NIGHTDRAGON

MARKET REPORT:

PHYSICAL SECURITY

January 2025

www.nightdragon.com

Foreword

The beginnings of physical security can be traced back to ancient civilizations where people used fortifications, guards, or natural barriers to protect valuables, communities, and territories. Today, we face new physical security challenges - school shootings, geopolitical risks, rising theft, impacts of natural disasters, and much more. Over the past 5 years, 60% of companies have encountered breaches in their physical security measures and 75% of companies place physical security as one of their foremost priorities.

The good news: we also live in an age of incredible physical security innovation. Systems today are often connected, integrated, automated, and cloud-based, allowing for increased security, seamless deployment, and faster information for emergency response. This can greatly improve physical security outcomes, even as risks rise and become more complicated.

Today, we can see that innovation playing out across six key areas, according to an AGC report:

- Access Control: Systems that manage who can enter or exit a physical space, ensuring only authorized personnel can enter (supported by systems like video surveillance)
- Emergency communication: Facilitate alerts and information during crises using tools like intercoms, alarms, and mass notification systems
- End-to-end solutions: Integrate multiple security functions into a single system, covering everything from surveillance to access control
- Operations Management: Managing security operations, including monitoring, reporting, and response strategies
- Remote Monitoring: Remote monitoring involves surveillance and security management from off-site locations
- Threat Detection and Response: Identifying potential security threats through various means, including surveillance technology, sensors, and analytical software

Each of these areas play a critical role in the physical security world today, enhancing security and safety for all of us as we traverse our daily lives. In the following report, we'll explore the market's state, growth drivers, emerging innovation and a market landscape of critical companies in the space.

Table of Contents

The Challenge

Over the past few years, we've seen physical security challenges rise and evolve. Certain industries are seeing a particular rise in crime. For instance, physical attacks on the U.S. power grid average about 60 per day, rising 9% year over year from 2022 to 2023. In healthcare, meanwhile, the World Health Organization estimates that up to 38% of health workers suffer physical violence at a certain point in their careers. Additionally, there were more than 600 mass shootings in the U.S. alone over the past four years.

See below for an outline of the variety of physical security challenges that are driving demand for innovation and investment in physical security solutions:

VIOLENCE

Violence can take many forms, from mass shootings, to murder, to domestic incidents, to workplace attacks. These events pose immediate harm to those involved, including at home and in the workplace. Physical security solutions can help monitor these types of attacks and alert before an incident occurs.

TERRORISM

In 2023, the number of terrorist incidents decreased by 22% to 3,350, but the number of deaths increased by 22% to 8,352. According to the U.S. Department of Homeland Security, this threat is expected to "remain high" over the coming year, citing examples such as violent extremists, illegal drugs, influence operations, critical infrastructure security, and economic security.

UNAUTHORIZED ACCESS

Tactics like tailgating - closely following an authorized person through a secure door - can lead to theft, corporate secret espionage, vandalism, violence, and more. These unauthorized incidents have cost organizations an average of $4.47 million annually. Social engineering, using psychological

The Challenge

manipulation to bait someone into revealing sensitive information or allowing access to unauthorized spaces, is one tool that bad actors can use. Social engineering is especially prevalent in finance, healthcare, and government, where 60% of executives have been targeted.

SOCIAL UNREST

Dangerous situations and social unrest prevail in many areas. Since 9/11, perception of crime rates has steadily climbed and is now at an all-time high. Civil unrest and protests have also driven greater demand for real-time monitoring technology and advanced crowd control and management.

NATURAL DISASTERS

Natural disasters, such as hurricanes, tsunamis, tornados, snowstorms, and more can cause significant physical harm to individuals and businesses. In 2024, for example, Hurricanes Helene and Milton put 1.2 million and 1.9 million businesses, respectively, at risk due to high winds and other effects of the storm.

THEFT AND BURGLARY

Theft and burglary continue to be a challenge in today's landscape. In 2023, the nationwide larceny-theft rate in the United States was 1,347.2 cases per 100,000 of the population. This is a decline off of previous years, but still a significant risk when it comes to securing physical goods, intellectual property, and other important assets.

PROPERTY DESTRUCTION

Destruction or defacement of property or goods through vandalism and other tactics is another physical security risk that remains prevalent in today's world. These incidents can cause financial, operational or reputational harm to a business if physical security protections are not in place.

The Challenge

AI ADVANCEMENTS

While AI enables incredible advancements in physical security and safety, it also introduces new threats and vulnerabilities including AI-Driven Surveillance Attacks. While one AI model might be used to detect and signal abnormal activity or intruders, another Generative AI model, for example, may be used to create realistic voices, fake IDs or badges, and other biometric identities to bypass physical surveillance systems.

CYBER-PHYSICAL CONVERGENCE

While physical security deals with safeguarding people, assets, and physical environments, cybersecurity protects data, networks and digital systems. Though technically separate, cybersecurity and physical security have become inherently intertwined and interdependent, blurring the lines between digital and tangible. With the introduction of "smart" devices and systems, cyber threats have more real-world physical consequences than ever before.

