FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

A CEO Perspective

Transforming Physical AI Security Through Agentic AI, Autonomous Response, and Intelligent Orchestration

Steve Reinharz

CEO and CTO, Artificial Intelligence Technology Solutions, Inc. (AITX) and Robotic Assistance Devices, Inc. (RAD)

Sharing his perspective with Frost & Sullivan

Building the Next Era of Autonomous Physical Security

As physical security environments become increasingly complex, organizations are being forced to rethink traditional monitoring and response models. Rising labor costs, staffing shortages, delayed law enforcement response times, and expanding surveillance infrastructure are exposing the limitations of reactive, manpower-heavy security operations.

At the same time, advances in agentic AI, autonomous response orchestration, edge intelligence, and software-defined security are fundamentally transforming how organizations approach detection, verification, escalation, and operational decision-making.

In this Transformational Growth Leadership discussion, Steve Reinharz shares how Artificial Intelligence Technology Solutions, Inc. (AITX) and its wholly owned subsidiary Robotic Assistance Devices, Inc. (RAD) are helping reshape the future of physical AI security through AI-native platforms, autonomous workflows, and intelligent orchestration systems. Drawing on RAD's expanding deployments across logistics, healthcare, commercial real estate, education, construction, and critical infrastructure, he discusses the shift from human-centric monitoring toward AI-managed security operations built around speed, scalability, and operational efficiency.

Transforming Physical Security Through Agentic AI

Frost & Sullivan: *What do you see as the biggest shifts transforming the physical security industry right now?*

Steve Reinharz: ***The most important transformation happening in physical security is the shift from reactive monitoring to agentic, autonomous response.*** For decades, the industry operated through a fundamentally reactive workflow. A sensor detects something, a human operator notices it, another human decides what to do, and then somebody coordinates response. Every one of those steps introduces latency, operational cost, inconsistency, and the possibility of human error.

What's changing now is that agentic AI is collapsing that loop. Modern systems are no longer simply identifying anomalies. They are increasingly capable of interpreting context, evaluating options, initiating graduated responses, and escalating only when human judgment genuinely adds value. That changes the economics of the entire security operation. It also marks the emergence of what we call Physical AI Security, a model where intelligence, response, and infrastructure are seamlessly integrated.

Frost & Sullivan's **Transformational Growth Leadership Program** aims to honor visionary business leaders who possess the foresight and leadership acumen to drive positive change within their organizations. The leaders we celebrate hail from diverse sectors and company sizes, yet they all share an unwavering commitment to innovation and excellence.

A second major transformation is the disruption of the traditional central station labor model. The monitoring industry has struggled for years with staffing shortages, operator fatigue, throughput limitations, and rising labor costs. Offshore monitoring centers attempted to address part of the challenge, but they largely treated symptoms rather than the underlying structural issue.

> "Physical AI security is about to undergo the same transformation that manufacturing, logistics, and financial services already experienced during the Fourth Industrial Revolution. The difference is that this time the intelligence layer is agentic AI, and the companies that understand how to operationalize it responsibly will define the next generation of the industry."
>
> — Steve Reinharz, CEO and CTO, AITX and RAD

Agentic AI changes that equation by removing operators from repetitive triage workflows. AI can autonomously manage nuisance events, false alarms, verification workflows, and early-stage escalation while allowing human personnel to focus on situations where judgment, decision-making, and intervention truly matter. The result is that a single operator can now oversee what previously required significantly larger teams, creating a far more scalable operating model for the industry. That scalability is a defining trait of physical AI security, where AI systems do more than assist, they manage.

At the same time, the industry is witnessing the unbundling of intelligence from hardware and a broader shift toward AI-orchestrated private response models. Historically, security intelligence was tightly tied to specific cameras, robots, devices, or proprietary infrastructure environments. That model is now evolving, with intelligence increasingly becoming the core product layer while hardware functions as the sensor infrastructure underneath it. In parallel, public law enforcement agencies are increasingly deprioritizing alarm calls, response times are stretching and verified-response ordinances are becoming more common. Historically, private guard response was economically viable primarily for large enterprise customers because of the associated cost structure. AI fundamentally changes the economics of that model. By automating verification, triage, and dispatch coordination, AI now enables private response to become scalable and economically feasible for mid-market commercial properties, multifamily housing, retail, and eventually even residential environments. This is not simply improving the existing security model; it is establishing the foundation of physical AI security, a category that did not previously exist at scale.

