SIA EDUCATION at ISC

Security Practitioners & The Megatrends: What Trends Are Most Impacting Corporate Security Leaders

Geoff Kohl, Security Industry Association (SIA)

Eric Yunag, Convergint

Steve Van Till, Brivo

Tara Dunning, Wesco

Devin Love, Allegion

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

SIA EDUCATION at ISC

Geoff Kohl

Security Industry Association (SIA)

Bill Inzeo

Sr. Director, Security Standards & Technology

Salesforce

Gary Lunetta

Director, Physical Security Technology

Salesforce

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

SECURITY INDUSTRY ASSOCIATION

Information. Insight. Influence.

SPARC

SIA's Technical Practitioner Community

SECURITY INDUSTRY ASSOCIATION

Information. Insight. Influence.

Report Download:
securityindustry.org

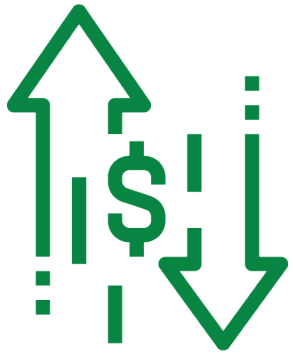
About the Security Megatrends

- The 10 industry-shaping trends
- First Edition: 2017
- Released annually by SIA at Imperial Capital SIC
- Based on extensive surveys, focus groups, SNG content, and input from advisors
- Designed to look out at least 3-5 years but will also recognize megatrends with immediate impact
- Presented at Securing New Ground, ISC West and major events

Foundational Trends

CYBERSECURITY

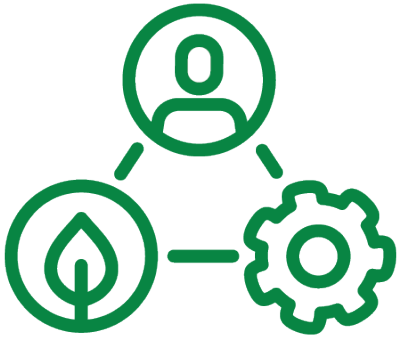
GLOBAL TENSIONS



CHANGING ECONOMIC CONDITIONS

CLOUD MODEL FOR TECHNOLOGY DELIVERY

WORKFORCE DEVELOPMENT

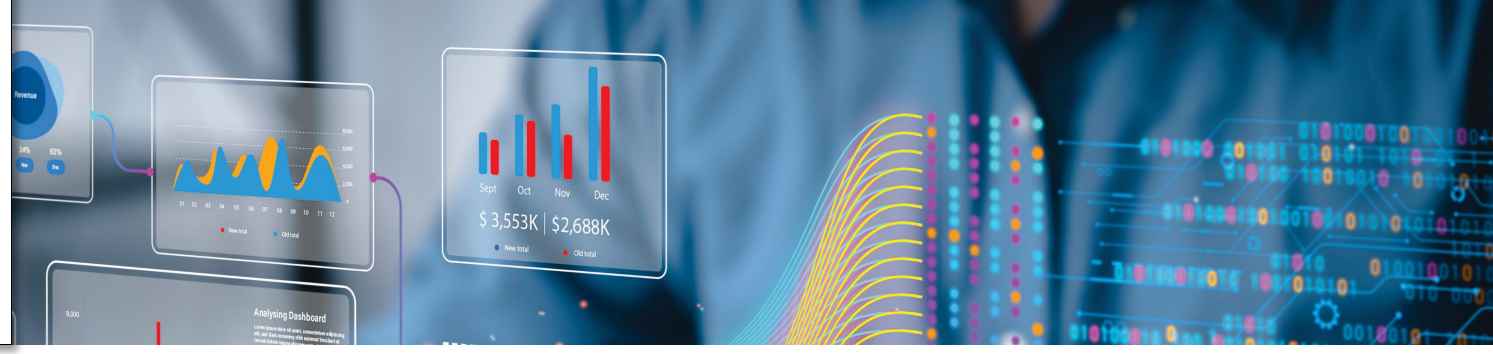


SUSTAINABILITY

SUPPLY CHAIN ASSURANCE

2025 SECURITY MEGATRENDS™

THE ANNUAL VISION FOR THE SECURITY INDUSTRY



1. Evolution of the Channel
2. AI: Intelligent Automation of Security
3. Correcting the Systemic Undervaluation of Security
4. Visual Intelligence, Not Video Surveillance
5. IT-OT Security Convergence
6. Platform Aggregation
7. Democratization of Identity and Mobile Credentials
8. Growth of Advanced Detection Technologies
9. Shift of Influence from Hardware to Software
10. SaaS, HaaS, DaaS and a Managed Services Future

MEGATREND 1

EVOLUTION OF THE CHANNEL

MEGATREND MOVEMENT

In both the Security Megatrends survey data and focus groups, there was no more important trend than the evolution of the channel, and it merged in and expanded beyond the 2024 Megatrend "SaaS Reshapes Integration Business Model" (ranked No. 6 in 2024).

Artificial intelligence (AI), cloud, technology upheaval, razor thin margins, new competitors, changing requirements of end users: They're all converging to create the most challenging wave of change the channel has ever seen, felt primarily in the systems integration channel.

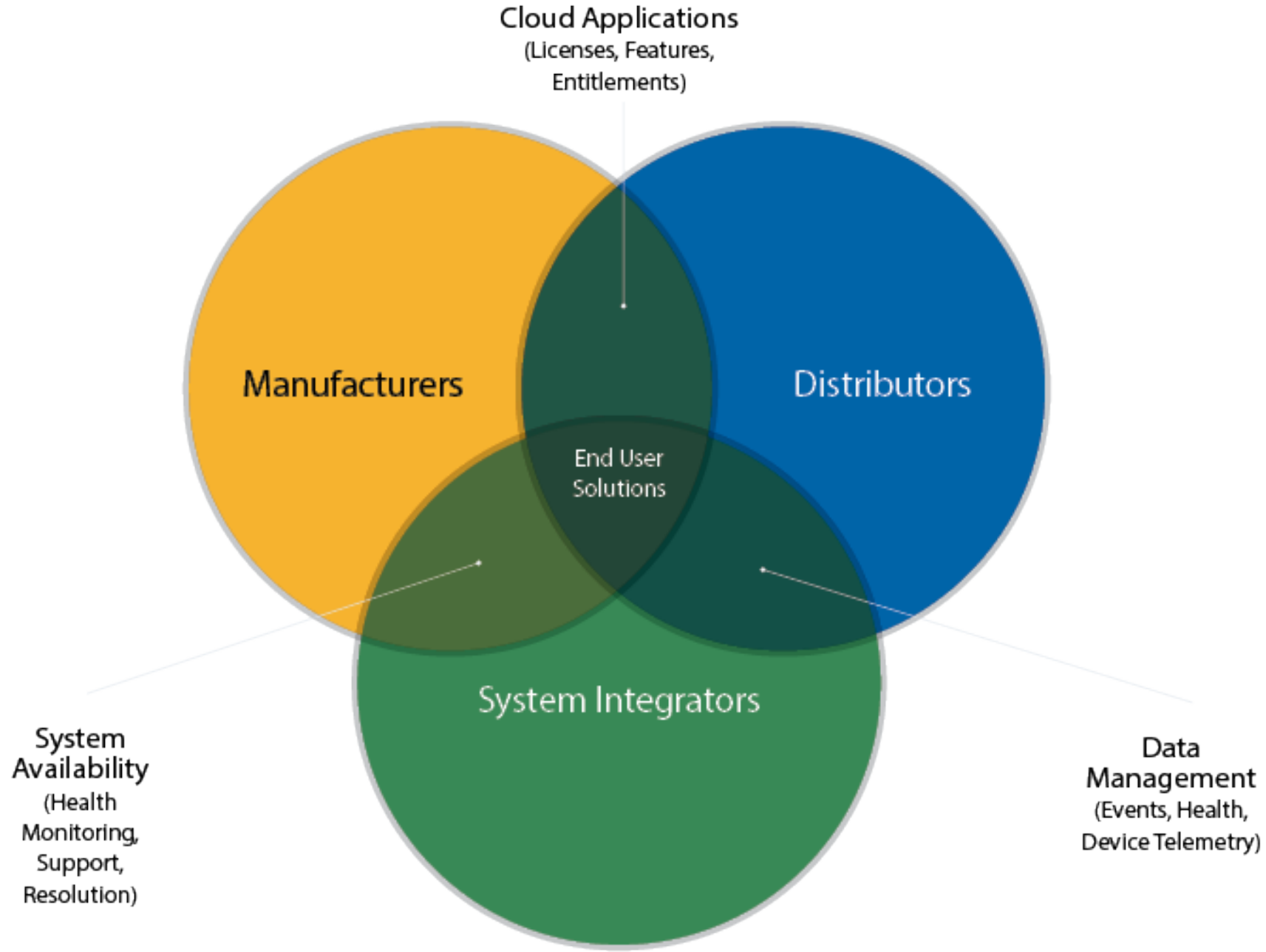
The first challenge is the delivery model. As security devices become both more advanced and less expensive, system developers and providers are more often adopting a "direct to end user" model of sales. What's more, these security as a service (SaaS) models that often accompany such AI enabled systems often do not connect the integrator to the recurring revenue stream, and that creates revenue problems for the integrator, says Bill Bozeman, a Megatrends advisor and chair of SIA's AI Advisory Board. Bozeman emphasizes that

"We have lived in a relatively static world where the risks were redefined periodically and the technology moved relatively slowly. That is just not the case anymore. We are now required to deliver solutions differently and respond more dynamically to evolving risks. We must be able to put solutions in place, leverage these emerging technologies quickly to address these risks and respond to the threats and incidents that occur in the environments that we all work to protect."

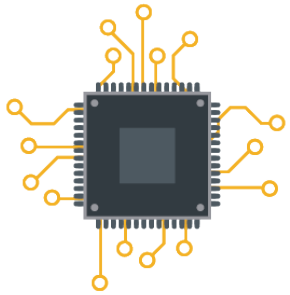
– ERIC YUNAG, EXECUTIVE VICE PRESIDENT OF PRODUCTS AND SERVICES, CONVERGINT, AT SECURING NEW GROUND (SNG) 2024

Key Takeaways:

1. **Evolving and Converging Roles: Manufacturers, Distributors, Integrators**
2. **Competition for Customer Ownership**
3. **Changing Demands from End Users**
4. **Technology Modernization Contributing to Evolution**


Cloud Applications
(Licenses, Features, Entitlements)
Manufacturers
Distributors
End User Solutions
System Integrators
System Availability
(Health Monitoring, Support, Resolution)
Data Management
(Events, Health, Device Telemetry)

Trends Impacting the Channel



Technology Modernization

- Move to cloud/SaaS
- Internet of Things (IoT) architectures
- AI/machine learning
- Enterprise software
- Data convergence

End-User Requirements

- Enhanced stakeholder expectations
- Dynamic and evolving risks
- Access to funding/return on investment (ROI)
- Beyond security use cases
- Access to skills and expertise

Market Dynamics

- Workforce challenges
- Shift to service models
- Globalization
- Supply chain resilience
- Compliance

MEGATREND 1

EVOLUTION OF THE CHANNEL

MEGATREND MOVEMENT

In both the Security Megatrends survey data and focus groups, there was no more important trend than the evolution of the channel, and it merged in and expanded beyond the 2024 Megatrend "SaaS Reshapes Integration Business Model" (ranked No. 6 in 2024).