INSIDER THREATS

48% of organizations reported that insider attacks have become more frequent over the past 12 months. These statistics highlight the need for physical security solutions, like cameras and access control, to recognize disgruntled, aggressive, or violent employees who may cause harm or follow up on an investigation.

" Insider threats have also become a key focus, spurring investment in behavioral analytics and tools capable of identifying patterns across physical and digital domains. This combination significantly helps spot insider threats before they materialize."

- Darren Argyle, Co-Founder, Cyber Leadership Institute

Challenges with Existing Solutions

While they have a place, legacy physical security solutions have proven to fall short in many ways regarding improving security and safety outcomes. Challenges with legacy solutions include:

SCALABILITY

As companies look to implement company-wide installations, the cost of installation, storage requirements for security data, adjustments for multiple locations, and training on a new system or integrating with legacy systems create pervasive barriers to entry. Additionally, a company may want to consider how it can drive scalability for teams by leveraging remote access capabilities or cloud-connected devices in a secure way.

ON-PREMISE LIMITATIONS

Many legacy solutions rely on on-premises technology, leaving users and corporate security teams without the scalability, analytics, and connectivity benefits of the cloud. Additional considerations include the cost and time of supporting anything on premises including updates and reboots. Many modern solutions are beginning to leverage cloud-based technology platforms to enable scalability and flexibility with data, as well as provide a secure place to be held and analyzed. Cloud services often work with artificial intelligence in security systems, allowing for more advanced analytics.

TECH LIMITATIONS

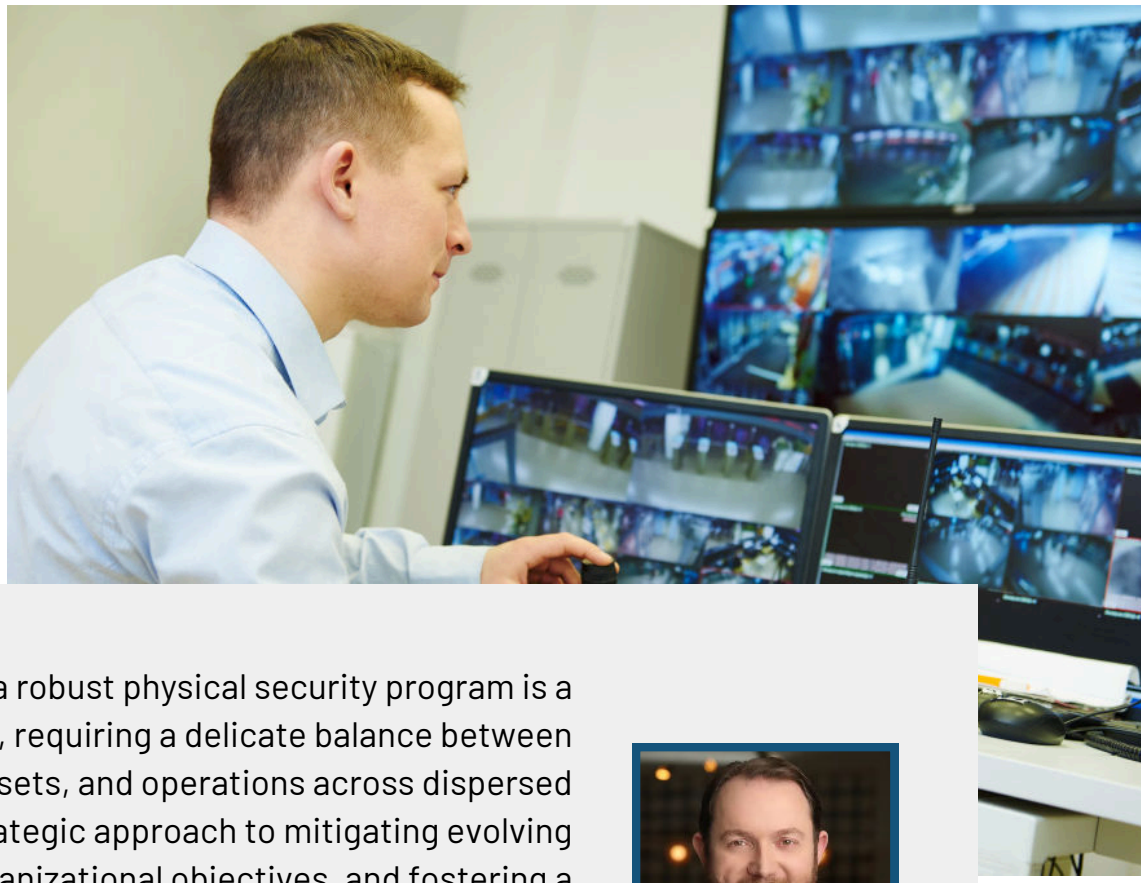
Limitations in technology can contribute to significant failings in a company's physical security architecture. Whether it be blind spots in camera coverage, an error causing a software issue, or a temporary disconnect from a network that disrupts information transfer or loss of data, legacy solutions can fall short without the reliability, uptime, and consistency needed to maintain full security coverage.