Building an AI-native Security Platform

Frost & Sullivan: ***How is RAD approaching this industry transition and positioning itself for the future?***

Steve Reinharz: RAD is not simply observing these trends; we are actively building around them. Years ago, we made a deliberate architectural decision to focus on autonomous response rather than autonomous detection alone. Detecting an event is only one part of the workflow. The real operational value comes from what happens next: how the system interprets the event, initiates response, communicates, escalates, and coordinates action.

That vision evolved into SARA, our Speaking Autonomous Responsive Agent platform. SARA was designed from the beginning as an agentic AI platform capable of operating across RAD devices as well as third-party cameras and infrastructure environments. We intentionally built the platform as an AI-native ecosystem rather than trying to layer AI capabilities onto legacy monitoring workflows later.

Our broader long-term vision is what we call "RAD Town," an integrated, AI-orchestrated security ecosystem where devices, sensors, software systems, monitoring environments, and third-party infrastructure all operate under a common intelligence layer powered by SARA. While the hardware remains strategically important, we increasingly view intelligence and orchestration as the true center of gravity for the business. Over time, we expect recurring software and AI-driven revenue to represent a much larger portion of the company's operational profile as the industry shifts toward platform economics.

> For decades, the physical security industry optimized around manpower because the technology wasn't capable enough to do more. That era is ending. Agentic AI platforms like SARA are changing the economics, speed, and effectiveness of security operations in ways the industry has never experienced before."
>
> — Steve Reinharz, CEO and CTO, AITX and RAD

Restructuring Security Operations Through AI-managed Workflows

Frost & Sullivan: ***How do you see security operations evolving as AI becomes more embedded into the industry?***

Steve Reinharz: The industry is moving toward AI-managed workflows supervised by humans rather than fully human-centered monitoring environments. Traditional workflows built around manually reviewing alerts, coordinating escalation, and managing every operational event individually simply do not scale efficiently anymore, particularly as surveillance infrastructure continues expanding.

Platforms like SARA allow intelligent systems to handle much of the operational heavy lifting autonomously while enabling human personnel to focus on oversight, judgment, exception handling, and strategic decision-making. AI can manage repetitive tasks far more consistently and efficiently than humans, especially in environments involving high alert volumes and repetitive triage workflows.

Importantly, I do not believe humans disappear from the process. There will always be situations requiring empathy, accountability, strategic thinking, and nuanced operational judgment. But the balance between autonomous systems and human involvement will shift significantly over time. The future security operator will increasingly look less like someone staring at monitors continuously and more like someone managing intelligent systems operating in the background.

Why Edge Intelligence Matters in Physical Security

Frost & Sullivan: *You have spoken quite a bit about edge intelligence. Why is edge-based decision-making becoming so important in modern security environments?*

Steve Reinharz: Latency, responsiveness, and operational resiliency matter enormously in physical security environments. If systems rely entirely on distant cloud processing, delays, connectivity limitations, bandwidth dependencies, and infrastructure interruptions can quickly become operational liabilities. Security decisions often need to happen immediately and consistently.

By processing intelligence closer to the point of detection, we can reduce response times, improve resiliency, lower bandwidth requirements, and maintain operational continuity even in challenging deployment environments. That becomes critically important in real-world security scenarios where reliability matters just as much as intelligence.

Edge intelligence also enables organizations to operationalize AI more efficiently across large deployments without completely rebuilding infrastructure around centralized cloud architectures. That flexibility is especially important because many enterprise customers operate complex environments consisting of both legacy and modern infrastructure systems.

Separating Meaningful Autonomy from AI Marketing Noise

Frost & Sullivan: *There's a lot of AI messaging in the market today. How do you separate real operational autonomy from marketing noise?*

Steve Reinharz: Organizations should approach AI claims carefully because the market is currently flooded with messaging that does not always reflect real operational capability. To us, operational autonomy means systems can consistently interpret events, make decisions within defined parameters, initiate appropriate actions, communicate clearly, escalate when necessary, and operate reliably in live environments without constant human intervention.

That is fundamentally different from systems that simply generate alerts or perform well in controlled demonstrations. Meaningful autonomy requires operational discipline, accountability, transparency, and consistent real-world performance over time. If a system cannot reliably perform in production environments, then it is not truly operational regardless of how compelling the demonstrations may appear.

Similarly, being AI-native means intelligence is foundational to the architecture itself rather than layered onto legacy workflows later. Our systems were designed from the beginning around autonomous response, intelligent coordination, and workflow orchestration. That changes how the technology behaves operationally and how customers ultimately experience the platform.

