Enterprise Strategy Group™ by TechTarget

Dataminr: The Importance of AI and Public Data to Address Third-party Risk

NOVEMBER 2024

This Enterprise Strategy Group eBook was commissioned by Dataminr and is distributed under license from TechTarget, Inc.

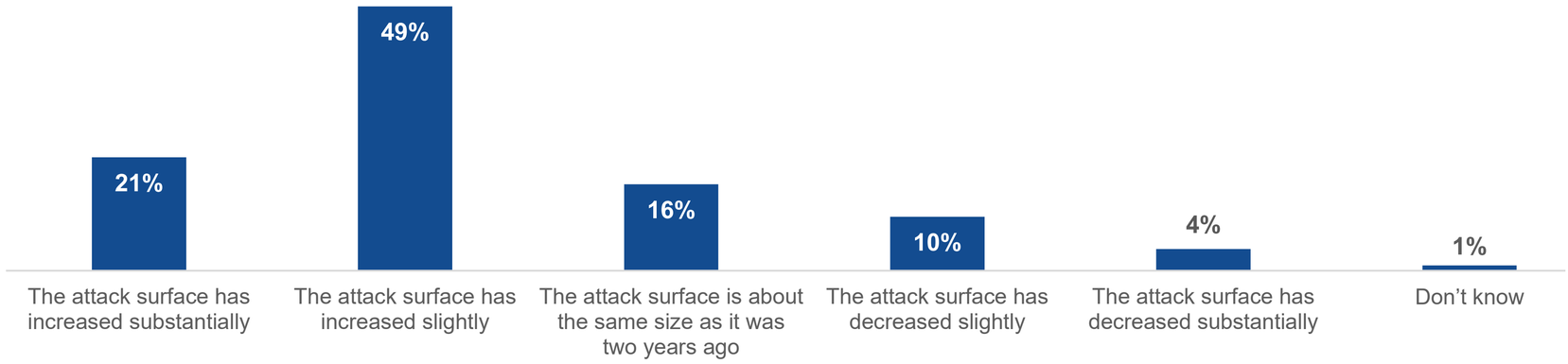
Introduction

Third-party risk (TPR) continues to grow for organizations across various industries, with AI-driven attacks adding a layer of complexity to the existing cyberthreat landscape. As businesses depend more on third-party vendors, the attack surface expands, which increases exposure to vulnerabilities. Risks can also arise from external sources such as suppliers, SaaS applications, and potential zero-day vulnerabilities in software. To address these challenges, leveraging advanced AI in combination with real-time data can enhance proactive risk identification and mitigation, offering a well-rounded defense strategy.

Attack Surfaces Keep Growing

Research from TechTarget's Enterprise Strategy Group found that 70% of organizations are experiencing growth in their attack surface, with 21% reporting a substantial increase. As companies depend more on external vendors, SaaS applications, and other third-party entities, the challenge for security teams intensifies. They must continuously address new vulnerabilities introduced by third parties, while at the same time still meeting traditional cybersecurity responsibilities in the context of a worsening threat environment.This heightened complexity makes it critical for organizations to implement robust third-party risk management strategies that monitor and alert on global threats and leverage AI and real-time data to stay ahead of potential risks.

Attack surface growth over the past two years.



"Dataminr provides our Cyber Threat Intelligence program with timely and relevant alerts that assist our analysts with actioning defensive measures against cyber threats. Dataminr regularly beats out other vendors when alerting us to breaking news with their customizable features. Whether the alerts notify us of widespread exploitation of a critical vulnerability or a ransomware attack on a third-party vendor, our analysts can quickly identify threats, assess risk, and implement defenses at a rapid pace."

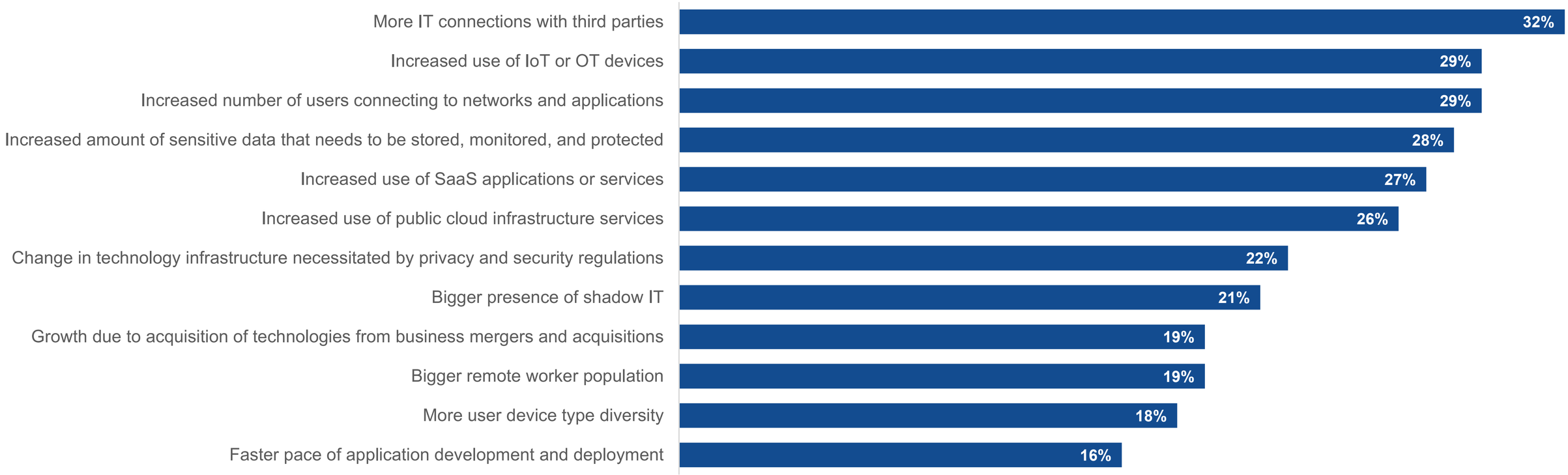
—Citizens Bank

Source: Enterprise Strategy Group Complete Survey Results, *Cyber-risk Management Best Practices*, October 2024.

Attack Surface Growth Is Being Driven by Third-party Connections

The expansion of attack surfaces is increasingly driven by connections with third-party vendors, the growing usage of IoT and OT devices, an increase in user bases, the proliferation of sensitive data, and the widespread adoption of SaaS applications. These factors create vulnerabilities that often lie beyond the direct control of security teams. Despite having security policies in place for third-party providers, organizations still struggle to effectively manage risks that originate from external sources. As attack surfaces grow, especially with third-party involvement, traditional security measures become insufficient. This makes a proactive, real-time approach to third-party risk management essential, combining automation, continuous monitoring, and collaboration across security and business units to mitigate threats before they materialize.

Primary reasons for the increase in organizations' attack surface.

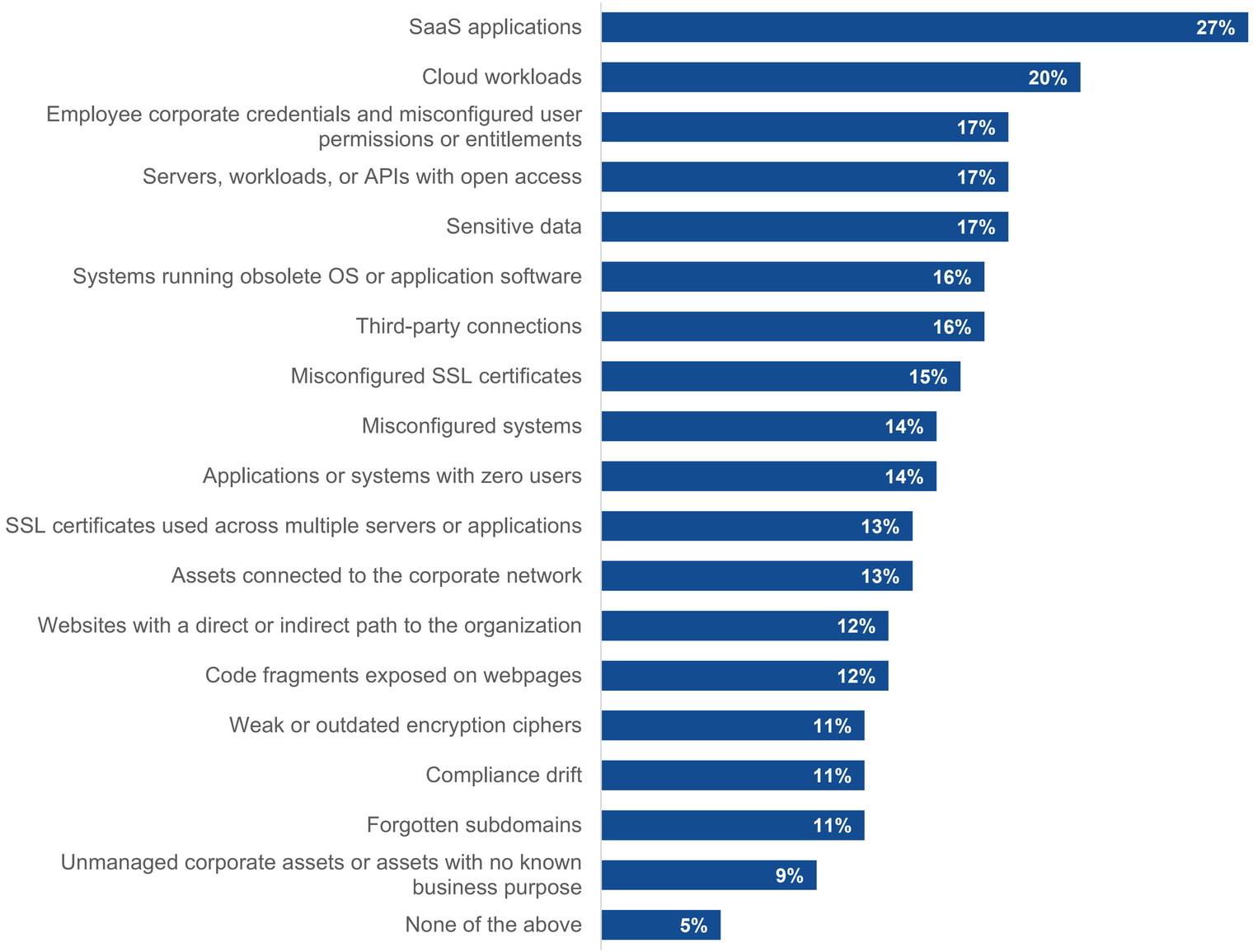


Source: Enterprise Strategy Group Complete Survey Results, *Cyber-risk Management Best Practices*, October 2024.

A Lack of Visibility in Attack Surfaces Creates Critical Weaknesses

Many organizations struggle with limited visibility across their expanding attack surfaces, with third-party SaaS applications, APIs, third-party connections, and cloud workloads posing the greatest challenges. The growing complexity of networks, combined with an increasing number of interconnections between applications and resources, significantly increases risk. As attacks escalate, security teams face mounting pressure to safeguard environments they can't fully see or control. This lack of visibility impairs their ability to detect and respond to threats effectively, making it essential to adopt advanced monitoring tools, real-time analytics, and a zero-trust approach to secure the expanding perimeter.

External attack surface areas with the least visibility.



Source: Enterprise Strategy Group Complete Survey Results, *Cyber-risk Management Best Practices*, October 2024.

75%

of organizations reported experiencing ransomware attacks, with 11% experiencing daily breaches.

Despite Efforts, Attacks Still Breach Defenses— Driven by Expanding Third-party Risk and Attack Surface Growth

Despite significant investments in security tools, ransomware attacks remain a persistent threat that affect organizations of all sizes. The widening attack surface, fueled by third-party connections, cloud usage, and SaaS applications, creates vulnerabilities that are difficult to control. 75% of organizations reported experiencing ransomware attacks, with 11% experiencing daily breaches, 16% experiencing weekly breaches, and 19% experiencing monthly breaches. Security teams are finding it harder to manage risks beyond their direct control. Third-party vendors, cloud providers, and interconnected services continue to challenge traditional security models, amplifying the exposure of sensitive data and critical systems to threats. This highlights the urgent need for more stringent third-party risk management, improved visibility, and robust defense strategies to mitigate these ongoing disruptions.

Ransomware attack frequency.

11%

Yes, we've experienced ransomware attacks on a **daily** basis

16%

Yes, we've experienced ransomware attacks on a **weekly** basis

19%

Yes, we've experienced ransomware attacks on a **monthly** basis

29%

Yes, we've experienced ransomware attacks on a **sporadic** (i.e., less than monthly) basis

22%

No, we **have not** experienced any attempted ransomware attacks in the last 12 months

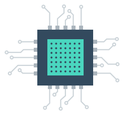
Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.

The Growing Attack Surface and Third-party Risk Multiply Opportunities for Sophisticated Cybercriminals

As the attack surface expands, so too do the tactics and targets of cybercriminals. Over time, attackers have become increasingly sophisticated, taking advantage of various entry points to maximize the effect of their efforts. While storage systems and cloud environments remain the most frequently targeted areas, networks and IT infrastructure top the list of high-value targets. Disabling parts of an organization's IT infrastructure can cause widespread disruption, effectively halting business operations and creating significant financial and reputational damage. The growing interconnectedness of third-party systems exacerbates this vulnerability. With more businesses relying on cloud services, SaaS applications, and third-party providers, the attack surface stretches beyond what traditional security models can easily manage.

By targeting these external connections, whether APIs, cloud workloads, or third-party SaaS solutions, attackers can bypass traditional security perimeters and gain access to critical systems or data.

Areas of impact by successful attacks.



38%
Key IT infrastructure

32%
Networks or connectivity

31%
Internet-of-things operations infrastructure

26%
SaaS or cloud-based business applications

24%
On-premises business applications

75%
of organizations reported being the victim of a successful attack **that had a negative financial impact or disrupted business operations** in the past 12 months.

Types of organizational impact.

53%
Data exposure

51%
Data loss

46%
Operational disruption

36%
Financial loss

29%
Reputational damage

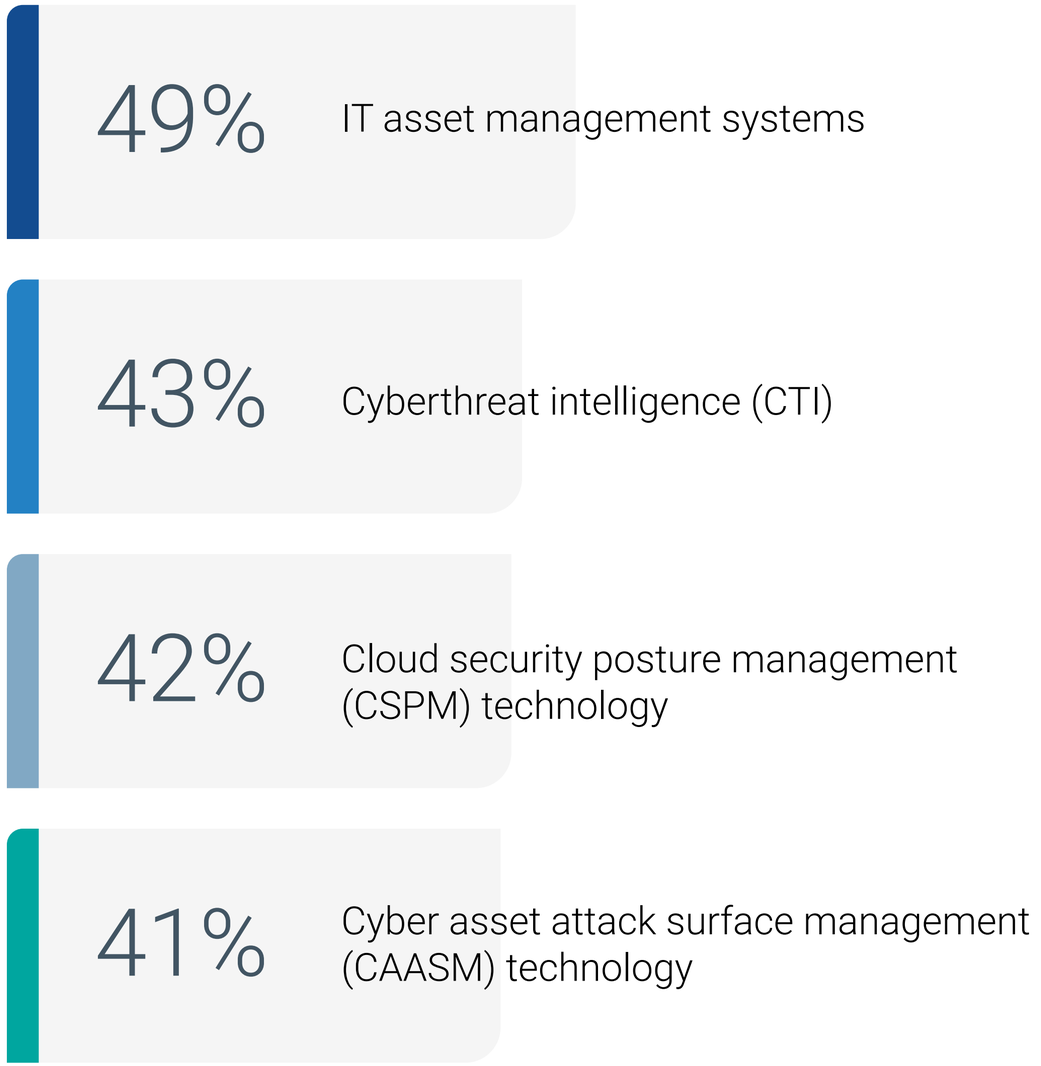
Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.