HUMAN FACTORS AND ERROR

Simple errors like weak PINs or lost/stolen badges or key cards can, unfortunately, place facilities and personnel vulnerable, while also leading to loss of time and resources from security teams to handle said incidents. Employee training can help to mitigate these issues.

INTEGRATION COMPLEXITY

Older "legacy" systems may not integrate well with new technologies, creating issues with ensuring real-time response and monitoring as well as issues with centralizing risk across various systems and infrastructure.



"Establishing a robust physical security program is a multifaceted challenge, requiring a delicate balance between safeguarding people, assets, and operations across dispersed locations. It demands a strategic approach to mitigating evolving threats, aligning with organizational objectives, and fostering a culture of vigilance—while navigating the complexities of technological integration, regulatory compliance, and the ever-present need for scalability and adaptability."

- Jesse Whaley, CISO, Amtrak

The Opportunity

As the challenge around physical security grows, so too does the opportunity for innovators to help remedy the problem. New products and services from startups and established companies can help position customers to meet new threats around safety and violence, while also adding new tracking, analytics, and additional capabilities through the transition from legacy to more modern systems.

The foundation of many modern systems emerging today is cloud-native technology, which enables scalability and flexibility with data, providing a secure place to be held and analyzed with artificial intelligence. Some applications of cloud-native technologies include cloud-based access control systems in smart offices or schools, video surveillance to reduce theft in retail, and real-time alerting and data analytics to secure premises and improve efficiency.

One example of a physical security market that has evolved thanks to the cloud and AI is video surveillance. The first generation of video surveillance systems centered around legacy DVR systems, physical tape, and on-premises viewing. It then evolved to a second generation that added the ability to tap DVRs through the internet. We're now entering a new third generation, which offers smarter security solutions to help streamline operations and improve safety at scale by leveraging the power of the cloud, AI analytics and a fully integrated technology stack. The result is a safer, more secure and efficient environment.

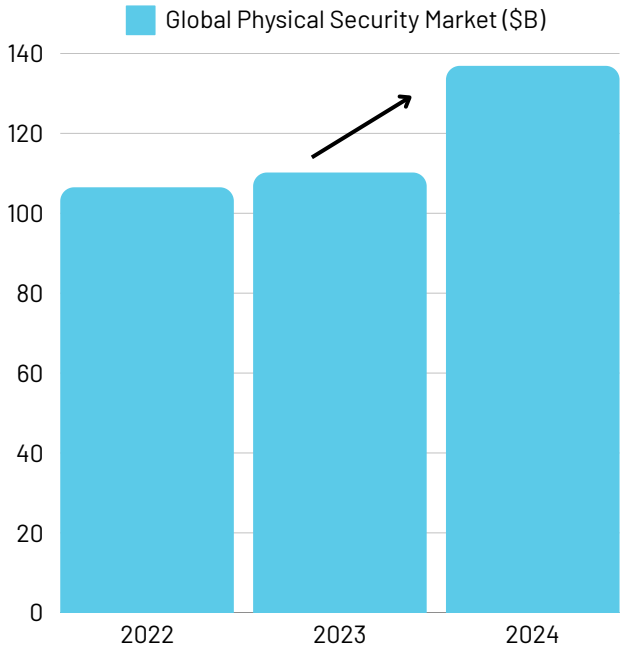
> "Cloud-based physical security solutions transform traditional security into an intelligent ecosystem, leveraging artificial intelligence. These systems serve up a world of actionable insights where none existed before, enhancing operational efficiency and threat prevention."
>
> **- Sridhar Jayanthi, CTO, NightDragon**

We are seeing these evolutions happen across many sectors of physical security, as well as converging it with relevant sectors, such as cybersecurity. As a result, the opportunity is greater than ever for innovators who can help advance the category and the customers who need these solutions to improve physical security outcomes.

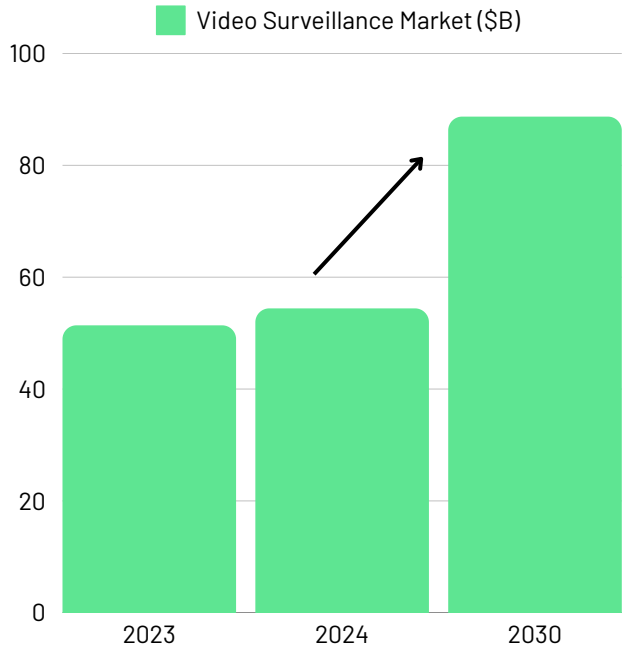
The Market

The global physical security market continues to grow strongly, driven by market factors and new technology innovations. According to research firm Markets and Markets, the physical security market was valued at $106.5B in 2022, rising to $110.2 billion in 2024 and expected to grow to $136.9 billion by 2028. The report cited a rise in malicious activities, security breaches, and the introduction of AI/ML-powered solutions and digital transformation as reasons for that growth. In addition, other growth drivers can include a shift from legacy to more modern systems, increasing concerns for employee safety, overall increases in shootings, and civil and government investments in physical security systems.

Video surveillance represents a significant portion of the overall physical security market. Markets and Markets reported a global market size of $54.42B in 2024, growing to $88.71B by 2030 (a CAGR of 8.4%). Growth drivers for this sector of physical security included introducing AI and cloud-based systems, growing city initiatives for surveillance systems, and integrating video with overall physical security solutions, among other factors.

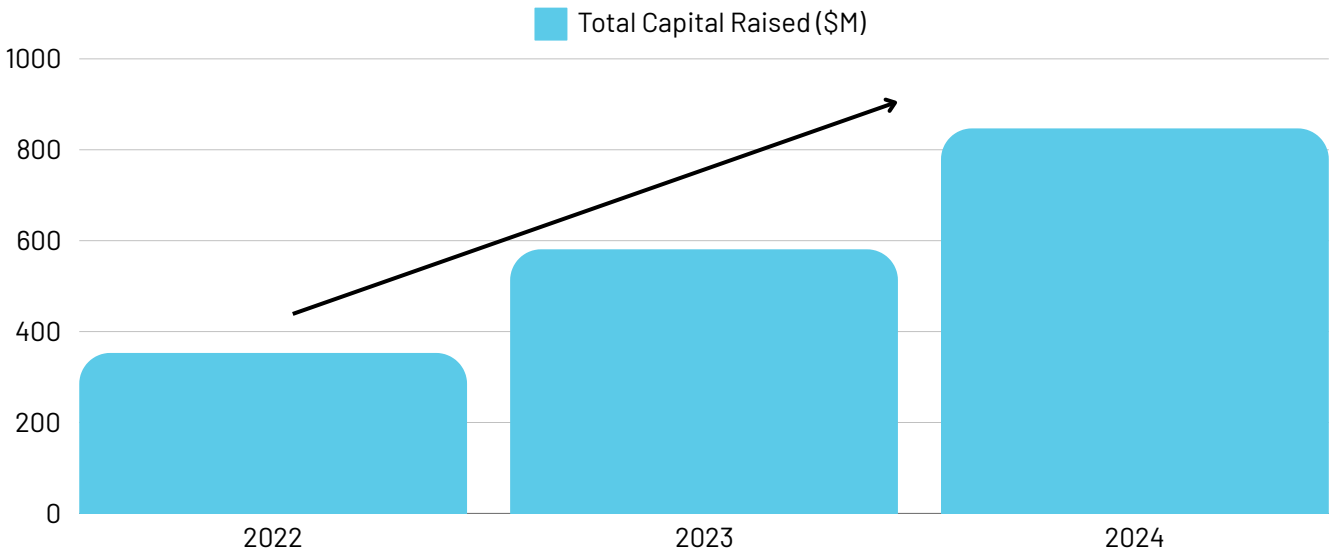


Source: Markets and Markets



Source: Markets and Markets

Investment in physical security companies has grown due to this market opportunity and innovation. In fact, 2024 investment into physical security was tracking to grow 140% from 2022. These growth numbers are especially significant against a backdrop of a 40% fall in total capital raised in the broader technology industry and a 20% fall in the number of investments.