Scaling Through Ecosystem Partnerships

Frost & Sullivan: *Where do you see the biggest growth opportunities for RAD over the next few years?*

Steve Reinharz: The biggest opportunity in front of us is relational rather than purely technological. We believe the companies defining the next era of physical security will be the ones building the broadest and

deepest ecosystem partnerships across the industry.

Monitoring platforms and central stations represent one of the highest-leverage opportunities because embedding agentic AI into existing operational environments allows SARA to scale rapidly without requiring organizations to completely rebuild infrastructure. Similarly, expanding compatibility across third-party cameras, sensors, access-control systems, and monitoring technologies increases the strategic value of the platform itself.

We also view dealers, integrators, enterprise customers, insurance stakeholders, standards organizations, and regulatory bodies as critical parts of the broader ecosystem. The objective is not to win the market independently but to become the platform the broader security ecosystem wants to align with. That creates a very different growth dynamic compared to traditional siloed security models.

The Operational Challenges of Scaling Autonomous Security

Frost & Sullivan: *What do you see as the biggest challenges in scaling this vision over the long term?*

Steve Reinharz: The challenges in front of us are primarily executional rather than existential. There is no lack of market demand or missing technological capability preventing this transformation from happening. The real challenge is executing at the pace required to lead category transformation while maintaining operational consistency.

One major challenge is balancing the pace of opportunity with enterprise adoption cycles. The market is moving toward agentic AI and autonomous response faster than many organizations are operationally prepared for, but procurement processes, security reviews, pilot programs, and budgeting cycles still move at enterprise speed. That requires patience, discipline, and strong execution.

Another major challenge is scaling trust alongside deployments. Agentic AI operating in physical environments does not allow much tolerance for inconsistency. Every successful deployment strengthens market trust, while every poor deployment can damage long-term credibility. As a result, scaling infrastructure, customer success, deployment operations, engineering, and support capabilities simultaneously becomes critically important.

AI as the Foundation of the Company

Frost & Sullivan: *AI is obviously central to RAD's vision. How are you thinking about AI internally, both operationally and philosophically?*

Steve Reinharz: : AI is not simply something RAD uses; AI is fundamentally what RAD is. Our company exists because agentic, multimodal, real-time AI reasoning over physical-world inputs has finally reached the

point where it can perform operational tasks that historically required human personnel.

Capabilities such as autonomous response orchestration, anomaly detection, facial recognition, license plate recognition, intelligent escalation, and communication workflows are all examples of AI solving operational problems within physical security environments. Internally, we also use AI across engineering, operations, support, and communications functions, but those applications are secondary compared to the fact that AI itself is the core architecture of the business.

I do not think framing AI as either a savior or a curse is particularly useful. AI is an incredibly powerful tool, and like every transformative technology throughout history, outcomes depend on how responsibly it is built and deployed. In our environment, responsible AI deployment is already improving operational efficiency, reducing friction, improving scalability, and allowing human personnel to focus on higher-value work that genuinely requires judgment and oversight.

Driving Innovation Through Speed and Operational Learning

Frost & Sullivan: *What drives your approach toward innovation and product development?*

Steve Reinharz: Our approach to innovation is what I would describe as disciplined opportunism. We maintain a very clear architectural North Star around agentic AI orchestration while remaining flexible enough to move at market speed. One of the most important disciplines we apply internally is evaluating whether innovation decisions move us closer to that long-term vision or simply create distractions.

Customer feedback also plays a central role in our innovation process. Many of our strongest product decisions emerged directly from observing live deployments, understanding operational friction points, and listening carefully to how customers actually use the systems in real-world environments.

We intentionally compress development cycles relative to traditional industry norms because the pace of AI advancement simply does not allow for extremely long iteration cycles anymore. That sometimes means revising assumptions, adjusting architectures, or redirecting resources quickly, but the cost of moving too slowly is often much higher than the cost of learning quickly.

Building Competitive Advantage Through Responsiveness and Ecosystem Scale

Frost & Sullivan: *In such a rapidly evolving market, how do you think about staying ahead of competitors?*

Steve Reinharz: Our strategy rests on three primary pillars: speed of innovation, operational responsiveness, and ecosystem scale.

The first is speed. The pace of agentic AI development in physical security is moving fast enough that organizations unwilling to ship, learn, iterate, and adapt rapidly will inevitably fall behind regardless of size or capital resources.

The second pillar is responsiveness. In our experience, responsiveness is one of the most underrated competitive advantages in the security industry. When customers raise deployment issues, request features, or require support, the speed and quality of response significantly shape long-term trust and customer loyalty.

The third pillar is ecosystem partnership development. We believe the future of physical security belongs to platforms capable of building the broadest and strongest ecosystems around themselves. The more organizations aligned with SARA, the more strategically valuable the platform becomes.