Artificial intelligence (AI), cloud, technology upheaval, razor thin margins, new competitors, changing requirements of end users: They're all converging to create the most challenging wave of change the channel has ever seen, felt primarily in the systems integration channel.

The first challenge is the delivery model. As security devices become both more advanced and less expensive, system developers and providers are more often adopting a "direct to end user" model of sales. What's more, these security as a service (SaaS) models that often accompany such AI enabled systems often do not connect the integrator to the recurring revenue stream, and that creates revenue problems for the integrator, says Bill Bozeman, a Megatrends advisor and chair of SIA's AI Advisory Board. Bozeman emphasizes that

"We have lived in a relatively static world where the risks were redefined periodically and the technology moved relatively slowly. That is just not the case anymore. We are now required to deliver solutions differently and respond more dynamically to evolving risks. We must be able to put solutions in place, leverage these emerging technologies quickly to address these risks and respond to the threats and incidents that occur in the environments that we all work to protect."

– ERIC YUNAG, EXECUTIVE VICE PRESIDENT OF PRODUCTS AND SERVICES, CONVERGINT, AT SECURING NEW GROUND (SNG) 2024

Questions:

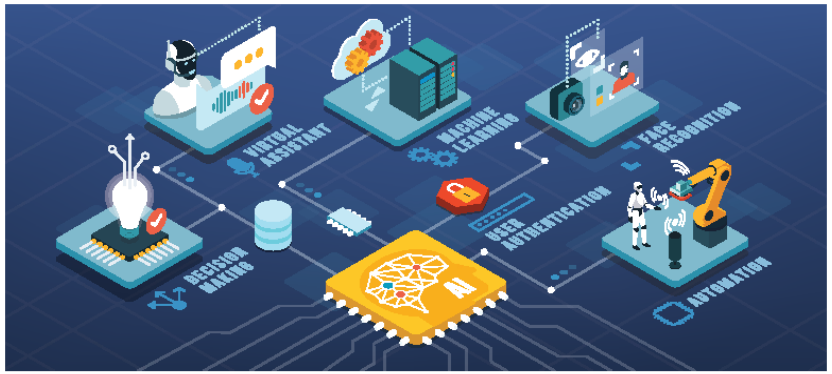
What do you need more of from the channel in terms of ideas, support and service?

How have your channel partners adapted to better serve your needs?

What are existing frustrations you have with the channel?

MEGATREND 2

AI: INTELLIGENT AUTOMATION OF SECURITY



MEGATREND MOVEMENT

After sweeping the top four Megatrends in the 2024 report, AI risked being overhyped. It was reassimilated to a single ranking, only edged out of the top position by the massive upheaval being felt by security integrators and other aspects of the channel.

Artificial intelligence, in spite of the risk of being overhyped by marketers, remains among the top drivers of the security industry's future.

The consistent feedback from our Security Megatrends focus groups and in our survey completed by industry executives indicates that the greatest desires of AI for our industry are:

- Create more efficiency in security operations
- Create actionable insights from the proliferation of sensor data and other data that is fed to security
- Be able to automate previously onerous security processes

Thus, in the coming years we believe that a more cautious optimism for AI in the security industry won't be the application of general intelligence that replaces a human, but will be in its ability to intelligently automate repetitive business and security processes, allowing humans to do more in less time and with the right insights at their fingertips.

As Axis Communications' Fredrik Nilsson noted at the 2024 SNG conference, approximately 80% of the spend on security today is in manual labor, while in most other high tech industries the labor costs are around 50%. "AI is the holy grail to capture that value with technology instead of manual labor," espoused Nilsson.

"AI brings us to the next level. Not only do I see the door is open, but I also see if someone came in when they shouldn't have, so we get more value out of that. Instead of making the PACS system the centerpiece to our stack, perhaps we should review and see if AI should be the centerpiece to our stack."

– PHIL JANG, CONVERGED SECURITY LEADER, TIKTOK USDS

Key Takeaways:

1. Create more efficiency in security operations
2. Create actionable insight from proliferation of sensor data and other security or operational information
3. Automate previously onerous security practices

80%

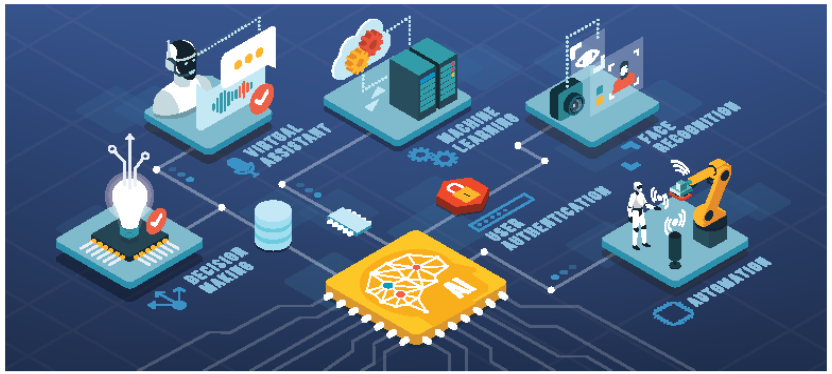
of the spend on security today is manual labor

50%

typical amount spent on labor in most other high-tech industries

MEGATREND 2

AI: INTELLIGENT AUTOMATION OF SECURITY



MEGATREND MOVEMENT

After sweeping the top four Megatrends in the 2024 report, AI risked being overhyped. It was reassimilated to a single ranking, only edged out of the top position by the massive upheaval being felt by security integrators and other aspects of the channel.

Artificial intelligence, in spite of the risk of being overhyped by marketers, remains among the top drivers of the security industry's future.

The consistent feedback from our Security Megatrends focus groups and in our survey completed by industry executives indicates that the greatest desires of AI for our industry are:

- Create more efficiency in security operations
- Create actionable insights from the proliferation of sensor data and other data that is fed to security
- Be able to automate previously onerous security processes

Thus, in the coming years we believe that a more cautious optimism for AI in the security industry won't be the application of general intelligence that replaces a human, but will be in its ability to intelligently automate repetitive business and security processes, allowing humans to do more in less time and with the right insights at their fingertips.

As Axis Communications' Fredrik Nilsson noted at the 2024 SNG conference, approximately 80% of the spend on security today is in manual labor, while in most other high tech industries the labor costs are around 50%. "AI is the holy grail to capture that value with technology instead of manual labor," espoused Nilsson.

"AI brings us to the next level. Not only do I see the door is open, but I also see if someone came in when they shouldn't have, so we get more value out of that. Instead of making the PACS system the centerpiece to our stack, perhaps we should review and see if AI should be the centerpiece to our stack."

– PHIL JANG, CONVERGED SECURITY LEADER, TIKTOK USDS

Questions:

What are pain points you feel that need automation?

How is your business generally applying automation or AI outside of the security domain and what lessons can we draw from those applications?

Beyond security, how are you using AI to make your security team more efficient?

MEGATREND 3

CORRECTING THE SYSTEMIC UNDERVALUATION OF SECURITY

MEGATREND MOVEMENT

In the 2024 Security Megatrends, "Expansion and Evolution of Security's ROI" was ranked No. 3. This new megatrend presupposes that security does show ROI, and given the real value security provides (including nontraditional value) the cost for security is systemically undervalued.

This Security Megatrend starts with the single belief that a business' workforce and workplace must be safe before it can be productive. There is a "duty of care" that an organization owes its employees. As the law firm Thompson Solicitors writes in its summary of this topic: "Employers have a duty of care to their employees. It is a legal requirement for employers to take reasonable steps to keep their employees as safe as possible at work. Appropriate and reasonable health and safety measures should be put in place to prevent employees from becoming ill or injured."

While there is no legal requirement that a firm must make money or that it must have the best performing business tools, there truly is an expectation to keep employees safe, so why then is security always looked upon as a place to apply cost savings and generally a cost to minimize?

Today's security teams and security systems don't just provide the duty of care for employees – the technology systems can actually be used to provide business insights like office occupancy, retail queue delays, video confirmation of vendor services and deliveries, remote verification of operations and more.

With these additional use cases, modern software platforms are getting closer and closer to the center of the enterprise in terms of operational outcomes – and thus can be seen by the end user as more like enterprise software that underpins the business.

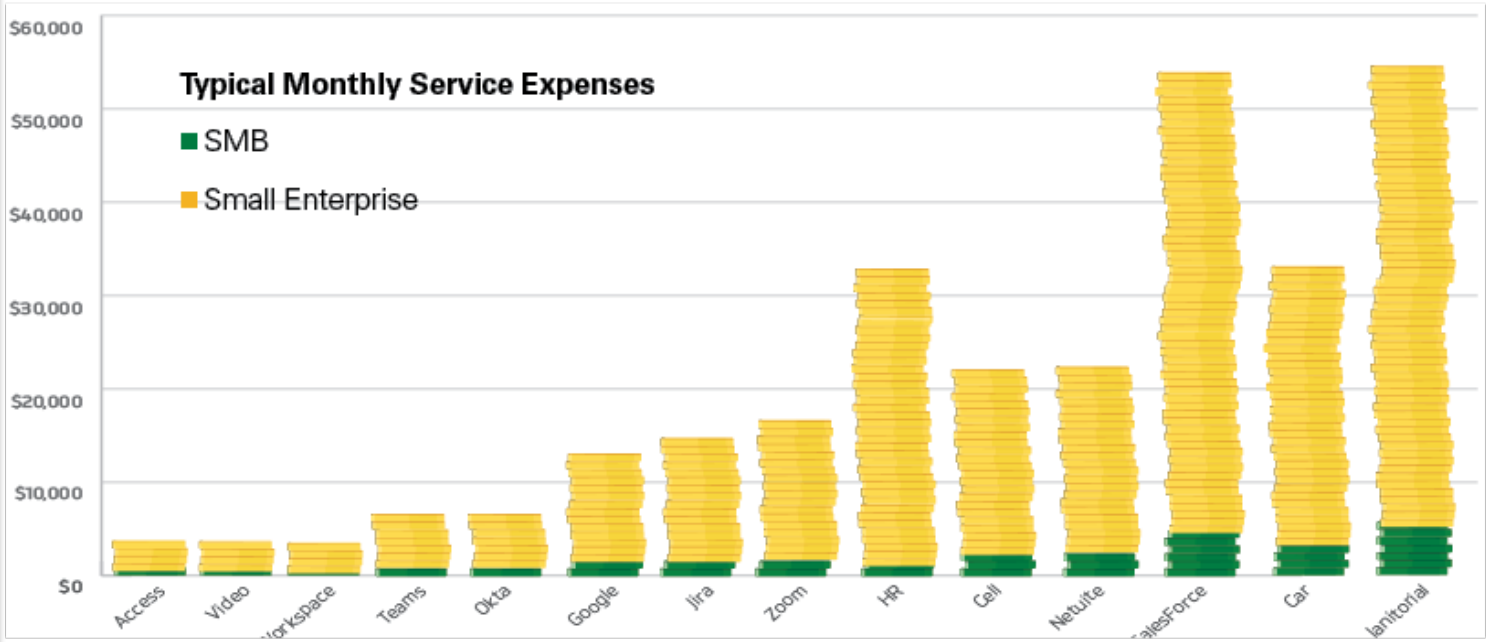
Yet when comparing the typical expense profile of our industry's systems to what is thought of as traditional business enterprise wide systems and monthly cost centers like employee communications (e.g., Teams or Zoom), employee project management (e.g., Slack), customer relationship management (CRM) platforms, video conferencing or employee cellular communications, it is clear that our cost to the business is dramatically less than that of systems that show comparative value.

"We have to sell our value and create value – and the cost of not doing so is catastrophic"

–TARA DUNNING, VICE PRESIDENT OF GLOBAL SECURITY & INFRASTRUCTURE, WESCO

Key Takeaways:

1. Value of security not fully recognized by business leaders
2. Security leaders challenged to "prove the negative" must flip the script and demonstrate ROI



MEGATREND 3

CORRECTING THE SYSTEMIC UNDERVALUATION OF SECURITY

MEGATREND MOVEMENT

In the 2024 Security Megatrends, "Expansion and Evolution of Security's ROI" was ranked No. 3. This new megatrend presupposes that security does show ROI, and given the real value security provides (including nontraditional value) the cost for security is systemically undervalued.

This Security Megatrend starts with the single belief that a business' workforce and workplace must be safe before it can be productive. There is a "duty of care" that an organization owes its employees. As the law firm Thompson Solicitors writes in its summary of this topic: "Employers have a duty of care to their employees. It is a legal requirement for employers to take reasonable steps to keep their employees as safe as possible at work. Appropriate and reasonable health and safety measures should be put in place to prevent employees from becoming ill or injured."

While there is no legal requirement that a firm must make money or that it must have the best performing business tools, there truly is an expectation to keep employees safe, so why then is security always looked upon as a place to apply cost savings and generally a cost to minimize?

Today's security teams and security systems don't just provide the duty of care for employees – the technology systems can actually be used to provide business insights like office occupancy, retail queue delays, video confirmation of vendor services and deliveries, remote verification of operations and more.

With these additional use cases, modern software platforms are getting closer and closer to the center of the enterprise in terms of operational outcomes – and thus can be seen by the end user as more like enterprise software that underpins the business.

Yet when comparing the typical expense profile of our industry's systems to what is thought of as traditional business enterprise wide systems and monthly cost centers like employee communications (e.g., Teams or Zoom), employee project management (e.g., Slack), customer relationship management (CRM) platforms, video conferencing or employee cellular communications, it is clear that our cost to the business is dramatically less than that of systems that show comparative value.

"We have to sell our value and create value – and the cost of not doing so is catastrophic"

–TARA DUNNING, VICE PRESIDENT OF GLOBAL SECURITY & INFRASTRUCTURE, WESCO

Questions:

How are you flipping the script and finding operational benefits from your security investments?

How are you justifying the value of security differently today?

MEGATREND 4

VISUAL INTELLIGENCE, NOT VIDEO SURVEILLANCE

MEGATREND MOVEMENT

Ranked second in our 2024 Megatrends report, this trend dropped two ranking spots in 2025 but remains one of the most important trends based on survey data and will undoubtedly remain a long-term trend guiding the security industry.

Of the estimated over 90 million cameras installed globally, very few use AI, but that is changing. If you further divide those 90 million cameras, a low percentage are using standard analytics (be that in the camera or the video management system [VMS]) and even fewer are using what you might call "real AI." Simply put, most existing security cameras are still functioning as simple scene recording devices and are not yet providing the "visual intelligence" that this trend conveys.

But all of that is about to change. Practitioners today are looking at their video surveillance investments as tools to provide visual oversights of their operations, and that makes this trend inherently connected to 2025 Megatrend No. 3, the undervaluation of security. After all, if your security cameras are no longer "video surveillance" but provide "visual intelligence," those systems are worth more to the business.

Of course, providing these additional values requires AI or at least "analytics," and this creates a huge opportunity for video product makers, VMS vendors and systems integrators

"There's more opportunity for cameras to become a source of data for our organizations than there ever has been. This allows us to put more infrastructure in, do a better job securing our environment, but also deliver other use cases—energy efficiency and savings, maintenance savings, space optimization, productivity and user experience—in addition to security, safety and compliance."

