Dataminr

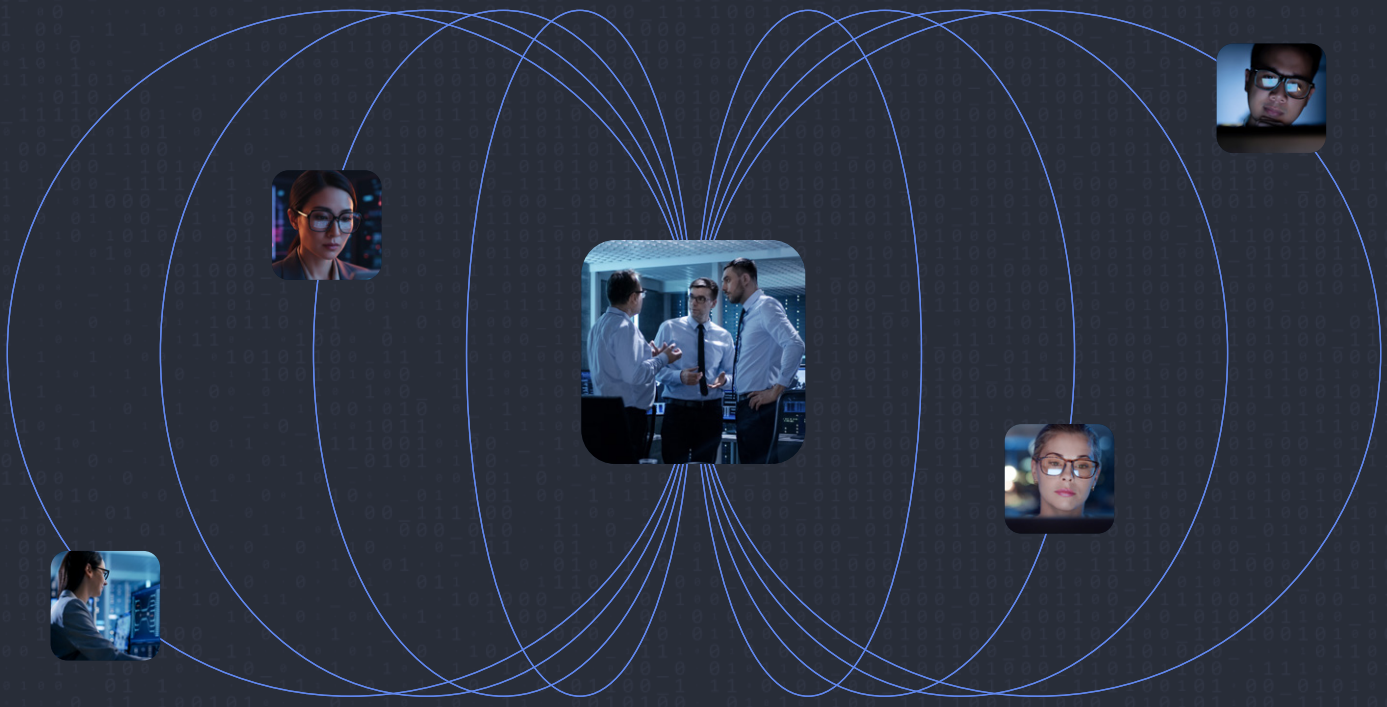
ebook

Dataminr Guide to the Expanding Risk Landscape

Go from chaos to clarity with AI-powered real-time event, threat, and risk intelligence

dataminr.com

The interconnected nature of today's digital businesses and high velocity, AI-powered threats coming from across the threat universe have created unique obstacles for security teams. Compounding these challenges are risks that are no longer siloed being monitored and mitigated by security teams that often are. These factors lead to a perfect storm of security blind spots, fatigued teams, and a dangerous blurring of traditional security boundaries.



The interdependent nature of today's digital business means a security risk in one domain can quickly tumble into another. There are, of course, benefits to this interconnectedness: a better customer experience, improved product delivery, and streamlined operations. In real-life applications, grocery apps deliver to the front door, hospital systems share electronic medical records for procedures and surgeries, and auto insurance companies use smartphones to digitally track driver safety.

