are. Guarding is, after all, a multibillion-dollar industry that has seen only relatively minor adoption of technology, and a key theme captured in the annual Security Megatrends survey of 100+ industry executives is that the guarding industry is one of the areas most likely to face disruption in the coming years. In addition to applying autonomous devices, the industry is facing the issue of drone threats, and SIA has responded with the formation of a Counter UAS Working Group that is focused on the legislative/regulatory environment for C-UAS.

QUANTUM COMPUTING AND POSTQUANTUM CRYPTOGRAPHY

Quantum computing is beyond binary computing and uses "qubits" rather than regular bits of 1s and 0s. Once this computing power comes to fruition, it could solve data problems nearly instantly that would take today's most powerful computers years, even decades to solve. And one of those problems would be cracking keys and passwords that protect systems of all kinds. Today, the world's leading nations and top tech companies are all in a race to develop quantum computing, and organizations like the National Institute of Standards and Technology are tasked with developing "postquantum" cryptography standards—generating a new breed of cryptographic algorithms that would be resistant to quantum computing.

ELIMINATION OR REDUCTION OF PHYSICAL CREDENTIALS

With major tech players like Apple getting more serious about interfacing with physical security access control, and with many university campuses now rolling out or doing significant pilot projects for phone-based access control, key cards, fobs and other physical credentials are on a path for eventual reduction, if not full elimination at some end-user sites.

EXECUTIVE TAKEAWAYS

A COLLECTION OF QUOTES FROM SNG 2023, MEGATRENDS INTERVIEWS, FOCUS GROUPS AND NEWS MEDIA COVERAGE, FROM INDUSTRY THOUGHT LEADERS ON TOPICS RELEVANT TO THE 2024 SECURITY MEGATRENDS

"Supply chain awareness is growing and has a prominence in the C-suite that it never had before. Companies are looking at it in a different way, and that focus will be a driver."

— Bill Geary, EVP and GM, Communications and Security Solutions, Wesco

"We couldn't succeed as a monitoring company without AI."

—Kurt Takahashi, CEO, Netwatch Group

"The proliferation of sensors of all types is creating an avalanche of data. A wealth of data and a poverty of attention. AI shines at pulling insights out of massive amounts of data."

—Hamish Dobson, CVP, Product - Enterprise Physical Security Solutions, Motorola Solutions

"We're seeing a fundamental lack of skills and training in the marketplace, so we're doing apprenticeship and career development programs to address that."

—Julaine Simmons, VP of Security & Electronic Systems, M.C. Dean Inc.

"We will always be lagging behind the speed of technology."

—Svenja Hahn, member of the European Parliament in writing the EU's A.I. act, as quoted in The New York Times

"AI has helped us create a massive amount of event data. We know when the door open alert comes through. It's not that we more data. We still need to integrate this data with different systems."

—ONVIF Chair Leo Levit, on the continued need to integrate data from disparate IoT devices and management systems

8455 Colesville Rd.
Suite 1200
Silver Spring, MD 20910
301-804-4700
securityindustry.org