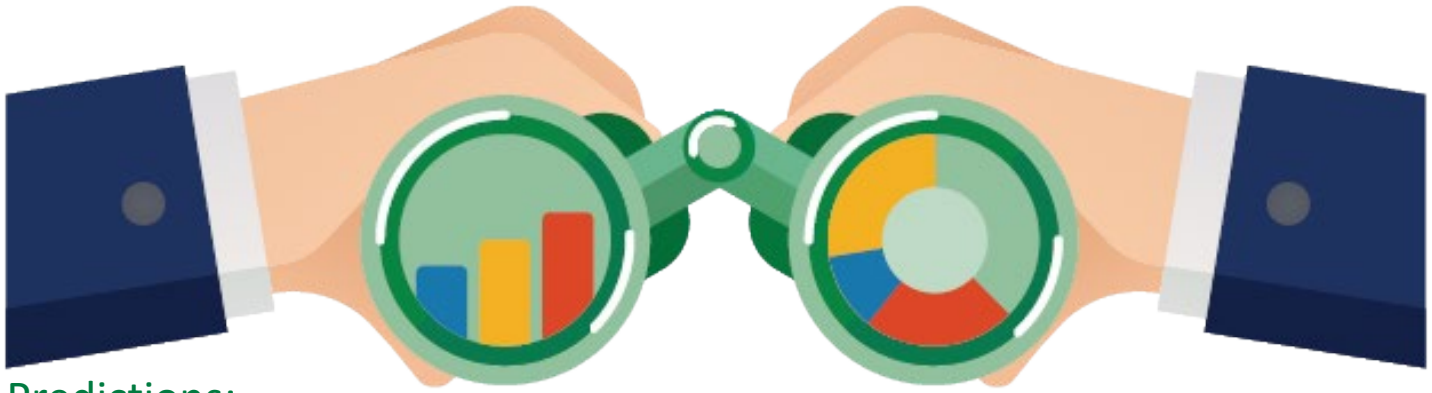
– ERIC YUNAG, EVP, PRODUCTS AND SERVICES, CONVERGINT

"Because of the power of technology, we're able to drive business value in other areas. Customers do integrations through our APIs and use the cameras through new ways they hadn't thought of before."

– FILIP KALISZAN, CEO, VERKADA

Key Takeaways:

1. **Video today still largely not AI-enabled, but technology refresh cycles will change that status**
2. **Cameras are the ultimate sensor and a platform for "sensorization"**
3. **Business insights from video investments**



Predictions:

1. AI will allow **deep search of recorded content**.
2. Future of video **is all content analyzed in real-time**.
3. Video operational ownership will **not be exclusive to the security team**.
4. **Justifications for investments** in video technology become easier.

MEGATREND 4

VISUAL INTELLIGENCE, NOT VIDEO SURVEILLANCE

MEGATREND MOVEMENT

Ranked second in our 2024 Megatrends report, this trend dropped two ranking spots in 2025 but remains one of the most important trends based on survey data and will undoubtedly remain a long-term trend guiding the security industry.

Of the estimated over 90 million cameras installed globally, very few use AI, but that is changing. If you further divide those 90 million cameras, a low percentage are using standard analytics (be that in the camera or the video management system [VMS]) and even fewer are using what you might call "real AI." Simply put, most existing security cameras are still functioning as simple scene recording devices and are not yet providing the "visual intelligence" that this trend conveys.

But all of that is about to change. Practitioners today are looking at their video surveillance investments as tools to provide visual oversights of their operations, and that makes this trend inherently connected to 2025 Megatrend No. 3, the undervaluation of security. After all, if your security cameras are no longer "video surveillance" but provide "visual intelligence," those systems are worth more to the business.

Of course, providing these additional values requires AI or at least "analytics," and this creates a huge opportunity for video product makers, VMS vendors and systems integrators

"There's more opportunity for cameras to become a source of data for our organizations than there ever has been. This allows us to put more infrastructure in, do a better job securing our environment, but also deliver other use cases—energy efficiency and savings, maintenance savings, space optimization, productivity and user experience—in addition to security, safety and compliance."

– ERIC YUNAG, EVP, PRODUCTS AND SERVICES, CONVERGINT

"Because of the power of technology, we're able to drive business value in other areas. Customers do integrations through our APIs and use the cameras through new ways they hadn't thought of before."

– FILIP KALISZAN, CEO, VERKADA

Questions:

How are you utilizing video today (or how do you envision you will use video differently) beyond classic "security camera" applications of the past?

As video's domain expands beyond security, what challenges do you have in managing access to video assets/data?

Same questions: Access Control

MEGATREND 6

PLATFORM AGGREGATION

MEGATREND MOVEMENT

Platform aggregation was a new trend concept introduced by the 2025 Megatrend advisors and received a strong response from survey respondents following its presentation at SNG 2024 by Megatrends Advisor Tara Dunning. This new Megatrend connects back to "Proliferation of Sensors" (a 2023 Megatrend), as the explosion of security data from those sensors and the explosion in the number of software platforms used today by security and facilities has created challenges in understanding security and facility trends.

The ability to create new solutions, devices and systems is inspiring, and today there seems to be a system for everything. Operational, facility and security leaders have data coming in from everywhere, and if they are ahead of the curve, they have followed the playbook outlined in Megatrend No. 5, "IT OT Security Convergence."

But today, even if they have started down that convergence path, the most likely result is direct integration between systems and not a holistic integration of all systems. And even if the number of systems integrated is substantial, the integration of systems is not convergence and is just one step along that path. Moreover, these systems weren't all purchased from the same vendors, weren't guaranteed to be interoperable and certainly weren't purchased at the same time with a clear strategy for linking the data, so users will find functional limits to the number of system to system integrations that can be done.