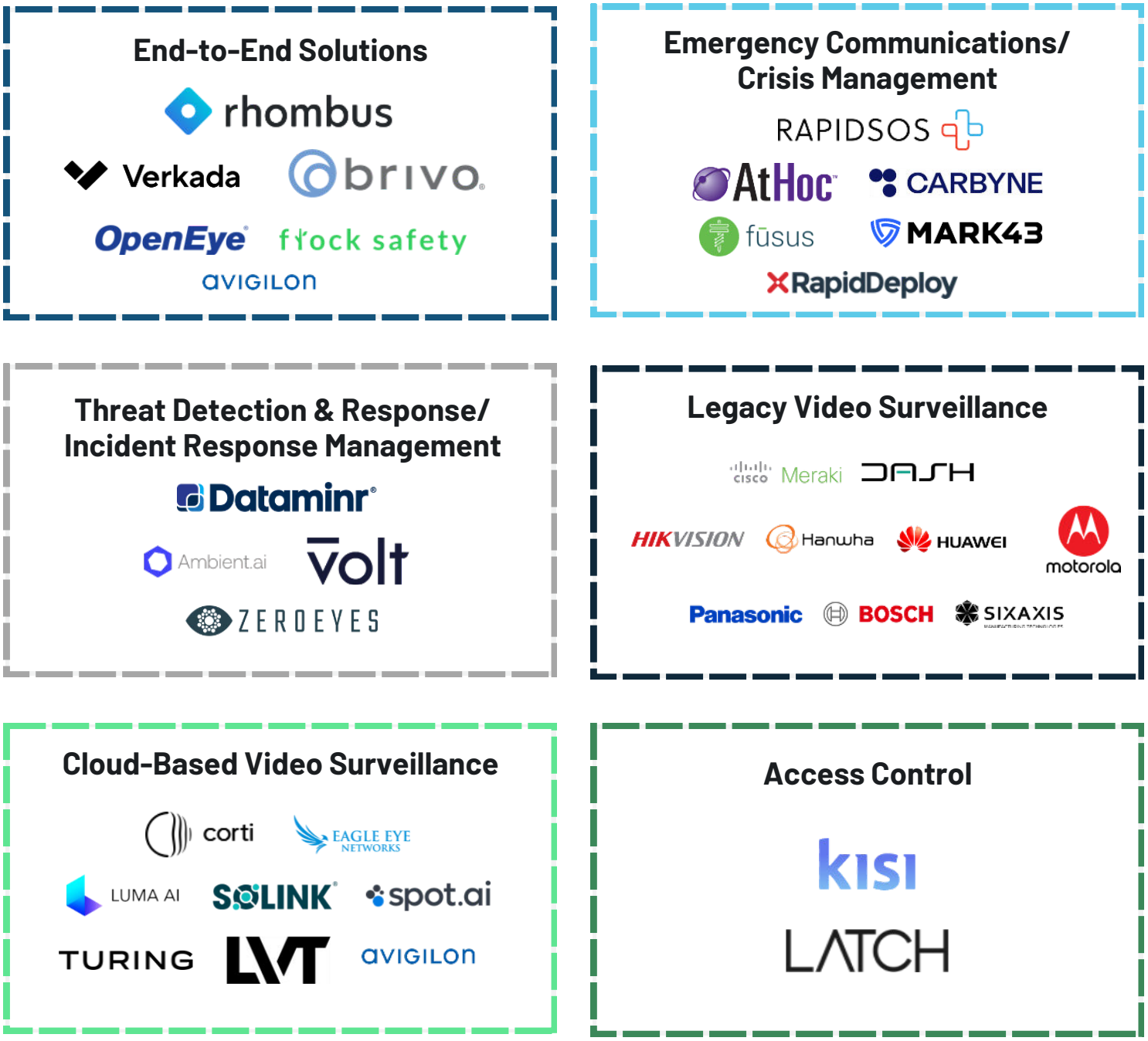
Source: Pitchbook

"The physical security landscape in 2025 reflects the growing convergence of traditional and digital threats. While AI-powered surveillance and biometrics have become standard, we're seeing a concerning rise in hybrid attacks that target both physical and cyber vulnerabilities simultaneously. The key challenge isn't just keeping intruders out – it's creating resilient security ecosystems that can adapt to evolving threats."

- Hanan Szwarcbord, VP, Chief Security Officer, Micron

The result of increased innovation, investment and demand for technologies is a vibrant market for physical security solutions. Key companies and categories can be found below, as outlined by the NightDragon investment team:

Physical Security Market Map



Q&A: Rhombus CEO Garrett Larsson

Rhombus is one of the new leaders in the physical security market, raising $45 million in Series C capital in 2024 from investors including NightDragon, Bluestone Equity Partners, Caden Capital, Cota Capital, Tru Arrow Partners, and Uncorrelated Ventures. It offers a unified, cloud-based physical security platform that brings security cameras, access control, sensors, alarms, and integrations together under a single pane of glass. Rhombus is on a mission to make the world safer with simple, smart, and powerful physical security solutions.

We sat down with Garrett to discuss the latest evolutions and growth in the physical security market. The following is an except from our conversation:

What are some of the most significant physical security risks facing organizations today?
While the usual suspects of theft, shoplifting, and vandalism are still pervasive. The confluence of the shift to remote work and a labor shortage in physical security roles also means that a lot of organizations are forced to cobble together remote access to older physical security systems. Outdated firmware and encryption methods make these systems much more susceptible to attacks, creating a potentially easy entry point for bad actors. This is especially true for large enterprises who are at increased risk of failing cyber audits due to the extra-large attack surface area presented by their connected physical devices (e.g. cameras, door readers, alarm pads).

Where do legacy solutions fall short in addressing those risks, and what sort of new innovations are we seeing in physical security today?
Many legacy systems lack modern encryption methods for communication between devices, making them vulnerable to interception and manipulation. These systems are also often siloed, lacking integration with IT and cybersecurity frameworks, leaving gaps in overall cyber threat

Q&A: Rhombus CEO (continued)

detection and response. Additionally, manufacturers may no longer provide firmware updates, leaving systems further exposed to known vulnerabilities.

How has the use of AI changed the physical security market?
AI is democratizing a higher standard of physical security, making a heightened level of security and safety more accessible to everyone. Security-wise, much of what is being done today could also be done by a human watching a 24x7 feed. However, addressing these types of needs without a human is revolutionary.