Defining the RAD Brand and Market Position

Frost & Sullivan: *As the company continues to scale, how do you want customers and the broader market to perceive RAD?*

Steve Reinharz: We want RAD to be viewed as the company that helped define what agentic AI in physical security actually means. That positioning starts with technical credibility. When enterprise security leaders evaluate autonomous security platforms, we want RAD to be viewed as a reference point based on architecture, operational performance, and deployment experience.

Second, we want customers to associate RAD with trust and operational reliability. Security buyers are naturally conservative because they are protecting people, infrastructure, and operational continuity. Customers need confidence that they can build long-term operational environments around the platform.

Third, we want to be viewed as genuinely customer-centered and ecosystem-positive. Our goal is to strengthen partners, support integrators, and create value across the broader security ecosystem rather than competing unnecessarily with every participant in the industry. Ultimately, we want RAD to be recognized as one of the companies that helped define how modern physical security evolved.

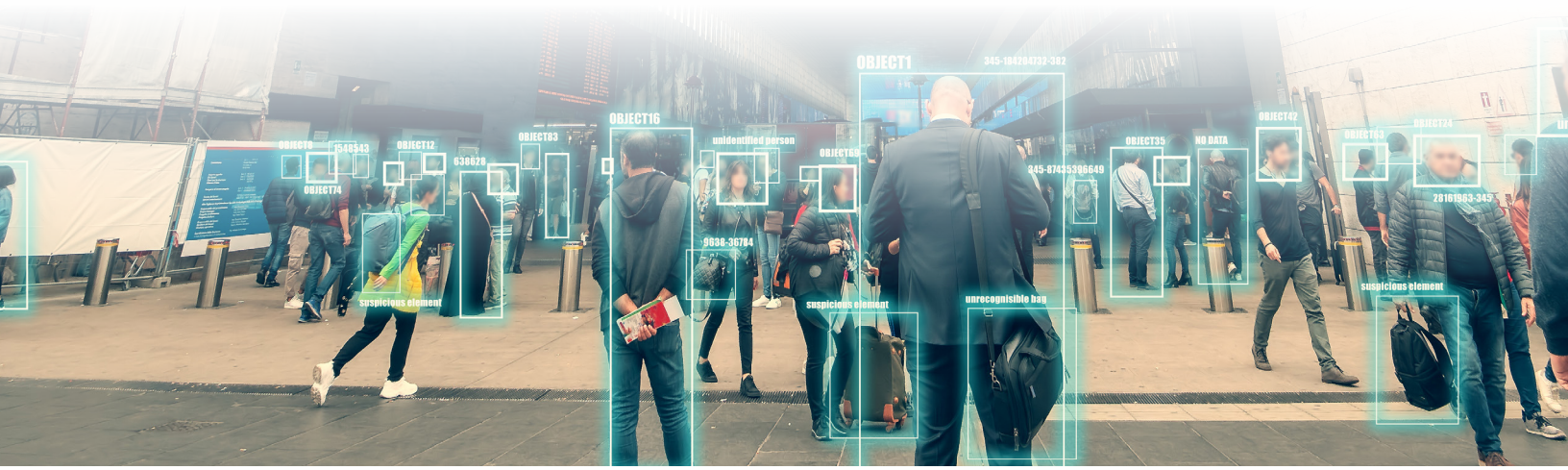
Building a Culture Around Speed, Ownership, and Mission Focus

Frost & Sullivan: *What kind of culture are you trying to build at RAD as the organization grows?*

Steve Reinharz: Our culture is built around four principles: fast, honest, owner-minded, and mission-serious.

Speed matters because the industry itself is moving extremely quickly. Organizations that cannot operate with velocity will struggle to keep pace with the evolution of AI and autonomous systems.

Honesty matters because trust is fundamental in security environments. Internally, teams need to surface problems



quickly and transparently. Externally, customers need clear communication about what systems can and cannot do operationally.

Owner-mindedness means employees focus on outcomes rather than narrowly defined job functions. Mission-seriousness reflects the reality that these systems operate in environments directly tied to safety, operations, liability, and public trust. As the company scales, preserving those cultural characteristics will remain just as important as scaling infrastructure or technology.

The Future of Autonomous Physical Security

Frost & Sullivan: ***Looking ahead, what is the one message you want the industry to really understand about where physical security is heading?***

Steve Reinharz: Physical security is currently undergoing the most important transformation it has experienced in a generation. The combination of agentic AI, autonomous response, and AI-orchestrated private dispatch is creating an entirely new category of physical security that is faster, more scalable, more affordable, and more broadly accessible than traditional models ever allowed.

