



# THREE STEPS TO UPLEVELING YOUR CYBERSECURITY DATA STRATEGY



CHAMPION  
GUIDES

EBOOK

# TABLE OF CONTENTS

- 3** Introduction
- 4** Step 1: Take control of your data
- 6** Step 2: Conduct proactive threat hunting across all your data
- 7** Step 3: Foster collaboration with your data team
- 9** Conclusion: A successful cybersecurity program requires having a modern data strategy
- 10** About Snowflake

# INTRODUCTION

Security organizations can benefit from existing data platform investments in order to more successfully deal with threats and reduce risk for the business.

Can better access to data resolve a billion-dollar contradiction in the cybersecurity industry? According to **Gartner**<sup>®</sup>, an estimated \$150.4 billion was spent worldwide on information security and risk management technology and services in 2021. Just 15 years ago, that number was a mere \$3.5 billion, reported by **Cybersecurity Ventures**. Yet, cybersecurity breaches have reached record levels and the stakes have never been higher. **IBM** estimates a single data breach can cost organizations, on average, \$4.2 million, which is the highest figure in the 17 years IBM has been reporting on data breaches.

This contradiction between investment and outcome is a result of the growing asymmetry between threat actors and the teams defending against them. Threat actors have quickly adapted to enterprise trends such as dynamic cloud infrastructure, interconnected software supply chains, and a workforce operating largely outside the office perimeter. They take advantage of the scale and complexity of their targets to gain access and remain undetected until they achieve their objectives. Security teams, meanwhile, are largely trying to make sense of the new enterprise environment and threat landscape using outdated solutions.

At the same time that defenders were falling behind in the race to secure the business, other departments enjoyed dramatic gains made possible by innovation in the modern data stack. As such, an

opportunity has emerged for defenders to leapfrog their adversaries by treating cybersecurity as a data problem. Successful cybersecurity organizations will be those that mobilize data across sources and time without limitations and with the full benefit of advances in data platforms and analytics.

At the heart of this new strategy is the adoption of a centralized security data lake, enabled by a modern cloud data platform. A security data lake enables organizations to remove traditional limitations on visibility and cost constraints related to how much data you can ingest, store, and retain, and for how long. Support for standard analytics languages such as SQL and Python is also crucial, enabling collaboration between security analysts as subject matter experts, data analysts for self-service reporting, and data scientists for behavioral models and machine learning. And support for granular access controls and secure data sharing to enable collaboration within an organization, between industry peers, and with third-party data providers, are all critical aspects of today's security data lakes.

In the pages that follow, we'll share three proven steps you can take to successfully transition to a data-driven cybersecurity strategy.

# STEP 1: TAKE CONTROL OF YOUR DATA

Controlling your data means having freedom—freedom to ingest and retain as much data as you want, freedom to analyze recent and historical data sets, and the freedom to choose which security solutions will support your mission to protect your business.

## CHALLENGE: TRADITIONAL SIEMs LIMIT DATA FREEDOM AND CONTROL

Most security teams use a security information and event management (SIEM) solution for threat detection and incident response. The SIEM is the source of truth for the security program. However, legacy SIEMs are vertically integrated and require the use of their built-in, proprietary databases. These vendors have unsurprisingly failed to keep up with the performance and scalability of general-purpose cloud data platforms, and operate as an independent data stack for cybersecurity—off to the side from the rest of the business.

As a result, security teams must contend with rudimentary analytics and fragmented data silos. Some security data can be searched some of the time, but can't be combined easily with contextual data, which could include business data or any other data that will provide security teams with greater context about a potential threat. Security data alone is not enough to thoroughly assess potential threats.

Moreover, the steep licensing costs of traditional SIEMs force their users to increasingly store security data elsewhere—especially in cloud buckets that only solve the storage problem. This approach introduces cumbersome processes and overhead when these data sets must be integrated for analysis, lengthening response times during a breach, and failing to support key use cases such as threat hunting and threat intelligence. Data governance challenges compound the problems of data sprawl in the form of self-managed storage tiers.



## SOLUTION: CENTRALIZE ON A CLOUD-BUILT SECURITY DATA LAKE

A modern security data lake is a repository where logs and other data sets are stored in cheap, near-limitless cloud storage where they can be quickly analyzed. Modern data lakes are designed to provide centralized, secure access to an organization's data. A multitude of immediate benefits can be realized when organizations centralize their security data in a single platform, including:

- **The ability to cost-effectively ingest and retain petabytes of event logs**
- **The opportunity to integrate security data with business and application data for contextualizing and eventually automating security operations**
- **The freedom to conduct investigations without knowing in advance which data records may be relevant or having to retrieve historical data from cold archives**
- **The power to control which vendors have access to which data sets**
- **The flexibility to migrate security solutions without having to move the collected data**

A modern security data lake can enable teams from across the enterprise to access the same single source of truth for multiple cybersecurity use cases: threat detection and response, vulnerability management, compliance automation, and board-level risk reporting.

Beyond enabling and accelerating security program initiatives, a modern security data lake can drive cost savings and budget efficiency. Cheap storage with compression at rest means lower storage costs. Even more significant is the elastic and near-infinite compute power provided by leading cloud data platforms. Gone is the need to over-provision resources. Platforms that combine compute elasticity with consumption-based pricing enable customers to pay only for the resources they need, when they need them. In the cybersecurity context, where you often need a little power but occasionally need a lot of it, that model dramatically frees up the security budget for other uses.

Implementing a modern, cloud-built security data lake can prove transformative for an organization. By housing your data in a single platform, your security teams have an opportunity to simplify your technology stack, consolidate disparate data stores, and enable advanced analytics across multiple use cases. Governance features and centralized auditing provide guardrails, while data collaboration opportunities boost overstretched security teams to succeed in their critical initiatives for years to come.



# STEP 2: CONDUCT PROACTIVE THREAT HUNTING ACROSS ALL YOUR DATA

The threat landscape is rapidly evolving, with enterprises increasingly dependent on third parties across supply chains and SaaS-based infrastructure. A posture of “assume breach” is necessary for mitigating the resulting risk to your business. Unfortunately, most security teams rely on a “hard shell, soft center” approach from which threats that get past initial defenses can persist inside your environment for months. This dangerous status quo is largely a result of limitations imposed by legacy SIEM solutions.

## CHALLENGE: THREAT HUNTERS DON'T HAVE ACCESS TO THE DATA AND ANALYTICS THEY NEED

While basic threat detection can be performed in real-time as event logs are collected, advanced detections and proactive threat hunting require a combination of data sets across sources and timeframes. Threat actors, especially once they have a foothold in the environment, have a major advantage and plenty of places to hide. This is what makes threat hunters so potentially valuable to enterprise security programs.

Unfortunately, threat hunters can't succeed if they are unable to get answers to their questions. When data is siloed in various source systems, locked away in cold storage, or lost to retention policies, threat hunters

can't use it. Threat hunters are also held back when their queries take hours to run, their searches return cryptic “out of memory” error messages, or they run into resource contention with other teams.

Finally, most legacy security products restrict queries to proprietary search languages or rudimentary grep/regex techniques. This introduces a learning curve for new team members and keeps threat hunters from being able to properly express their hypotheses as code.

## SOLUTION: EMPOWER THREAT HUNTERS WITH A CLOUD DATA PLATFORM THAT SUPPORTS ANALYTICS AT SCALE

A cloud-built data architecture that underlies a security data lake and eliminates data silos is key to enabling proactive threat hunting. Once established, experienced security analysts can quickly begin to uncover latent threats using standard, universal analytical techniques. Given a sufficiently performant query engine, threat hunters can work across months' or years' worth of data measured in the petabytes.

Even more junior members of the security operations team can participate through a partnership with data analysts from across the enterprise. While data analysts would never be able to help with threat hunting in a niche, security-only environment, they are adept at turning business logic into SQL within the familiar enterprise data platform. More on that later.

Further threat hunting gains are enabled by cloud data platforms that offer a data marketplace with threat intelligence listings. Data marketplaces built on modern data sharing technology can enable threat intel vendors and research organizations to publish indicators of compromise (IOCs) and other intel products for near-instant consumption. Security teams that consume intel feeds in this way are able to seamlessly apply up-to-date IOCs to their log data automatically. In this way, threat hunters and automation tools can reliably spot known bad actors without the overhead of API integrations or manually looking up indicators in a portal.

The ways in which this approach empowers threat hunters are representative of the big opportunity that cybersecurity has in aligning to the enterprise-wide data strategy: As new data analytics capabilities and methodologies emerge, the defenders will increasingly shrink the bad actors' advantage.

# STEP 3: FOSTER COLLABORATION WITH YOUR DATA TEAM

The fastest growing organization at many enterprises is the data team. Data analysts, data engineers, and data scientists are key enablers for marketing, finance, and other departments in your organization. Now, security leaders are putting in place the technology and processes that enable detecting threats and reducing risk through collaboration between the security and data teams.

## CHALLENGE: SECURITY TEAMS SPEND TOO MUCH TIME ON NON-SECURITY WORK, INCLUDING DATA COLLECTION AND REPORTING TO STAKEHOLDERS

When your team is stretched thin trying to keep up with attackers, it doesn't make sense for them to spend time on anything that doesn't require their expertise. Instead of triaging alerts or investigating threats, many security teams spend large portions of their time chasing down data, updating spreadsheets, or bringing search clusters back to life.

Security also plays an important role in the certifications and audits that businesses must maintain in order to sell to their customers. These can become big burdens when they translate into cybersecurity teams engaging in endless meetings between stakeholders across compliance, IT, DevOps and leadership.

From three decades and two vastly different approaches of enabling effective data analytics, the modern data platform has emerged. It represents the power of traditional data warehousing, the flexibility of big data solutions, and the elasticity of the cloud at a fraction of the cost of previous solutions.



## **SOLUTION: FORM A PARTNERSHIP BETWEEN SECURITY ANALYSTS AND DATA PROFESSIONALS TO SECURE THE ENTERPRISE TOGETHER**

Review the different ways in which the security team is spending its time. Which tasks don't require their subject-matter expertise? Of these tasks, which are primarily concerned with preparing, analyzing, or reporting on data? Engage your peers in the data organization in an open discussion about these areas for collaboration.

For example, collecting HR records for enrichment in detection and response may be a data pipeline task best performed by data engineers. Measuring security patching SLA performance is straightforward for data analysts. And identifying unusual file movements given the proper activity logs can be a walk in the park for data scientists.

Integrating security data with the rest of the organization sets the foundation for a partnership between security teams and data professionals. This collaboration can dramatically enhance an organization's ability to achieve high-fidelity security analytics, while making the most of the talent they have within the enterprise.

Self-service business intelligence (BI) reports can be a great way to eliminate meetings and take strapped security teams out of the critical path of routine company processes. For example, a typical patch management program may involve security engineers evaluating the risk of vulnerability findings, and compliance analysts prioritizing the remediation of those findings. That prioritization could be based on where the issues exist (customer-facing production vs internal sandbox, for example) and how long they've been around. Those considerations are a product of compliance frameworks that the business must adhere to if it is to continue serving its customers.

Actionable dashboards that apply business logic and contextual data sets to security issues in an automated, timely fashion can empower remediation teams to fix issues without meetings. Status updates are also eliminated when any authorized individual can see the latest status in the enterprise BI tool. Data analysts routinely make this happen for other departments, which means you can bring this digital transformation to your security organization.

This approach shifts cybersecurity from being a compartmentalized, reactive practice to a broad collaboration for solving problems with data-driven solutions.

# CONCLUSION: A SUCCESSFUL CYBERSECURITY PROGRAM REQUIRES HAVING A MODERN DATA STRATEGY

You've now learned three proven steps to upleveling your cybersecurity data strategy. This is an essential part of protecting a modern, cloud-scale organization from cyber threats.

To be successful, your security analysts need a modern security data lake, enabled by a cloud data platform and delivered as a service, for fast access to relevant data in a central location. This is as true for large, sprawling enterprises as for fast-moving startups. A single breach event for any type of organization could mean game over.

Remember that your cybersecurity teams should no longer operate on their own, away from the data tooling and expertise now present in virtually every enterprise. Security leaders can set a foundation for their team to leverage expertise from other parts of the organization and thereby focus on cybersecurity elements that no one else will handle.

By following the three steps outlined in this ebook, you can move from reactive cybersecurity management to increasingly support proactive approaches such as threat hunting and self-service reporting. Over time, a data-driven approach will enable your cybersecurity organization to reach its full potential and successfully translate security investments into greater assurance for your business and its customers.





## ABOUT SNOWFLAKE

Snowflake delivers the Data Cloud—a global network where thousands of organizations mobilize data with near-unlimited scale, concurrency, and performance. Inside the Data Cloud, organizations unite their siloed data, easily discover and securely share governed data, and execute diverse analytic workloads. Wherever data or users live, Snowflake delivers a single and seamless experience across multiple public clouds. Snowflake's platform is the engine that powers and provides access to the Data Cloud, creating a solution for data warehousing, data lakes, data engineering, data science, data application development, and data sharing. Join Snowflake customers, partners, and data providers already taking their businesses to new frontiers in the Data Cloud. [snowflake.com](https://www.snowflake.com)



© 2022 Snowflake Inc. All rights reserved. Snowflake, the Snowflake logo, and all other Snowflake product, feature and service names mentioned herein are registered trademarks or trademarks of Snowflake Inc. in the United States and other countries. All other brand names or logos mentioned or used herein are for identification purposes only and may be the trademarks of their respective holder(s). Snowflake may not be associated with, or be sponsored or endorsed by, any such holder(s).

---

### CITATIONS

<sup>1</sup> Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021

<sup>2</sup> Global Cybersecurity Spending To Exceed \$1.75 Trillion From 2021-2025