But the drawbacks and potential blind spots can be severe and far-reaching. A disruption in an airline's digital systems can ground entire fleets for hours, while a ransomware attack on a hospital can impact patient care if doctors are unable to access digital health records or write electronic prescriptions. The consequences of being unprepared for the risks of today's interconnected business reality can be devastating for both employees and customer safety. This doesn't mean that organizations should limit innovation or fear these security challenges. High-performing organizations will approach the new world of security with well-planned strategies, educated teams, and critical tools and platforms. This also means security leaders need to undergo a radical rethinking of the organization's approach to threat detection and response.

The expanding risk landscape

Increasing risk across all domains of an organization presented by high velocity, AI-powered threats, information overload, and organizational silos.

Cross-domain security strategy

When an organization takes a cross-domain approach to threat monitoring with both physical and cyber security teams working together to share insights and data sources.

Cross-domain threats

Threats that originate in one domain and present risk in another domain.

Cyber-physical systems

Intelligent systems engineered to connect the physical to the digital, allowing interaction between the two domains e.g., autonomous cars and smart grids.

Hyperconnectivity creates a larger attack surface

The expansion of the risk landscape can be partially attributed to the increasingly global nature of the world and hyperconnectivity that comes with digital business. High-velocity AI-powered threats, information overload, and organizational silos create new vulnerabilities and introduce emerging bad actors.

Adding to the security evolution are the approximately 18 billion Internet of Things (IoT) devices worldwide. By 2030, that number is expected to rise to approximately 40 billion.[1]

This widespread use has created a much larger surface area of risk for nearly all types of organizations and security teams have seen an uptick in bad actors exploiting the increasing vulnerabilities. In 2024, a Swedish Tietoevry data center suffered a ransomware attack. Despite being limited to one part of the data center, the attack impacted a number of customers, including a national movie theater chain that was unable to sell online tickets and a farming supply store that had to temporarily close all its stores. Many customers, including universities and government entities, experienced disruptions to payroll and HR systems.

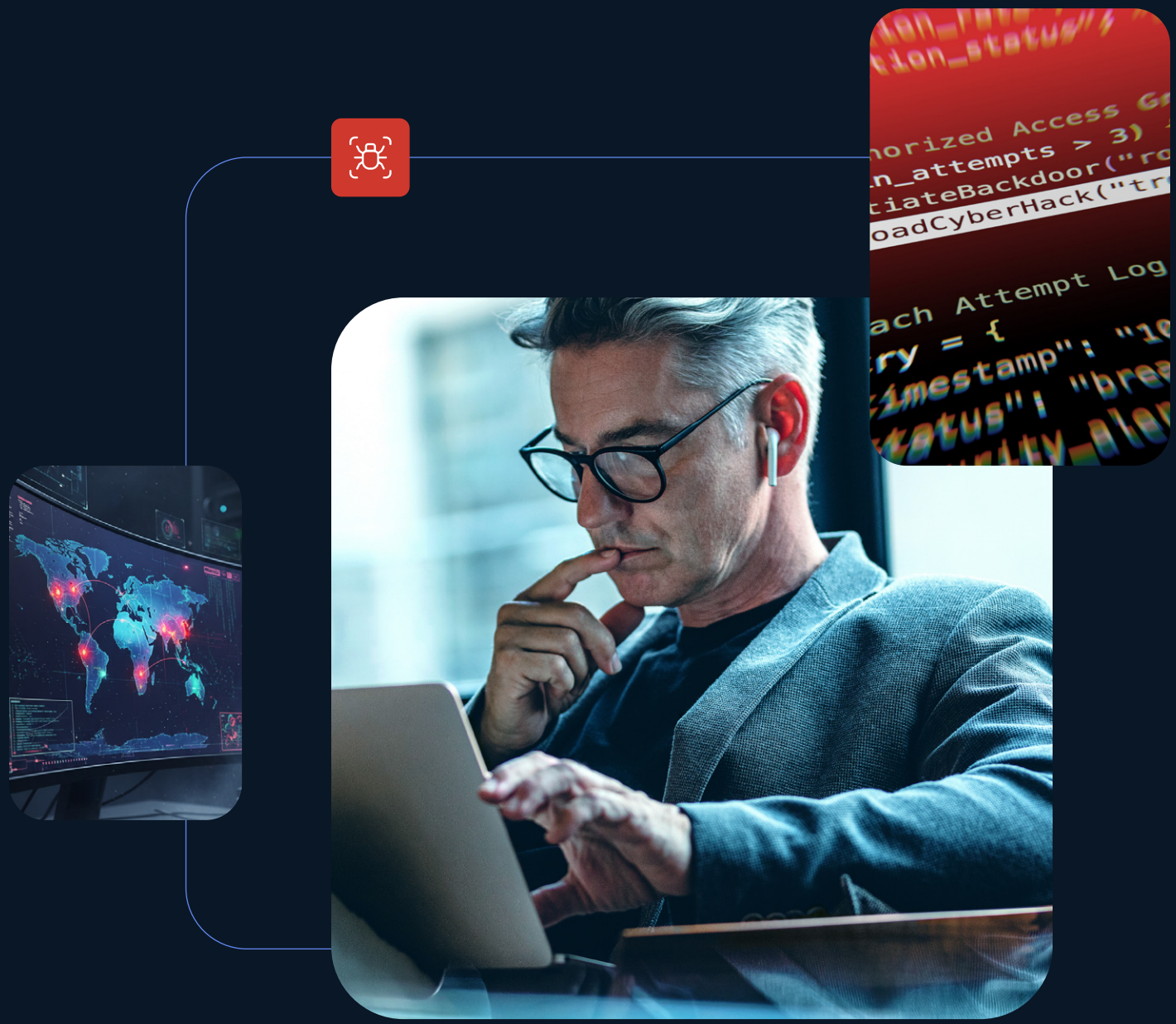
> Take for example, a 2024 cybersecurity survey of healthcare organizations. It found that: **92% of organizations experienced a cyberattack in the past 12 months**. Many of those same organizations said that cyber attacks negatively affected patient care and safety—and contributed to a rise in mortality rates.
>
> **Source:** https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report

1. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally

A new type of threat

Reactive risk management is a strategy of the past and will prove ineffective against modern security risks. Security teams who want to offer the best protection and mitigation need to focus on a strategy that prioritizes a proactive, holistic view of the organization and threat landscape.

Security risks are no longer fitting into predictable patterns, but rather exhibiting accelerating volatility.



The risks of too much security information

A critical area of potential failure in security is information overload. Today's security teams are drowning in data. Monitoring the expanding risk landscape has exponentially increased the volume of information security teams need to parse through and manage. There are more devices, more security tools, more threats, more inaccurate disinformation, and more players than ever before.

In fact, 59% of security leaders say they receive too many security alerts and 47% of Managed Service Providers said they felt overwhelmed by the large volumes of security data. This is a constant source of anxiety for security leaders because the risk of missing a critical piece of information amid a landslide of fragmented, security data could be catastrophic. It is essential that today's security teams utilize platforms that accurately parse information and report critical pieces to customers.

59%

of security leaders say they receive too many security alerts

47%

of Managed Service Providers said they felt overwhelmed by the large volumes of security data

Examples of the expanding risk landscape

1 June 2025

UNFI, one of the largest grocery distributors in North America, was hit with a cyberattack as part of Scattered Spider leading to a complete shutdown of its network and resulting in empty grocery shelves. UNFI estimated sales losses of up to $400 million.

2 June 2025

Bank Sepah, Iran's state-owned bank, went completely offline after a cyberattack, with customers unable to access accounts or process payments.

3 April 2025

U.K. retailer Marks & Spencer was the victim of a ransomware attack that halted online sales, impacted operations at a key distribution center, and created inventory issues in stores.

4 February 2024

Change Healthcare, a major processor of healthcare transactions in the U.S., was the target of a ransomware attack. As a result, 74% of hospitals reported direct patient care impact, including delays in authorizing medically necessary care. Pharmacies were unable to fill prescriptions and hospitals had to divert patients to other facilities or revert to paper processes.

1 September 2025

Collins Aerospace, an aviation IT provider, was taken offline by hackers leading to delays at several large European airports, including Heathrow and Brussels. The attack, which targeted check-in technology provided by the company, resulted in canceled and delayed flights and increased wait times as airport staff reverted to manual check-ins and boarding pass confirmations.

2 July 2025

Winelab, a large alcohol specialty retail chain in Russia, closed its retail stores after a cyberattack impacted operations and sales.

3 May 2025

Kettering Health, an Ohio-based healthcare system, experienced a cyberattack that led to canceled elective inpatient and outpatient procedures, diversion of some emergency cases to different hospitals, and inaccessible electronic health records systems.

4 September 2024

Transport for London (TfL), which manages London's public transportation network, experienced a cyberattack associated with the Scattered Spider hacking group. Though it did not impact physical transportation like trains or buses, the attack did affect key IT systems like journey history, contactless payments, and some live transport updates. It also disrupted Dial-a-Ride, TfL's door-to-door transport service for those with a disability.

5 June 2024

CDK Global, a major IT/Software provider for the automotive industry, took its own systems offline after a ransomware attack impacting 15,000 dealerships. The attack led to disruptions in car purchases and the service department, payroll, tracking and ordering car parts, and scheduling appointments, and cost car dealerships more than $1 billion.

Global response to the expanding risk landscape

Recognizing the potential impacts of the expanding risk landscape and the urgent need for more holistic, innovative approaches, a number of regulators and governments have developed new regulations and initiatives. Some are amending and expanding existing legislation for today's security needs and others are launching entirely new frameworks and directives.

European Union

NIS2 Directive:

A legal framework to enhance cybersecurity capabilities, and expand risk management measures and reporting requirements to additional sectors including: public electronic communications, waste and wastewater management, critical product manufacturing, etc.

Critical Entities Resilience (CER):

An EU directive complements the NIS2 by focusing on physical security and organizational resilience of critical infrastructure.

North America

U.S. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA):

A federal law that aims to improve the cybersecurity in 16 public and private critical sectors by establishing requirements for reporting incidents and ransomware payments.

Canada's Bill C-8 (Pending):

The proposed Act would grant more power to the governor and minister to take action against telecom providers in order to protect the broader infrastructure, establish required cybersecurity programs and reporting structures for critical cyber infrastructure.

Australia

Security of Critical Infrastructure Act (SOCI):

A legal framework designed to ensure protection and resilience among critical infrastructure assets and services (both physical and cyber). SOCI requires mandated reporting, outlines rules for third party data storage, and establishes a required risk management program for critical infrastructure.

Asia

Singapore Cybersecurity Act:

A legal framework designed to strengthen cybersecurity within essential services, investigate cybersecurity incidents, share information, and establish a licensing framework for cybersecurity service providers.

Japan's Active Cyber Defense Law:

Updated in early 2025, Japan's legislation contains new rules for cyber reporting, expands data collection practices, and mandates reporting of cybersecurity incidents in critical infrastructure.

A holistic security strategy for modern risks

> "There are still a lot of companies out there that are siloed, and a lot of CSOs who do not want to touch any part of cybersecurity. They don't necessarily understand it. They fear it in some cases, because they haven't taken the time to learn about it. Those are the companies that are at the greatest risk, because all of the resources that could be used to identify and mitigate a problem are not being used properly."

Dave Komendat
Former VP & Chief Security Officer at The Boeing Company

Ensure all security teams work in lockstep

Organizational silos create a huge risk for organizations. Because security threats are no longer isolated to one domain, organizations with poor cross-communication between security teams can create blind spots, miss critical security cues, and perform duplicative work. CSOs rank 'data and organisational silos' as one of the top three obstacles to the effectiveness of corporate security, according to The Clarity Factory Annual CSO Survey. The outcomes can range from missed opportunities to catastrophic events.

Many organizations operate the cyber and physical security teams as distinct, standalone disciplines with little to no collaboration on managing risks. Today's cyber and physical security teams require a formal means of communication and a standard of collaboration—ensuring that when threats emerge, they see beyond their area of responsibility and understand the attack from a holistic security perspective.

Though cyber and physical security teams must be in a position to collaborate and communicate, they can remain as distinct teams as long as they are interoperable. Some organizations have opted for a single unified function, but it is not required to establish an effective cross-domain security strategy.

What's most important is that cyber and physical security teams have a shared commitment to work together to prepare for and respond to cross-domain threats. To do so successfully, those teams should consider the following actions:

Identify and close gaps between security and risk teams

- Conduct a formal risk assessment to uncover points of intersection, shared dependencies, and cascading effects.
- Consider cross training and orientation, so that there is a degree of mutual understanding.
- Begin working as a coalition so that the teams can collectively advocate for their shared priorities and resource needs—both cyber and physical, as well as other risk management areas.

Develop and maintain a shared playbook

Work together to develop cohesive strategies and action plans. With multiple players, potentially in multiple departments, it is essential to have a well-documented, agreed-upon, and easy-to-follow set of processes that uses common language and supports consistent response.

Clearly delineate roles and responsibilities

Within the cyber and physical security teams, outline specific roles, responsibilities, and organizational hierarchies so there is complete task clarity for all involved in incident response.

Ensure business continuity

Appoint a project leader for each team and leverage established frameworks to respond to any disruption while safeguarding operations. Identify the most essential functions, how they should be maintained, and what needs to be done to mitigate immediate risk.

Fortify business resilience

Maintain the focus on team collaboration and establish a transparent and standardized process for timely information sharing with the goal of protecting long-term business value.

Keep an eye on regulations, tech, and your industry

1

View Regulations as the Floor, not the Ceiling

Meet the required industry regulations and government legislations but also identify any additional criteria that need addressing in order to strengthen the organization against potential threats.

2

Employ the Right Technology

Find a software solution that will provide both the cyber and physical security teams with a shared, accurate and single picture of reality and surface the most relevant threats. This calls for an AI-powered real-time event, threat & risk intelligence solution that can keep pace with the scope, number and frequency of emerging threats and ensure nothing is missed.

3

Acquire Industry Insights

Know what's percolating within your industry, but also in adjacent sectors, and react accordingly. Communicate with industry peers to learn how they are managing cross-domain threats. Ask questions around phishing campaigns and/ or ransomware groups and industry-based vulnerabilities and vendors, including control systems or software platforms.

4

Accept the Job is Never Done

Remember that strengthening resilience against cross-domain threats is a dynamic, continual process with lessons learned and adjustments made on an ongoing basis.

The value of real-time, actionable intelligence

Today's organizational risks don't mimic traditional security challenges. They require a complete reimagination of the role and responsibilities of security and a progressive solution. Real-time event, threat and risk intelligence is the bedrock of resilience and a critical piece of a contemporary security strategy.

On July 4, 2023, there were reports of operational disruptions at Nagoya Port in Japan, which were later found to be associated with a LockBit 3.0 ransomware attack. The disruptions caused a system failure that shut down port operations, affecting 10% of all Japanese trade for two days. Our AI-powered Dataminr Pulse for Cyber Risk solution immediately recognized that this event fit the profile of a cyber attack and alerted Dataminr customers of the disruptions in real time—six hours earlier than other reports. Customers' cyber and physical security teams were then able to quickly initiate incident response and continuity planning, allowing them to minimize the effects of supply chain disruptions.

Dataminr's AI platform processes trillions of computations daily, analyzing multi-modal signals to curate the fragmented (and overwhelming) influx of data. It delivers actionable intelligence faster than a human analyst, enabling security teams to stay one step ahead of risks and threats and be prepared to mitigate cross-domain threats while ensuring resilience and strategic thinking. Additionally, Dataminr offers a comprehensive view of the entire threat universe to help security teams eliminate blind spots and improve cross-domain communication, while synthesizing critical data into actionable intelligence that updates as the event or threat evolves.

> What matters most when it comes to managing the expanding risk landscape is having the right people, processes, and technology in place to prepare for and respond to modern security concerns.

Dataminr is the global leader in AI-powered real-time event, threat & risk intelligence. The company delivers the earliest actionable intelligence on breaking events, emerging threats, and unexpected risks across the physical, digital, and cyber domains. Dataminr first pioneered Multi-Modal Fusion AI, synthesizing text in 150 languages, image, video, audio, and sensor signals across 1M public data sources to deliver the fastest, most accurate real-time detection. Dataminr's AI innovations, including ReGenAI, Intel Agents, and PreGenAI, build on this foundation by delivering Live Briefs, Agentic AI-powered context, and Predictive Intelligence. More than 100 U.S. government agencies, 20 international governments, two-thirds of the Fortune 50, and half of the Fortune 100 trust Dataminr to protect people, assets, and operations and respond with unmatched speed and confidence. For more information, visit www.dataminr.com.