This transformation extends beyond the security industry itself. When responses to incidents become economically viable at scale, communities become safer. When monitoring centers operate more sustainably, operators work in better environments. When AI handles repetitive workflows, human personnel can focus on the tasks requiring actual judgment and decision-making.

Most importantly, advanced security capabilities become accessible to organizations and customer segments that historically could never afford them.

This transformation is already happening, and our goal is to help define the platform architecture on which the next era of physical security operates.

Closing Reflection: The Shift from Monitoring to Autonomous Security Operations

The physical security industry is entering a pivotal transition point where AI is evolving from a supporting technology into the operational core of modern security environments. As organizations face increasing pressure around scalability, labor shortages, response efficiency, and operational complexity, traditional monitoring models are no longer sufficient to meet the demands of rapidly expanding security ecosystems.

The emergence of agentic AI, autonomous response orchestration, and intelligent edge-based decision-making is fundamentally reshaping how organizations approach detection, verification, escalation, and incident response. Rather than relying solely on manpower-intensive workflows, the future of physical security will increasingly revolve around AI-managed operations supervised by human judgment and oversight.

For AITX and its subsidiary RAD, this transformation is not simply about deploying smarter devices or improving existing workflows. It is about redefining the architecture of physical security itself through intelligent orchestration platforms capable of delivering faster, more scalable, and more operationally resilient security outcomes. As autonomous security ecosystems continue evolving, the organizations that succeed will be those that can effectively combine AI-driven intelligence, operational scalability, and ecosystem-wide integration to create the next generation of proactive physical security operations.

Steve Reinharz | CEO and CTO, Artificial Intelligence Technology Solutions, Inc. (AITX) and Robotic Assistance Devices, Inc. (RAD)

Steve Reinharz is the **Founder, CEO, and CTO of Artificial Intelligence Technology Solutions, Inc. (AITX)** and its wholly owned subsidiary Robotic Assistance Devices, Inc. (RAD), where he is driving the transformation of physical security through AI-powered autonomous technologies. A recognized technology futurist and inventor, Steve has built RAD into one of the industry's most visible innovators in autonomous security, intelligent monitoring, and AI-orchestrated response systems.

Prior to founding AITX and RAD, Steve built and led a successful security integration company that was later acquired in a $42 million transaction. Today, he is widely recognized for pioneering AI-native security platforms that combine robotics, edge intelligence, autonomous response, and intelligent orchestration to modernize traditional security operations.

Steve currently serves on the Security Industry Association's Board of Directors and chairs its AI, Drones, and Robotics Interest Group, helping shape the future direction of the security industry. He is also a frequent speaker at major industry events including ISC East, ISC West, GSX, and ASIS, where he is regarded as a leading voice on the future of AI-driven physical security and autonomous operations.

Ready to Lead the Transformation?

- **Book a Growth Strategy Session:** Align your growth roadmap with Frost & Sullivan's Visionary Growth Pipeline™ Dialog.
- **Engage with Growth Experts:** Co-design AI-enabled, data-driven operating models that scale industry-specific and commercial impact.
- **Share Your Transformation Story:** Position your organization as a transformation leader through Frost & Sullivan's Transformational Growth Leadership platform.
- **Join the Growth Council:** Collaborate with industry leaders shaping the future of your ecosystem.
- **Nominate for Best Practices Recognition:** Be recognized for excellence in growth strategy, execution, and customer impact.
- **Demonstrate Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Activate Brand & Demand Growth:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.

Appendix: Advancing Autonomous Security and AI-orchestrated Operations

As organizations modernize physical security environments, the industry is rapidly shifting toward AI-native architectures capable of autonomous monitoring, intelligent orchestration, and real-time operational response.

At the same time, growing pressure around labor shortages, operational scalability, infrastructure complexity, and response efficiency is accelerating demand for agentic AI platforms, edge intelligence, and software-defined security ecosystems.

To support organizations navigating this transformation, Frost & Sullivan provides forward-looking intelligence across autonomous security operations, AI-enabled monitoring, intelligent infrastructure, and next-generation response ecosystems, including:

- AI Usage in Security Operations, Global
- Macroeconomic Growth Opportunities of Artificial Intelligence
- Frost Radar™: Autonomous Security Robot Solutions

Together, these analyses reinforce the central themes explored in this Transformational Growth Leadership discussion: autonomous response, AI-managed workflows, edge intelligence, intelligent orchestration, and the future evolution of physical security operations.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN