PULSEMETER

Techstrong Research

# Security Data Fabrics

SPONSORED BY

DataBee
COMCAST TECHNOLOGY SOLUTIONS

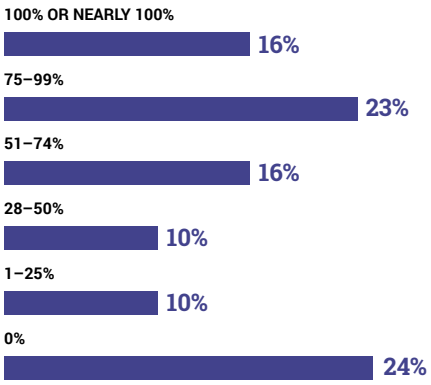
**THERE'S NOTHING MORE COMPLEX** than managing petabytes of data from sources with proprietary schemas and inconsistent formats and tools that don't integrate or work efficiently together. And while we may not recognize it as such, it's security organizations that bear the brunt of this massive data management challenge. Security teams are faced with this challenge every minute; constantly wrestling with how they acquire, manage and leverage security data from across the organization, whether in the cloud, on-premises or both.

The crux of the problem lies in the need to simultaneously have a granular and a big-picture view of their security posture. Organizations have a large number of security tools, each creating its own data silo. At the same time, security teams must comprehensively view information, threats and events from across the organization to perform analysis, inform decision-making, respond to threats and perform real-time security and compliance reporting. That's nearly impossible to do at a very large scale with traditional security tools. Security information and event management platforms (SIEMs), which provide a consolidated view of security information from multiple data sources, continue to be an essential element in the security toolset, although they don't fully meet needs such as compliance monitoring, visibility and decision making, and are highly dependent upon proper rule configuration.[1]

Large data management challenges aren't new, though a modernized approach is needed in security data management. A recent trend in solving security data management challenges is to leverage proven data management approaches and

**What percentage of your organization's security data is intergrated into a SIEM or data repository you manage?**

Organizations still struggle to pull together and integrate security data into a common platform. 44% of respondents have 0-50% of their security data integrated.




[1] https://purplesec.us/resources/cyber-security-statistics/#SIEM

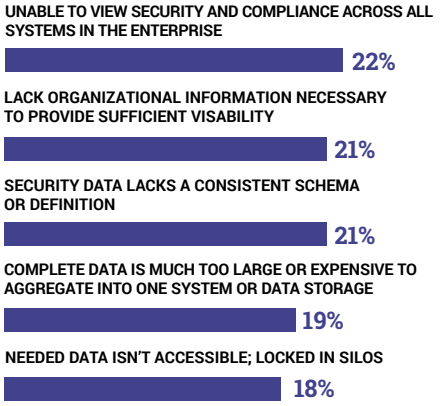
technologies, such as data lakes and data fabric. Security data lakes store massive volumes of diverse security data in their native format, including logs, network telemetry, threat intelligence feeds, alerts and more.

Data fabrics are a proven data management architecture IT data engineers utilize to centralize and streamline data integration across an organization. Described as "modular and composable" by Gartner, this architecture fosters continuous connections between various data points or sources. Unlike traditional data management solutions that often necessitate a rip-and-replace of existing solutions, data fabrics augment and enhance current tools and capabilities. This architecture facilitates access to data, supports easy access by multiple personas within an organization, and enables more informed decision-making processes. Data fabrics also facilitate cost savings and ensure that data from diverse sources and formats, cloud-based and on-premises, is continuously and efficiently integrated.

Security data fabrics further refine this approach by concentrating on managing and analyzing security-related data and telemetry. Security data fabric is an architecture that encapsulates and interprets this complex data. By integrating data from various security tools and platforms, security data fabrics facilitate a more coherent and actionable understanding of an organization's security posture. Security data fabrics empower organizations to detect and counteract security threats in real-time and near real-time, offering a holistic view of their security stance, controls, enforcement and network operations. Security data fabrics also enable more effective risk

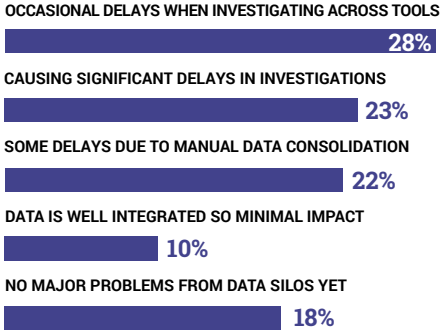
## What gaps exist in your current SIEM, observability and monitoring systems?

There is no "one gap to fix," but multiple challenges to integrating security data across the enterprise.




## How are data silos impacting your security operations and compliance?

Lacking integrated security data is causing most enterprises delays in security investigations and operations.




management, compliance adherence, and overall optimization of security workflows. This approach enables organizations to identify and respond to security threats in real-time, provide a comprehensive view of their security posture and controls, manage network operations and more.

To better understand practitioners' views of managing and using security data, Techstrong Research surveyed cybersecurity professionals in early 2024 to assess the state and usage of security data. The results make clear that security tools and management platforms face real challenges in attempting to meet the changing needs of security organizations.

While 52% of respondents indicate they have more than half of their security data integrated into a SIEM or data repository, 22% indicate they are unable to view security compliance across all systems, and 21% indicate they lack the organizational information necessary to provide sufficient visibility across the enterprise.

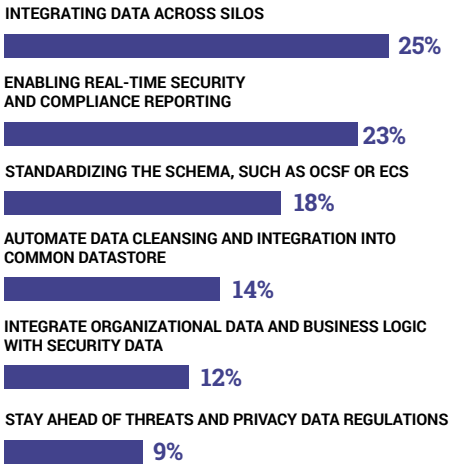
## TECHSTRONG RESEARCH ANALYST VIEW

Security professionals are deeply committed to their work, adopting a purpose-focused approach that underscores their dedication to upholding security, compliance and privacy objectives. While there is no shortage of security products and tools available, a new approach is required to meet the demands the business places on security and compliance professionals. Organizations are approaching security by folding it into their larger enterprise strategy, creating opportunities for security data to be joined with other information about the business, enabling the business to do more, increase customer trust, reduce their attack surface and mitigate risks.

Storing, managing and data sharing of very large and growing security data repositories quickly is critical for security teams. Yet, some organizations are responding to this is by increasing the storage capacity of a repository or aggregation solution. This doesn't truly address the changing nature of security and data workflows, nor does it help unravel the complexities holding back the information security teams. In addition, this solution becomes expensive and unwieldy, potentially slowing investigations and ultimately does little to satisfy high-priority use cases across the organization.

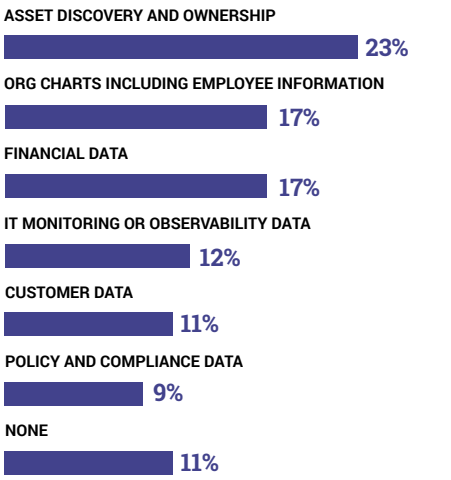
### When improving your security data workflow, what's most important to you?

There is an emphasis on data integration for a more efficient security strategy and a shift toward proactive security measures.




### Which of the following do you currently integrate with security data?

Organizational structure and financial data are most commonly integrated with security data. However, varying integration levels in other areas show that organizations benefit when multiple data sources are brought together.



Managing security data isn't a security problem; it's a data management problem. Utilizing data lakes and data fabrics brings proven data technologies to bear for security data. Security data fabric brings flexible techniques for ingestion of continuous parallel data pipelines, support of native data formats, on-demand data transformations, scalability and long-term data retention to demonstrate compliance or perform historical analysis. Additionally, taking a security data fabric approach brings the real-time data analysis capability necessary for success, whether teams are analyzing compliance across the organization or tracking down the latest threat.

Security data fabrics help to ease the friction from challenges like data cleansing, data interoperability, continuous data ingestion and the lack of real-time analysis, so they don't stand in the way of protecting systems and data and ensuring business continuity. As we look to the next generation of security data technologies, it's time to streamline access, improve data integrity, reduce data duplication, normalize data representation to an extensible vendor-agnostic schema and enrich security data with organizational information to unlock actionable insights through a security, risk and compliance data fabric platform approach.

### Rate how well your security team currently meets the needs of the business

Security team strengths tend to be monitoring, incident response and security compliance; there's opportunity for improvement in real-time compliance monitoring, privacy auditing, threat hunting and risk assessment.