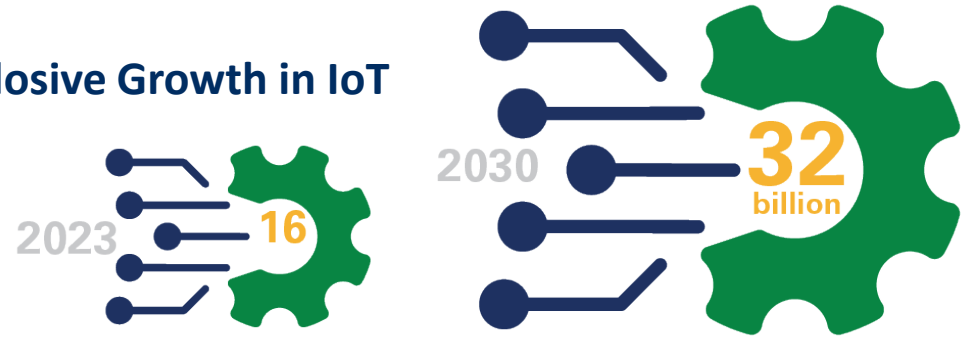
The answer for many is platform aggregation, an emerging trend likely to shape our industry's future, particularly for high demand, complex end users.

Some may call the end result a "single pane of glass," but the real metaphor may be something more like a hologram, such that all leaders are looking at the same picture but are receiving different visions of multidimensional data, tailored upon their perspectives and needs.

Key Takeaways:

1. Practitioners/businesses overwhelmed with data as IoT device numbers explode
2. Today: visualization/dashboarding; future of "aggregation" is likely to be the application of an AI layer to aggregated information
3. Driven by smart building sector
4. Evolution of VMS companies into platform providers

Explosive Growth in IoT



MEGATREND 6

PLATFORM AGGREGATION

MEGATREND MOVEMENT

Platform aggregation was a new trend concept introduced by the 2025 Megatrend advisors and received a strong response from survey respondents following its presentation at SNG 2024 by Megatrends Advisor Tara Dunning. This new Megatrend connects back to "Proliferation of Sensors" (a 2023 Megatrend), as the explosion of security data from those sensors and the explosion in the number of software platforms used today by security and facilities has created challenges in understanding security and facility trends.

The ability to create new solutions, devices and systems is inspiring, and today there seems to be a system for everything. Operational, facility and security leaders have data coming in from everywhere, and if they are ahead of the curve, they have followed the playbook outlined in Megatrend No. 5, "IT OT Security Convergence."

But today, even if they have started down that convergence path, the most likely result is direct integration between systems and not a holistic integration of all systems. And even if the number of systems integrated is substantial, the integration of systems is not convergence and is just one step along that path. Moreover, these systems weren't all purchased from the same vendors, weren't guaranteed to be interoperable and certainly weren't purchased at the same time with a clear strategy for linking the data, so users will find functional limits to the number of system to system integrations that can be done.

The answer for many is platform aggregation, an emerging trend likely to shape our industry's future, particularly for high demand, complex end users.

Some may call the end result a "single pane of glass," but the real metaphor may be something more like a hologram, such that all leaders are looking at the same picture but are receiving different visions of multidimensional data, tailored upon their perspectives and needs.

Questions:

What are your paint points in terms of getting a full understanding of the data you have coming in from different aspects of your security program?

MEGATREND 7

DEMOCRATIZATION OF IDENTITY AND MOBILE CREDENTIALS

MEGATREND MOVEMENT

Recognized as an emerging microtrend in our 2024 report ("Elimination or Reduction of Physical Credentials"), this trend has grown by leaps and bounds in the past 12 months, earning it a definitive spot in the Megatrends and aligning with the past year's Megatrend of "Impact of the Megatech Companies" (trend No. 7 in 2024).

The badge office—ostensibly positioned as the purveyor and provider of identity cards—is ripe for disruption. The oversimplification of what most badge offices do is transform physical keys into plastic keys that can be assigned to an individual. Certainly, there is great convenience with the card or fob. Unlike the metal keys they replaced, the card could be disabled if lost or stolen, and in the lanyard worn form factor, it could combine visual verification with door access. But there are obvious security weaknesses that are retained. The key card can easily be handed off to another user, much like a physical key, or worse yet, some cards could be cloned surreptitiously.

The future direction is to move into one of two form factors:

- Biometric based identity
- Mobile credentials that leverage phones and wearables to deliver the credential or identity authentication

"The history of identity has largely been driven by the physical space, through the state bureau (DMV) that produces a document that's not secure [and which] doesn't allow transactions to happen in a risk-free posture. More and more, those things [secure transactions] are expected to occur on our phones. The real promise of this is being able to know who's on the other side of the computer screen – to drive down fraud and abuse."

– DONNIE SCOTT, CEO, IDEMIA, AT SNG 2024

Key Takeaways:

1. Emerging form factors: 1) biometric, 2) credentials/phone
2. Cost of badges not being fairly compared to the cost of mobile credentials
3. Competition for dominance: credential issuers, wallet platforms, middleware companies
4. Clear need for standards

MEGATREND 7

DEMOCRATIZATION OF IDENTITY AND MOBILE CREDENTIALS

MEGATREND MOVEMENT

Recognized as an emerging microtrend in our 2024 report ("Elimination or Reduction of Physical Credentials"), this trend has grown by leaps and bounds in the past 12 months, earning it a definitive spot in the Megatrends and aligning with the past year's Megatrend of "Impact of the Megatech Companies" (trend No. 7 in 2024).