Monitoring External Attack Surfaces: A Complex Challenge for Third-party Risk

To keep pace with the ever-expanding attack surface, organizations have adopted a variety of methods to monitor and manage external threats. Among the most commonly used tools are IT asset management systems, threat intelligence platforms, and cloud security posture management solutions. Non-technical solutions like risk scoring help prioritize third-party risks based on their potential impact. Additionally, attestations and surveys provide valuable insights into a third party's security practices and compliance efforts, aiding in risk management.

While these tools provide critical insights and can be effective in identifying vulnerabilities within an organization's own systems, they often fall short when it comes to managing third-party risk. The lack of visibility into third parties, specifically the inability to accomplish continuous monitoring in the same way an organization does with its own infrastructure, leaves organizations exposed to risks that might not be immediately visible or easily mitigated by traditional tools.

Most common external attack surface monitoring methods.



Source: Enterprise Strategy Group Complete Survey Results, *Cyber-risk Management Best Practices*, October 2024.

It's Time to Tackle the Third-party Risk Challenge

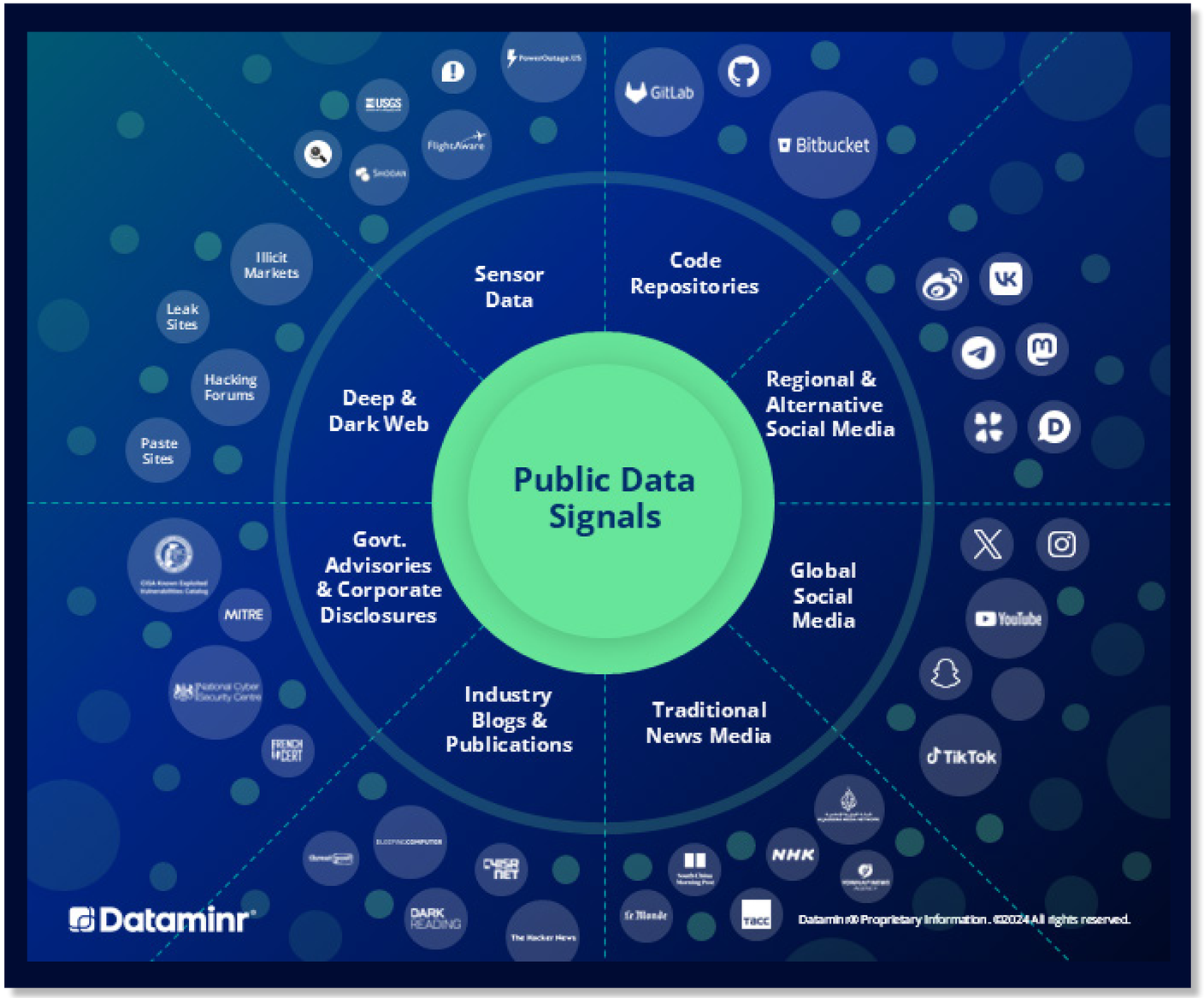
Managing third-party risk requires constant vigilance, and public data sources are an invaluable resource for this effort. Publicly available information enables organizations to monitor third parties continuously by providing a dynamic lens into potential risks. This approach mirrors the way organizations use internal data tools, such as SIEMs, to monitor activity within their own environments.

However, harnessing the full potential of public data is no small feat. The vast and complex ecosystem includes millions of data sources, billions of metadata points generated daily, and information in thousands of languages. Without the right tools, this abundance of data is too unwieldy to analyze effectively.

Dataminr solves this challenge by leveraging advanced AI models to analyze public data signals and transform them into actionable insights. This ensures organizations can proactively address potential third-party risks with the early warnings they need to prepare and respond.

"Dataminr's real-time alerts have helped decrease our incident response time by nearly 70%, which is fantastic. It makes the difference between being owned and not being owned from a cyber perspective."

—Sierra Nevada Corporation



AI-powered External Risk Detection With Speed, Scope, and Relevance Is Needed

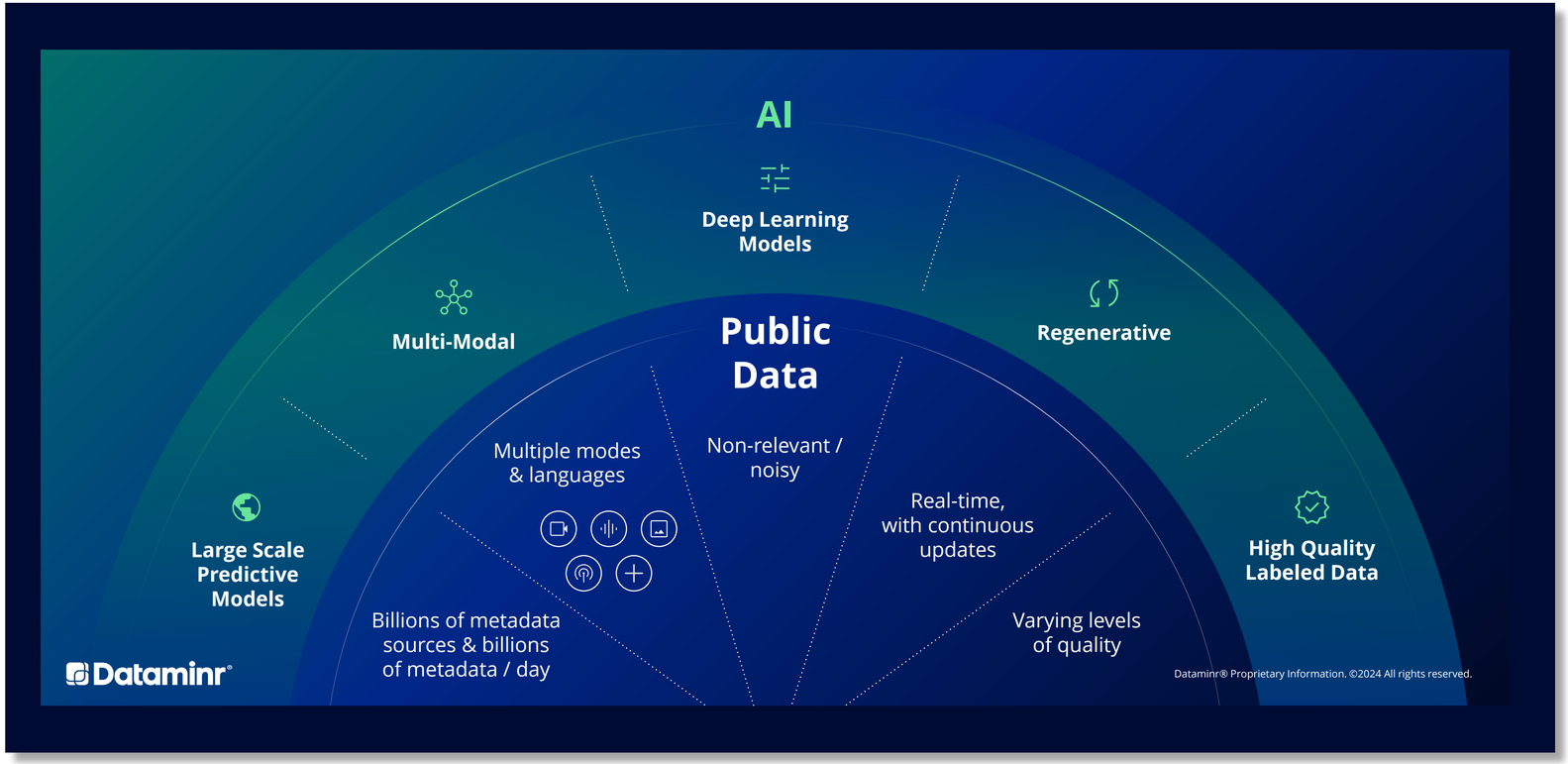
Dataminr provides real-time information alerts sourced from public data to help organizations make informed decisions quickly. Using artificial intelligence and machine learning, Dataminr analyzes more than 43 Terabytes of text, images, and video daily from more than 1 million public data sources in 150 languages and from 220+ countries and territories, including social media, news outlets, blogs, and other online platforms, to continuously detect emerging events and potential risks as they happen.

Dataminr turns massive amounts of raw data into actionable insights to reduce third-party risk and helps organizations stay ahead of crises and manage risks effectively.

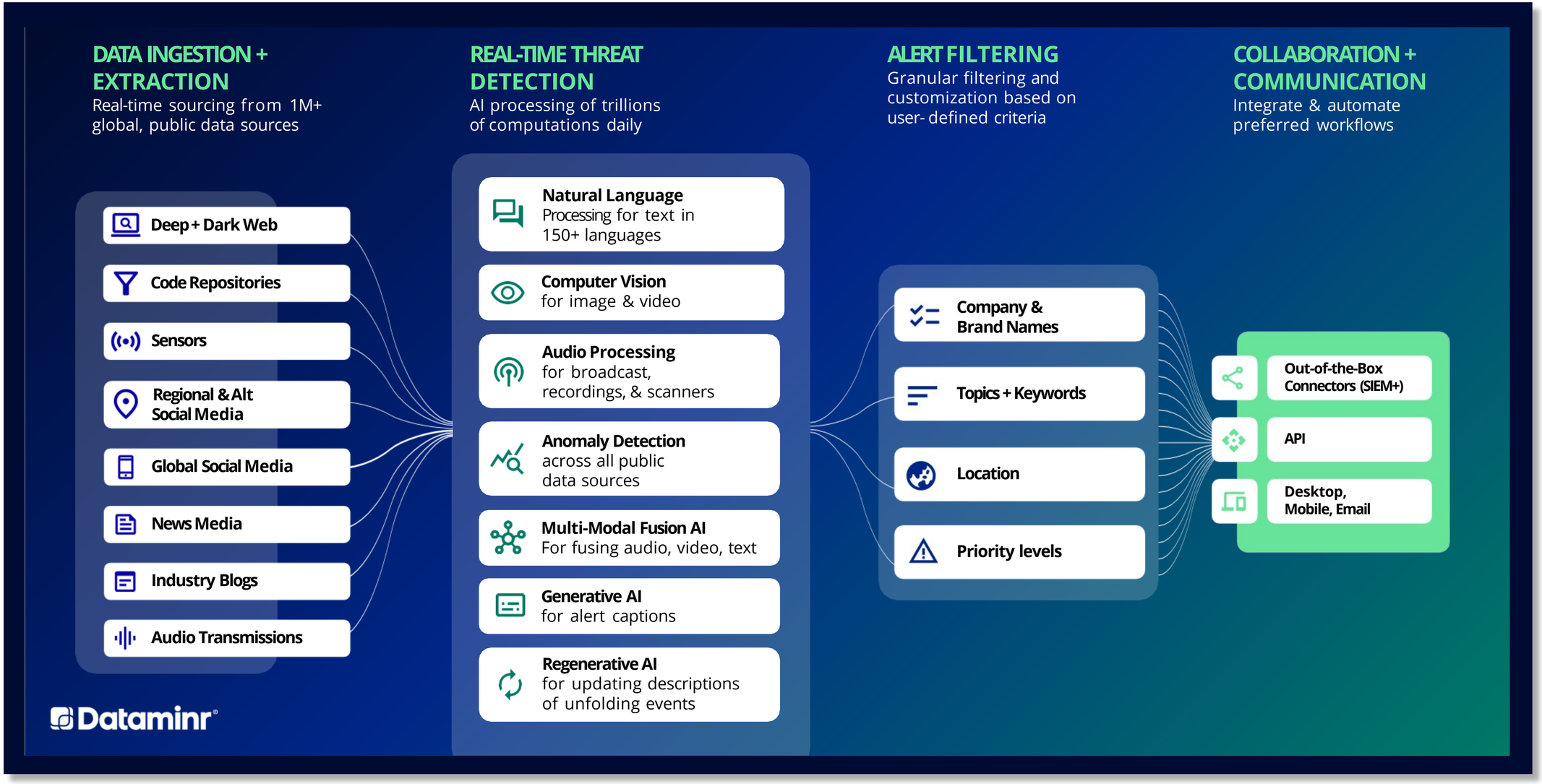
1M+ Data Sources
human and machine generated

43TB+
text/image/video per day

150+ languages
in **220+** countries



How Dataminr Pulse for Cyber Risk Works



Conclusion

Organizations are increasingly feeling the effect of new third-party threats, making it essential to oversee both internal and external environments in parallel. Dataminr Pulse for Cyber Risk addresses this growing need by empowering security teams with real-time alerts and insights on emerging threats from external sources.

By leveraging Dataminr's advanced AI-driven detection that delivers alerts with unmatched speed, scope, and relevance, security teams can quickly detect and respond to targeted and pervasive threats in time to respond effectively.

Integrating Dataminr's real-time alerting with organizations' existing internal monitoring tools not only enhances overall threat detection but also bridges the gap between internal and external security coverage.

This dual-layer approach ensures that organizations can monitor their own infrastructure while also gaining visibility into third-party risks. By extending these capabilities beyond internal systems, security teams can proactively address vulnerabilities introduced by third parties, strengthening their defenses and ensuring greater resilience in today's interconnected digital landscape.

Real-world examples.

Dave Komendat, Founder and President of DSKomendat and former Boeing CSO, on the benefits of using Dataminr's AI-driven insights to stay ahead of cyber risks.

Jesse Whaley, CISO at Amtrak, on how Dataminr Pulse for Cyber Risk's real-time, AI-driven external threat detection helps his company stay ahead of evolving threats.

Dataminr®

ABOUT

Recognized as one of the world's leading AI businesses, Dataminr enables faster response, more effective risk mitigation and stronger crisis management for public and private sector organizations spanning global corporations, first responders, NGOs, and newsrooms. Dataminr is one of New York's top private technology companies, with employees across six global offices.

LEARN MORE

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.