How have you seen customer needs evolve with technological advancements?
The combination of better cameras, AI, and more user-friendly systems means that it's no longer just about security. There's a very real opportunity to impact the bottom line, and customers are eager to uncover what operational benefits are possible with these systems. Large organizations especially are thinking about how they can do more with their data and existing tech stack by overlaying AI or adding more advanced cameras and sensors to the mix.They're looking for actionable insights on everything from bottlenecks and compliance with safety protocols to space utilization and improving customer service in physical spaces.

What is the significance of an "Open Platform"?
There remains a large subset of the market that has not yet experienced the new advancements available in physical security. For consumers new to these technologies, an essential piece to adopting them is openness and interoperability capabilities. These characteristics make it easier for organizations to realize the promise of these updated technologies, given the realities of change management, budgets, operational disruptions, etc.

Securing the Security Systems

As physical security systems are increasingly cloud-based and connected to the Internet, it becomes more important to consider how they are secured from cyberattacks. Failing to do so can leave the business open to compromise from a cybersecurity attack or create new safety concerns. For example, there are hundreds of examples of incidents between 2019-2024 involving Ring and Wyze cameras in which hackers exploited accounts without the user's knowledge.

Picture this: your child is suddenly terrified of their room, citing strange noises and pointing at the security camera on their wall. Like many parents, you brush it off and blame childhood imagination. Then one day, you hear it too, and in the case of one child, you hear "Santa Clause" asking questions and playing chilling music. More than 13,000 individuals were impacted by Ring cameras alone in these hacking incidents, and, unfortunately, these privacy breaches are still occurring today.

This dynamic is often referred to in the industry as cyber-physical convergence, where lines blur between risks in the cyber and physical domains, and a risk that originates in one domain has a significant impact on the other. In addition to compromising data, the implications of cyber vulnerabilities on physical systems can have wide-reaching operational – or even life-threatening – impacts. For example, in February 2023, a cyber-attack on Florida healthcare organizations paralyzed all hospital IT systems, forcing employees to switch to pen and paper. Many non-emergency surgeries were also canceled, and countless patients in acute conditions were at risk. Other attacks have threatened power grids, water systems, oil pipelines, and satellites.

Securing the Security Systems

The type of incidents mentioned above have placed the need for a more robust cybersecurity posture top of mind for both companies and customers. There are several things that security leaders can do to improve the cybersecurity protections of their physical systems:

Leverage Strong Passwords and Multi-Factor Authentication
Statistics show that over 80% of data breaches can be attributed to weak or reused passwords. Security leaders should ensure that device and software passwords are complex and leverage multi-factor authentication where possible.

Access Controls and Secure Sharing
Access control minimizes risk by controlling who is allowed to access what (or where, in the case of physical security). The use of tools like biometric scanners, key cards, security cameras, password-protected doors, and security personnel is crucial to ensuring that the wrong individuals don't gain entry or access to prohibited or sensitive areas.

Vet Products for Cybersecurity
Some vendors have incorporated strong cybersecurity protections into their hardware and software, but some have not. It is important to ensure your physical security vendor uses cybersecurity best practices, such as deploying end-to-end encryption, automatic security updates, hardware security, built-in data privacy protection and up-to-date best practices and regulations in physical security.

Q&A: Dataminr Chief Product Officer

Dataminr sits at the intersection of the cyber and physical worlds, with a leading solution to provide companies with real-time information discovery and critical insights from more than one million public data sources. Through advanced AI and machine learning, Dataminr delivers real-time alerts that help organizations stay ahead of risks and opportunities in the physical and cybersecurity worlds.

To better understand their view on the state of the physical security market and the role for AI in mitigating risk, we sat down with Dataminr Chief Product Officer Adam Bates. Here's what he had to say:

Using your insight from the millions of events that Dataminr ingests, what are some of the most significant physical security risks and trends facing organizations today?

From geopolitical risks to natural disasters and severe weather-related crises, it often feels like today's world is more uncertain than ever. We recently asked Dataminr's customers what they see as the top risks and challenges they face, and the responses ranged from long-standing concerns, including terrorism, severe weather, and supply chain disruptions, to more recent alarming trends, such as election security and threats of violence to executives. Common among all these concerns is the profound impact they can have on an organization's people and assets — business critical in the most literal sense.

What are some of the biggest challenges organizations face in mitigating these risks?

Security leaders tell us their biggest challenge is timely awareness of the sheer volume of risk events that unexpectedly arise across their unique operational footprints across the globe, as they're expected to have Scenario Literacy on each. However, the options for timely awareness have not traditionally been up to the challenge. Human Analysis provides rich

Q&A: Dataminr (continued)

intelligence on many facets of a risk but simply doesn't scale to all the surface area leaders need to cover, while OSINT feeds ostensibly contain the breadth of signal required, but are notoriously difficult to operationalize.

How are you seeing these risks converge with the cybersecurity risks we also see in the landscape?

The complexity of timely awareness and Scenario Literacy is compounded when Security Leaders contemplate exposure to cyber risk — typically tens of thousands of endpoints collectively running thousands of different software applications, each exposed to a perpetually morphing set of vulnerabilities or subject to vendor updates that may inadvertently halt operations. Sometimes the impact of a disruption event is isolated to information systems, but to a growing extent, those events have physical world implications, and not just in OT/IOT scenarios. Consider last year's Crowdstrike Falcon update as one extreme example: Security Leaders were struggling to wrap their heads around the extent of outages within their own four walls but also contending with disruption arising from unexpected outages in services their organizations depend upon — travel, shipping & logistics, employees' ability to access routine healthcare services, etc. While an extreme example in its global reach, it exemplifies the sprawling cyber-physical implications that Security Leaders are experiencing routinely in more isolated incidents.

How can AI help organizations combat these rising risks?

The good news is that the information required to detect and understand disruption events in a timely manner (be they physical, digital, or converged) is out there in publicly available data sources. The bad news: it's spread across 1M+ (and growing) sources generating billions of daily inputs in thousands of permutations of languages and modalities. Complexity of this scale can't be solved with approaches that require humans to curate the output. An agentic approach is needed, and that's exactly the route we've taken at Dataminr. Our real-time AI platform continuously analyzes those billions of inputs — accomplishing in one hour what it would otherwise take a team of 60 analysts working 24/7 to accomplish in a year — autonomously filtering out relevant signal from noise, detecting critical risk events across an organization's unique risk footprint in real-time and connecting disparate signals into

Q&A: Dataminr (continued)

cohesive, continuously updating event summaries that provide actionable insight on emerging threats to the business.

What are the next advancements you expect around AI in the world of physical and cybersecurity?

Progressive organizations are actively seeking to create an environment that is instantly aware of threats and is set up operationally to respond to real-time information. As these organizations gain familiarity with the scale of agentic approaches like those employed by Dataminr, I expect they will begin to adopt them internally, automating response protocols and decision-making to a greater degree whether it be generating automated comms for detected risks in certain cases, activating war rooms with the right stakeholders and playbooks, or even deploying resources. Key to this will be a continuous flow of high-resolution, real-time risk and situational awareness information that spans the physical and cyber domains.

Integrators Under Pressure

One of the challenges that organizations face when it comes to physical security is the complexity of systems and the need for integration across a multitude of disparate vendors and products to achieve maximum benefits. This complex dynamic has driven a rise in security system integrators, who act as the man in the middle to help drive integrations, maintain systems, and maximize security outcomes for customers.

A "systems integrator for physical security systems" is a company or individual that designs, installs, and manages multiple physical security systems and seamlessly integrates them under a unified control platform. Additionally, they bring integration expertise from multiple manufacturers, customize the design of systems as needed for the customer's unique needs, install and configure hardware and software, and provide ongoing maintenance and support.

As the physical security market has evolved, so too has the systems integrator space in significant ways. The rise of cloud-based, end-to-end systems appeals to customers because of ease of use, analytics capabilities and less on-premise hardware needed. Additionally, these systems often come with the ability to easily integrate and often a more direct sales model, which can challenge the role of a systems integrator in its traditional form. Instead of choosing solutions or integrating them, the new model has customers leaning on integrators for installation and maintenance, which could lead to lower margins.

"As cloud based end-to-end systems gain in popularity driven by ease of use, native integration and much less on-premises hardware to support, the integrator's traditional role is being disrupted. Security system vendors and integrators will need to find new ways of partnering to achieve combined success," said Richard Sumnall, TITLE at Blue Path Security.

With all that said, while the value and business model of integrators are fundamentally being changed, there is still a role. Forward-thinking physical security vendors are moving to open platform systems, allowing for solutions integrations between their own products and third parties. Additionally, increased convergence between physical, cyber and IT teams creates new opportunity for integrators, with 68% of system integrators saying they expect more involvement with IT. "Convergence between IT and security departments within organizations has caused security systems integrators to become more IT-focused," a report by the Security Industry Association said.

Q&A: RapidSOS CEO Michael Martin

Already in 2025, the US set a new record for hourly 911 volume around 1 AM ET on New Years's Eve. As we face a growing safety challenge seen in the highest number of school shootings in US history (83 in 2024), continuing violent crime, major disasters like the LA fires and hurricanes, we sat down with RapidSOS founder and CEO Michael Martin to talk about how we can harness AI to transform the safety and security of communities globally.

RapidSOS spun out of MIT in 2015, pioneering artificial intelligence for safety, security, and emergency response. Today their platform fuses billions of data feeds from 200+ tech companies into 21,000+ state and local agencies covering six countries and supporting over 170 million emergencies per year.

Michael started his career in hard-tech venture capital before having personal experiences with emergency response which led him to found RapidSOS in graduate school. He's a frequent media contributor for Fox News, CBS, and NBC, was named to Forbes 30 Under 30 for Healthcare, has spoken on AI to predicting emergencies in advance at TEDMED, and has over 100 patents or patents pending in the space of artificial intelligence and emergency response.

What are some of the most significant safety gaps that RapidSOS sees in the world of safety and physical security?

We spend over $600B annually on safety, security, and health monitoring services, most of which rely on the nation's 911 system—a network of thousands of local systems built in the 1960s that remain largely analog and voice-based.

This outdated infrastructure means first responders often lack critical information, such as a caller's name or precise location, and rely on human-to-human voice relays for sophisticated security and life-safety systems—sometimes even spelling out addresses in emergencies despite our connected world.

Q&A: RapidSOS CEO (continued)

The impact is severe: in 2022, an estimated 1 in 3 American fatalities occurred during emergencies, contributing to over $1T in insurance costs. First responders handle these challenges heroically, managing 200 million emergency calls annually in the U.S. (over 2 billion globally).

In this digital era, we have the opportunity to better support their life-saving work by enabling our connected technologies to seamlessly integrate with public safety when it matters most.

How can we better enable first responders to mitigate these risks?
21,000+ state and local governments now operate on the RapidSOS AI safety and response platform called HARMONY. This presents an opportunity for enterprises and consumer device companies to transform how they think about safety, security, and health monitoring services.

For example an enterprise security operations center can now seamlessly coordinate response with local first responders and employee devices - from AI-enabled detection of a fire, hazmat incident, medical, or security emergency to immediate coordination with local public safety and on-site personnel. HARMONY plugs into onsite sensors or operational centers to immediately escalate to 911 and first responders, dropping key data feeds (location, sensor data, blueprints, multimedia, location of trapped occupants, etc.) into one unified picture of the incident Simultaneously, HARMONY pulls in additional sensor feeds from RapidSOS' ecosystem of 200+ tech partners and 540 million devices - updating the incident in real-time and provide specific pre-arrival instructions to on-site personnel.

What new technologies are available to help close the safety gap for these first responders?
RapidSOS bridges the safety gap by integrating data from connected devices directly into 911 and

Q&A: RapidSOS CEO (continued)

public safety workflows. At the heart of this transformation is RapidSOS HARMONY AI, which processes and contextualizes data to deliver real-time, actionable intelligence to first responders. Any connected device can now work in harmony with 911 and first responders in an ecosystem of safety. This is a transformation in the ability of 911 and first responders to protect our communities.

For example, human voice transmits information at a rate of 39 bits per second. Multimedia capabilities in RapidSOS transmit data at 128,000x that rate. The result is business with security cameras, dashcams, schools, and home security systems can immediately pass video to 911 and first responders in an emergency - transforming response. In 2024, RapidSOS introduced the integration of multimedia capabilities into smartphones through Apple Emergency SOS Live Video and Google RCS, enabling live video and enriched messaging to 911.

How can AI be a tool to support emergency response?
After years of building with public safety agencies, in 2024 RapidSOS announced HARMONY, the first purpose built / trained AI platform for emergency response. HARMONY fuses critical data from millions of devices directly into specific local systems and standard operating procedures.

For example, in a train derailment HARMONY takes real-time data from the train, surrounding camera feeds, and transport records to immediately generate a full picture of the incident for 911 and first responders, fusing data into their specific local systems and policies and recommending response based on authoritative information like the PHMSA Emergency Response Guidebook.

During Hurricane Helene, HARMONY supported public safety agencies overwhelmed with call volumes by managing low-priority calls, allowing responders to focus on critical emergencies. Additionally, agencies leverage HARMONY for real-time language translation, keyword detection, and workflow automation, enhancing their efficiency and effectiveness.

NightDragon Perspective

As a SecureTech firm committed to securing our world for tomorrow, NightDragon recognizes the vital importance and immense growth potential of the physical security market. Recent global events underscore the urgent need for enhanced safety measures, crisis communication systems, and advanced threat detection and response tools. Examples include the recent devastating plane crash in South Korea, the attack on the United Healthcare CEO, and the wildfires spreading across Los Angeles in early 2025, among other crises.

For example, we see a paradigm shift in video surveillance, with analog on-premises systems transitioning to end-to-end cloud-based ecosystem providers. This is driving a sizable market refresh of legacy technology, as well as opening opportunity for innovators with superior security outcome capabilities, such as enhanced remote monitoring, advanced AI-driven analytics, real-time alerting for faster response times, and more. Looking ahead, we anticipate the continued evolution of video intelligence, with video camera edge-computing playing a critical role in improving operational efficiency and enabling sophisticated AI capabilities.

Additionally, we see significant opportunities for companies that can accelerate the delivery of actionable intelligence to first responders during critical situations. By leveraging richer and more diverse data sources, these innovators can enable faster and more informed decision-making, dramatically enhancing safety and security during emergencies.

These examples illustrate the vast and multifaceted opportunities within physical security today. Innovators leveraging AI and other advanced technologies are uniquely positioned to enhance security intelligence, improve safety outcomes, and bolster operational resilience. As we look to the future, NightDragon remains committed to closely monitoring this dynamic market and supporting the solutions that will help secure our world for generations to come.

Contact Us

If you're building interesting technology in this sector or have a perspective on physical security, please reach out to the members on our team following this market:

Morgan Kyauk
Managing Director
morgan@nightdragon.com

Alec Kiang
Senior Associate
alec@nightdragon.com

NIGHTDRAGON