The badge office—ostensibly positioned as the purveyor and provider of identity cards—is ripe for disruption. The oversimplification of what most badge offices do is transform physical keys into plastic keys that can be assigned to an individual. Certainly, there is great convenience with the card or fob. Unlike the metal keys they replaced, the card could be disabled if lost or stolen, and in the lanyard worn form factor, it could combine visual verification with door access. But there are obvious security weaknesses that are retained. The key card can easily be handed off to another user, much like a physical key, or worse yet, some cards could be cloned surreptitiously.

The future direction is to move into one of two form factors:

- Biometric based identity
- Mobile credentials that leverage phones and wearables to deliver the credential or identity authentication

"The history of identity has largely been driven by the physical space, through the state bureau (DMV) that produces a document that's not secure [and which] doesn't allow transactions to happen in a risk-free posture. More and more, those things [secure transactions] are expected to occur on our phones. The real promise of this is being able to know who's on the other side of the computer screen – to drive down fraud and abuse."

– DONNIE SCOTT, CEO, IDEMIA, AT SNG 2024

Questions:

Mobile credentials comes together with recurring costs, significant upgrade work, creation of new internal processes, and complex technical management. Is the pain worth the gain?

MEGATREND 10

SAAS, HAAS, DAAS AND A MANAGED SERVICES FUTURE

MEGATREND MOVEMENT

implementation of this trend is likely to be through the integrator for this model to scale. It's also inherently tied to 2024's No. 6-ranked Megatrend "SaaS Reshapes the Integration Business Model."

"The first major video surveillance hardware manufacturer to figure out a true Hardware as a Service (HaaS) model will become the new juggernaut." So wrote an anonymous security industry executive when completing SIA's annual Security Megatrends survey, and this anonymous visionary perfectly summarizes the real business opportunity for the security industry—although it may not be limited to manufacturers and is a delivery model that could be implemented by integrators.

It's a model that's already seen early adoption in the business IT services arena, with companies like Dell, Lenovo and Microsoft all now offering PCs through a HaaS model, sometimes also referred to as device as a service (DaaS) or even desktop as a service. The model in the IT sector is expanding beyond desktops and moving into more varied network infrastructure, delivering infrastructure as a service (IaaS).

While the security industry has already begun to strongly adopt a software as a service model, particularly for cloud video and cloud access, the addition of HaaS/DaaS with managed services creates the opportunity to now monetize the hardware, and not just in a low cost annual license type of approach, but as a true managed services approach, where the full upkeep of the hardware, including patching, cybersecurity, maintenance, technical support and data analytics, is undertaken by the manufacturer or, perhaps more likely, the systems integrator, in exchange for strong recurring revenue.

"Annualized recurring revenue (ARR) is our roadmap. AI components could be the loss leaders for the integrator. We're focused on device management."

– MATT TYLER, VP OF STRATEGIC INNOVATION, WACHTER

Key Takeaways:

1. Goal of security teams is not to own, operate and manage technologies. Goal is to keep people safe, protect the business, protect both physical and digital/informational assets.
2. Businesses increasingly want to rent the technology but own the outcome.

15%

Annual growth rate of HaaS solely in the desktop-as-a-service market

Source: Statista

MEGATREND 10

SAAS, HAAS, DAAS AND A MANAGED SERVICES FUTURE

MEGATREND MOVEMENT

implementation of this trend is likely to be through the integrator for this model to scale. It's also inherently tied to 2024's No. 6-ranked Megatrend "SaaS Reshapes the Integration Business Model."

"The first major video surveillance hardware manufacturer to figure out a true Hardware as a Service (HaaS) model will become the new juggernaut." So wrote an anonymous security industry executive when completing SIA's annual Security Megatrends survey, and this anonymous visionary perfectly summarizes the real business opportunity for the security industry—although it may not be limited to manufacturers and is a delivery model that could be implemented by integrators.

It's a model that's already seen early adoption in the business IT services arena, with companies like Dell, Lenovo and Microsoft all now offering PCs through a HaaS model, sometimes also referred to as device as a service (DaaS) or even desktop as a service. The model in the IT sector is expanding beyond desktops and moving into more varied network infrastructure, delivering infrastructure as a service (IaaS).

While the security industry has already begun to strongly adopt a software as a service model, particularly for cloud video and cloud access, the addition of HaaS/DaaS with managed services creates the opportunity to now monetize the hardware, and not just in a low cost annual license type of approach, but as a true managed services approach, where the full upkeep of the hardware, including patching, cybersecurity, maintenance, technical support and data analytics, is undertaken by the manufacturer or, perhaps more likely, the systems integrator, in exchange for strong recurring revenue.

"Annualized recurring revenue (ARR) is our roadmap. AI components could be the loss leaders for the integrator. We're focused on device management."

– MATT TYLER, VP OF STRATEGIC INNOVATION, WACHTER

Questions:

What do you see as the pros? Scalability? Technology refresh lifecycle? Cybersecurity upgrade processes?

What do you see as the negative? Operating budget impact? Data ownership?

SECURITY INDUSTRY ASSOCIATION

Information. Insight. Influence.

Report Download:
securityindustry.org

Thank you!

Have thoughts about SIA Education@ISC?

Scan the QR Code on the left to provide your feedback on SIA Education@ISC Sessions at ISC West

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses