snowflake®

POWERED BY snowflake
NEXT GENERATION CYBERSECURITY APPLICATIONS
2023

THE NEXT GENERATION OF CYBERSECURITY APPLICATIONS

How AI, ML, search and analytical applications are developed and deployed to transform enterprise cybersecurity.

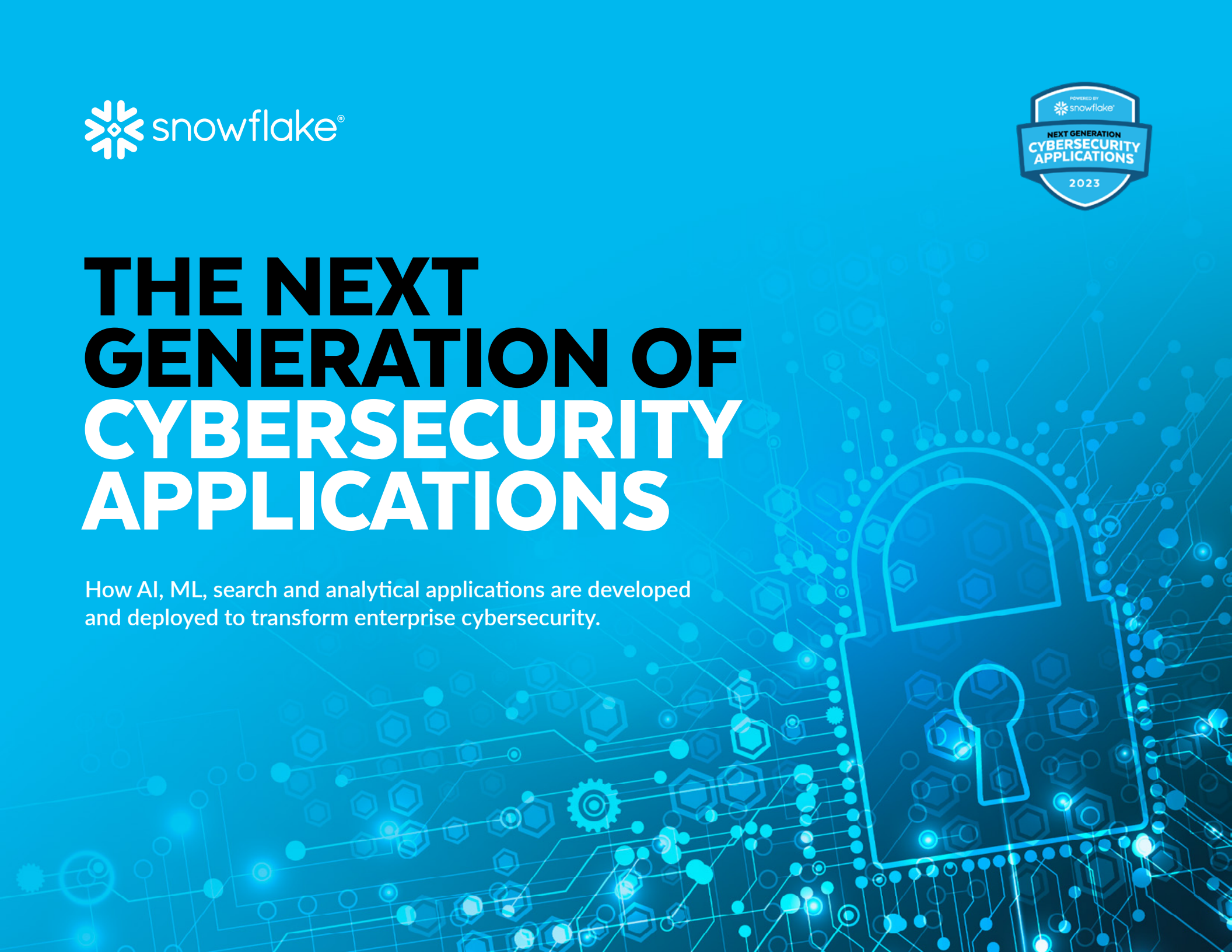


TABLE OF CONTENTS

A DATA-BACKED REPORT

The cybersecurity landscape is always changing with the increasing volume, variety and velocity of data. To help security teams stay ahead of adversaries, cybersecurity providers need to effectively turn large datasets into actionable insights, quickly deliver features to streamline and automate security operations, and confidently ensure high software reliability and scalability.

Cybersecurity solutions that maintain customer data in distinct silos, away from the rest of the organization's data, present a myriad of challenges. There is an urgency for cybersecurity providers to build solutions that connect to the security team's security data lake strategy.

Using aggregated usage data (See Appendix: Detailed Methodology), this report identifies cybersecurity providers currently using Snowflake to power their applications who are leaders and ones to watch across five categories that are leading in adoption among enterprise security teams.

The five categories evaluated — security information and event management (SIEM), cloud security, compliance, emerging segments (e.g. email security) and data enrichment — are ripe for transformation. Security teams require more effective detection and response capabilities, more holistic workload protection as more organizations migrate to the cloud, and increased automation for audits. The cybersecurity providers highlighted in this report are offering security capabilities to their customers, allowing those customers to achieve better data outcomes.

This report, which focuses on companies that are active members of the Snowflake Partner Network (or ones with a comparable agreement in place with Snowflake) or Snowflake Marketplace providers, explored each category that security teams generally need to to enable to ensure they protect their organizations amid the modern threat landscape.

MODERN SECURITY SOLUTIONS FOR THE EVOLVING THREAT LANDSCAPE

THE EMERGENCE OF NEXT-GENERATION CYBERSECURITY APPLICATIONS

We're seeing the emergence of a new class of cybersecurity applications. These next-generation cybersecurity applications are designed to connect directly to the customer's security data lake.

This class of cybersecurity applications stands in stark contrast to prior versions, which typically followed a more siloed approach, forcing security teams to ingest raw logs into multiple point products, creating multiple copies of siloed data. To bridge the gap, the industry has sought a more versatile model that allows customers to run multiple applications on the same data, which serves as a single source of truth. This new model provides enhanced data quality, eliminates data silos and helps reduce operating costs for security teams.

THE MOST COMMON DESIGNS INCLUDE:

CONNECTED APPLICATION MODEL

The cybersecurity application reads, writes and queries data in the customer's security data lake. The end-customer doesn't need to move or copy data, reducing data silos and improving governance and security.

MANAGED APPLICATION MODEL WITH DATA SHARING

The cybersecurity application uses their own data platform to read, write and query data. The application uses secure data sharing to bi-directionally share live, ready-to-query data with the end-customer.

SNOWFLAKE NATIVE APPS

Snowflake Native Apps are applications that run entirely in a customer's Snowflake. This is a new and emerging type of application.

NEXT-GENERATION CYBERSECURITY APPLICATIONS NEED A PERFORMANT CLOUD DATA PLATFORM

Cybersecurity providers today struggle with complex data management and scalability. A primary reason is that legacy security vendors built on-prem solutions and tried to Band-Aid them into the cloud over time. But these problems don't scale — organizations have been unable to handle the explosion of data volumes that come with a world shifting to the cloud.

Many cybersecurity providers are looking for a cloud-native database that can support the growing data volume and the ability to query logs quickly to deliver value for their customers. They are looking for a single platform to support the entire suite because it brings the security products to a common data model, allowing the different products within the suite to share insights, analytics and more.

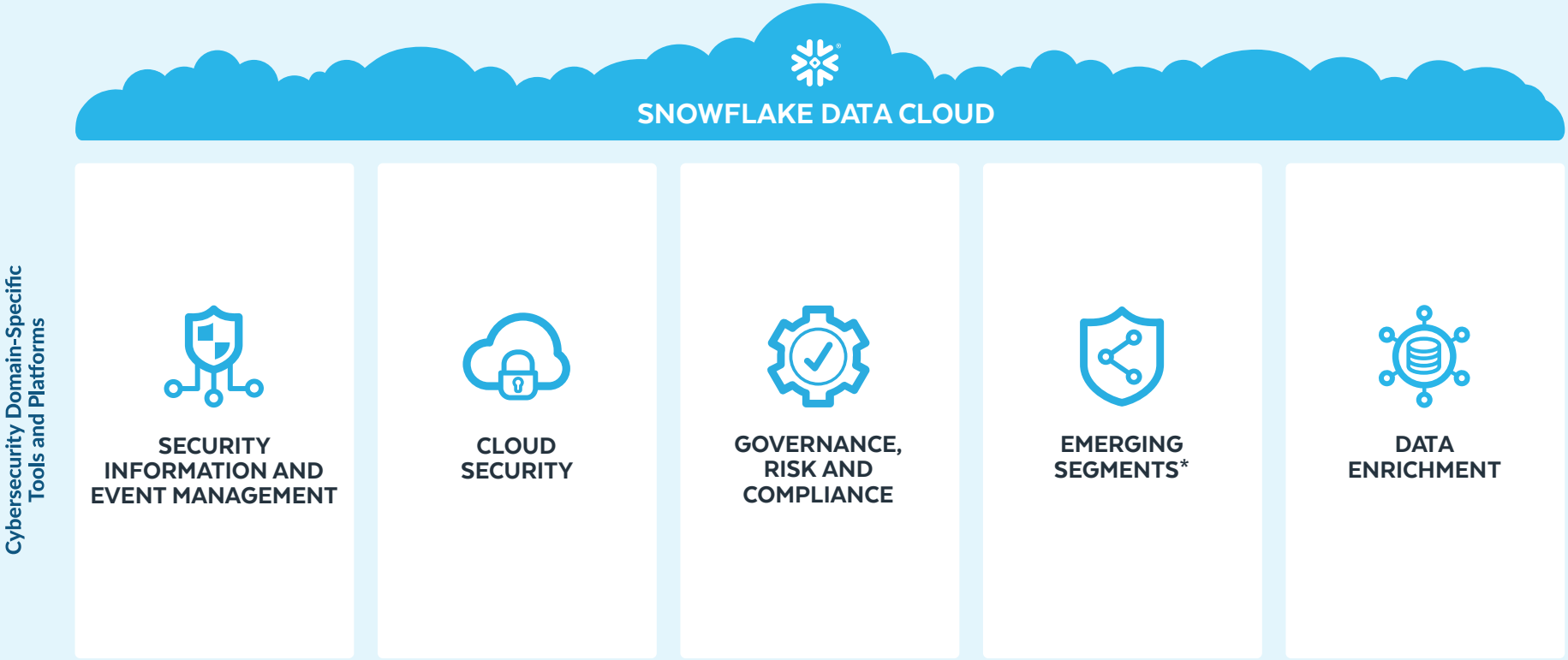
They need a platform that delivers performance and scale for app components specifically in analytics, search, streaming and AI. Scalability is key to keep the security focus on innovation, rather than infrastructure management, thereby reducing operational costs and ultimately increasing their bottom line. In reality, though, most cybersecurity applications today continue to have multiple back ends that support various parts of the application — keeping teams mired in infrastructure management.

Security applications Powered by Snowflake have begun to overcome this common barrier by delivering the functionalities security teams need to be more effective. With near limitless scale and performance, coupled with innovative tools that support streaming analytics, AI and machine learning and fast search, cybersecurity providers can remain focused on delivering top-notch security capabilities to their customers.

The three main challenges why the security industry needs next-generation cybersecurity applications today:

- The **poor scalability** of today's security tools makes it hard for security vendors to onboard new customers and new data sources.
- Solutions with **complex and siloed architectures** require cumbersome infrastructure management and prevent engineering teams from building better products and features to protect consumers.
- Security customers who rely on traditional security platforms with siloed data are **more susceptible to threats**.

The importance for modern cybersecurity applications is growing because legacy systems can't keep up with modern threats. This is causing organizations to accelerate their move to the cloud and their security teams to demand their providers align with their security data lake strategy.



* See Appendix: Detailed Methodology for additional details on selection and categorization of the referenced technologies.

THREE CYBERSECURITY MARKET TRENDS

These trends provide insight into the emergence and adoption of next-generation cybersecurity applications.

1 Cybersecurity providers are bringing their applications to the customer's data.

To prevent customers from the ineffective legacy approach of loading their logs into multiple data silos, cybersecurity providers are building solutions that plug directly into the customers' security data lake. This new architecture model helps vendors reduce infrastructure management and costs while giving customers control of their data. Customers can reduce data silos by having a single source of truth, using applications that read from a centralized data source. Customers are beginning to adopt this new model where there is a separation between their data vault and the security applications that deliver features and capabilities. A core benefit to this model is it prevents cybersecurity providers from holding a set of keys to the customer's data, and offloads data ownership and storage costs back to the customer.

2 Cybersecurity providers are building new, more secure AI and ML capabilities into their product, without typical architectural complexity.

Instead of spinning up a new tech stack to run AI and machine learning workloads, data scientists and app developers are joining their data teams in building these features on a single data platform. This results in faster implementation of AI features for customers — such as copilot with automated suggestions and LLM-powered chat boxes that turn traditional queries into natural language questions to speed up investigations. This also helps cybersecurity providers building on a data platform that supports ML workloads more easily test and deploy ML detections and anomaly detections.

3 Customers want solution providers to share insights back to their security data lake, without APIs or ETLs.

Context is important for making timely security decisions. Security analysts cannot protect their organization without the ability to correlate across datasets or insights. Cybersecurity providers understand this need and are supporting their customers' security data lake strategies by building secure data-sharing capabilities that do not require APIs, ETLs or other tools for transferring data. These direct shares from vendor to customer remain private, secure and governed.

CYBERSECURITY APPLICATION PROVIDERS AND DATA PROVIDERS

Cybersecurity Domain-Specific Tools and Platforms

SECURITY INFORMATION AND EVENT MANAGEMENT

LEADERS

HUNTERS
panther
securonix

ONES TO WATCH

ANVILOGIC
ELYSIUM Analytics
GURUCUL

CLOUD SECURITY

LEADERS

LACEWORK
tenable
WIZ

ONES TO WATCH

Gem
orca security

GOVERNANCE, RISK AND COMPLIANCE

LEADERS

CyberSaint SECURITY
DataBee

ONES TO WATCH

anecdotes

EMERGING SEGMENTS*

LEADERS

Application Security
snyk

Bot Detection
HUMAN

Email Security
Material Security

ETL
DASSANA
monad

Identity
dORT now part of CISCO

DATA ENRICHMENT

LEADERS

ipinfo.io

ONES TO WATCH

KELA
Panorays
Security Scorecard

* See Appendix: Detailed Methodology for additional details on selection and categorization of the referenced technologies.

SIEM

SIEM solutions help security teams with compliance, threat detection and security incident management, by gathering and studying both past and present security events, along with several other data sources. The main capabilities include collecting and organizing log events, analyzing these events and data from different sources, and assisting with tasks like threat detection, incident response and creating reports. These next-generation cybersecurity applications, Powered by Snowflake, have a modern approach to detection and response.

LEADERS

HUNTERS

An alternative to legacy SIEM solutions, the Hunters SOC Platform empowers security teams to automatically identify and respond to security incidents across their entire attack surface. Hunters uses Snowflake features, like Snowpipe, to remove data engineering challenges around ingesting security data into the Snowflake Data Cloud. The Hunters platform delivers built-in, regularly updated, detection capabilities, increasing the effectiveness of threat detection and eliminating the need to regularly build and maintain detection rules. With Hunters, security teams can focus on their unique use cases, knowing that Hunters' detectors cover the majority of the threat landscape. The Hunters platform automates the correlation of signals and alerts from various sources — such as endpoint, detection and response (EDR), and cloud and identity — as well as the triage and investigation process — to minimize the time to respond and contain threats. Powered by Snowflake, Hunters helps security professionals overcome volume, complexity and false positives. Learn more at *hunters.security*.

PANTHER

Integrating the Snowflake Data Cloud with Panther's cutting-edge detection-as-code methodology enables organizations to swiftly ingest, process and fortify their data, ensuring unmatched visibility and top-tier security. Panther seamlessly consolidates all security data within Snowflake, streamlining the normalization, enrichment and operationalization processes. This powerful synergy equips teams to detect and address threats with speed and precision. With Panther and Snowflake, your organization can establish a robust data-centric security framework, heightening security measures at scale while maintaining agility, cost efficiency and comprehensive end-to-end visibility.

SECURONIX

Securonix Unified Defense SIEM integrates with Snowflake's Data Cloud and transcends traditional SIEM limitations by offering an elevated security operations platform. This fusion facilitates seamless scalability amidst burgeoning data volumes without compromising performance. Securonix delivers immediate threat detection and response, courtesy of ready-to-use content, while utilizing Snowflake's capabilities for deploying advanced analytics. This allows security teams to fine-tune threat detection and minimize false positives. The Securonix Unified Defense SIEM platform's provision of 365 days of hot searchable data is invaluable for thorough investigations and effective threat hunting. It also promotes a collaborative defense culture, enabling intelligence sharing and autonomous threat sweeps. Through a unified workflow and a streamlined interface, Securonix on Snowflake harmonizes scalability, precision and collaborative defense, redefining threat detection and response.

LEADING MDRS EMBRACE THE DATA CLOUD

Managed detection and response (MDR) is a cybersecurity service that brings technology and human knowledge together for threat hunting, security monitoring and incident response.

MDR providers manage petabytes of customer data and run an exorbitant number of queries a day to detect, investigate and remediate threats. They need a reliable and performant data platform to power their applications and capabilities. **ReliaQuest**, a leading MDR provider, is a prime example of a successful partnership with Snowflake. ReliaQuest GreyMatter, a security operations platform, uses Snowflake to provide analysts with faster search, holistic visibility and scalability — enabling accelerated threat detection and response.

"With Snowflake as our data layer, we're able to store more data, process more telemetry, and respond to alerts faster than before. This allows us to drive better security outcomes for our customers," said Brian Murphy, chief scientist, Reliaquest. "Snowflake's multi-region and multi-cloud support also allows us to serve customers across the globe without any complexity. We trust that Snowflake will save us time, cost and headaches as we continue to roll out new features into different geographical regions."

By leveraging Snowflake as the data platform, Reliaquest GreyMatter delivers better security outcomes and is prepared to meet their customers' requirements today and tomorrow.

LEARN MORE

ONES TO WATCH

ANVILOGIC

Anvilogic's AI-powered Detection Engineering and Hunting Platform separates analytics from your data layer, giving you the choice to adopt a security data lake strategy (Snowflake) at your own pace alongside your SIEM or in place of it without disrupting current investments and productivity. It results in up to 80% cost savings while enabling teams to automate the end-to-end threat detection lifecycle across disparate data lakes and tools that let you gain more coverage and a continuous view into your detection posture against your highest-priority threats to reduce risk.

ELYSIUM ANALYTICS

Elysium Analytics seamlessly integrates with Snowflake's Data Cloud through the Snowflake connected application model, providing an extensive SIEM, Security Analytics and Observability platform that enables users to maintain complete ownership and data control, eliminating vendor lock-in. Elysium replicates the Elasticsearch experience while incorporating open source, and accelerates threat hunting and investigation through unified data. Elysium optimizes every aspect of log management and analytics at scale, handling data ingestion, engineering, alerting and machine learning. Elysium leverages Snowflake's unique features, such as Search Optimization Service (SOS), Data Sharing and the Snowpark ML Modeling API. The Snowpark ML Modeling API empowers users with self-service anomaly detection, Behavioral Analysis, SIEM, Splunk optimization and compliance mapping.

GURUCUL

The Gurucul Security Analytics and Operations Platform enables customers to seamlessly run Gurucul's Next-Gen SIEM on the Data Cloud as a Snowflake Connected Application. Enterprises can consolidate all their enterprise and security data into a single security data lake with next-gen analytics for real-time threat detection and automated response, addressing data breaches and internal and external threats. Additionally, customers can leverage Gurucul to analyze, correlate and generate security alerts on data residing in Snowflake. Customers can improve SOC efficiency, reduce threat detection time, decrease manual effort through automation, and deliver analytics for automated detection and targeted threat response. Learn more about Gurucul at ***gurucul.com/technology-alliances/snowflake.***

CLOUD SECURITY

Cloud security refers to the practices, measures and technologies used to protect data, applications and resources stored or processed in cloud computing environments. It includes a range of strategies and tools used to protect cloud-based assets from unauthorized access, data breaches and other security risks.

LEADERS

LACEWORK

Lacework keeps organizations secure in the cloud, allowing them to innovate faster with confidence. Cloud security requires a fundamentally new approach, and the Lacework platform, Powered by Snowflake, is designed to scale with the volume, variety and velocity of cloud data across an organization's cloud environment: code, identities, containers and multi-cloud infrastructure. Lacework provides security and development teams with a correlated and prioritized end-to-end view that pinpoints the largest risks and handful of security events that matter most. Lacework has a deep pedigree in AI and machine learning, including nearly 200 patents and pending applications, each of which touch AI. The Lacework Polygraph® Data Platform, at the core of anomaly detection capabilities, implements unsupervised machine learning functionality to identify malicious behavior and address alerts in a customer's environment without ever writing rules. Learn more at *lacework.com.*

TENABLE

Tenable's Exposure Management platform, Tenable One, is Powered by Snowflake and combines the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps and identity systems — all within one platform that builds on the **market leadership** from Tenable Research and adds comprehensive analytics to prioritize action and communicate cyber-risk. Tenable One also includes cloud native application protection platform (CNAPP) and cloud infrastructure entitlement management (CIEM) capabilities, delivering full asset discovery, contextual risk visibility, prioritization and remediation across infrastructure and identities, both on-premise and in the cloud. In 2019, Tenable pioneered the use of AI to predict vulnerabilities most likely to be exploited, and has continued to lead with the development of generative AI-based use cases. Tenable ExposureAI is fueled by the largest repository of contextual exposure data, ***Tenable Exposure Graph***, which is a scalable data lake Powered by Snowflake that empowers security teams to focus on proactive measures and turn analysts into expert defenders. Learn more at *tenable.com.*

WIZ

Wiz's Cloud Native Application Protection Platform (CNAPP) is designed to protect everything built and run in the cloud. Wiz's agentless approach delivers instant full-stack visibility, accurate risk prioritization and enhanced business agility. With less noise, customers gain complete context about their workloads, configurations, vulnerabilities and attack paths so security teams can focus their efforts on the risks that matter most. Security teams and developers use Wiz to create a shared understanding of their cloud threats and align to resolve issues earlier in the development life cycle. Joint customers can automatically push Wiz-identified cloud security issues to Snowflake for aggregate incident investigation and analysis, accurate reporting on cloud security metrics, and easy storage that lights a path for policymakers to make informed decisions, without any of the technical overhead. Learn more at *Wiz.io*.

ONES TO WATCH

GEM SECURITY

Gem's Cloud Detection & Response (CDR) platform significantly shortens the time to detect, investigate and contain threats across your entire cloud estate (AWS, Azure, GCP). Recognized by Gartner as a Cool Vendor™ for the Modern Security Operations Center, Gem leverages the Snowflake Data Cloud to cost-effectively ingest and analyze massive amounts of log data across a broad range of cloud services (such as Control, Identity, Data and Network). Gem integrates with existing tools including SIEM, SOAR, XDR, IAM, CSPM and ticketing. Using a combination of behavioral analytics and proprietary out-of-the-box detections for sophisticated cloud TTPs, Gem's agentless platform immediately identifies suspicious and unauthorized activities, while minimizing alert noise by building behavioral profiles of users, instances and buckets. When alerts trigger, Gem automatically creates an investigation timeline to rapidly triage alerts and identify the root cause. You can also trigger cloud-native actions to contain threats including deleting users, isolating compromised instances and taking forensic snapshots.

ORCA SECURITY

Orca Security is the agentless cloud security platform that identifies, prioritizes and remediates risks and compliance issues across your entire cloud estate. Orca delivers complete cloud security with coverage across vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, sensitive data at risk, API risks, overly permissive identities, and more. Together, Orca Security and Snowflake enable organizations to seamlessly integrate Orca's context-rich cloud security data into their Snowflake data lake repositories. By combining Orca's holistic cloud security data and telemetry with other business, IT or security data within the Snowflake Data Cloud, organizations can protect their public cloud estates while consolidating their enterprise and security data into a single location, resulting in better visibility for analytics, analysis and intelligence-based incident response spanning across the entire organization's security footprint. Orca's generative AI-powered capabilities include simplified cloud asset search using natural language and automatic generation of remediation code, to enhance detection, investigation and remediation of risks. Orca leverages several AI engines, including Azure OpenAI, GPT-4, Amazon Bedrock and Google Vertex AI. Learn more at ***orca.security*** and *orca.security/partners/technology/snowflake*.

GOVERNANCE, RISK AND COMPLIANCE

Governance, risk and compliance (GRC) is a technology used by organizations to structure processes that protect their data and assets through governance, risk management and regulatory compliance practices. Changes in regulations and threats happen often, add security leaders need tools that evolve with these changes to keep threats at bay. Security leaders must have a strategy in place to empower business goals, while managing enterprise risk and meeting compliance regulations.

LEADERS

COMCAST DATABEE

DataBee puts your data at the center for dynamic, detail-rich compliance metrics and reports. The cloud-native security, risk and compliance data fabric platform weaves together security data sources with asset owner details and organizational hierarchy information, breaking down data silos and adding valuable context to cyber-risk reports and metrics. By being a connected application Powered by Snowflake, DataBee makes continuous controls monitoring (CCM) a reality by enabling customers to securely and quickly access large, historical datasets in Snowflake while driving down costs and maintaining high performance. DataBee's robust analytics enables teams across the organization to leverage the same dataset for high fidelity analysis, decisioning, response and assurance outcomes without worrying about retention limits. From executives to governance, risk and compliance analysts, DataBee on Snowflake delivers a dynamic and reliable single source of truth.

CYBERSAINT

With the CyberStrong platform, CyberSaint enables Snowflake customers to leverage their security data in their Snowflake instance to automate large swaths of cyber-risk and compliance assessments, reducing manual effort and allowing organizations to get near real-time insight into their cyber-risk posture, presented in financial terms and business context. CyberSaint's Continuous Control Automation™ pulls third-party cybersecurity data from customers' Snowflake Security Data Lake into the CyberStrong platform to automate security control scoring and the provision of evidence within either customer-specific or standardized frameworks. Users can automate up to 60% of controls for a given framework depending on the data sources in their Snowflake instance. When combined with CyberStrong's data-backed, risk model-agnostic, cyber-risk quantification, users are able to operationalize their security and telemetry data to achieve real-time insight into their measured cyber-risk posture and communicate it effectively to the board and beyond. Learn more at *cybersaint.io*.

ONES TO WATCH

ANECDOTES

anecdotes' Cybersecurity Application, Powered by Snowflake, represents a game-changing innovation in the world of compliance data processing. Addressing the need for efficient and real-time compliance reporting, anecdotes leverages the Snowflake Data Cloud to create a dynamic and agile platform. This platform streamlines the complex task of regulatory compliance, allowing companies to gather, ingest, store and analyze data quickly and effectively to manage their compliance programs. By utilizing Snowflake's data platform and data-sharing capabilities, anecdotes ensures a seamless experience for compliance professionals and eliminates the need for deep data manipulation skills. anecdotes offers significant efficiency gains by aggregating thousands of data sources per customer within Snowflake, thereby eliminating the need for manual data aggregation. The integration of Snowpipe and external automation models simplifies data processing, accelerating time-to-value for data and compliance teams.

EMERGING SEGMENTS

Emerging Segments are areas and tools that are growing in the Snowflake cybersecurity ecosystem. They may represent tools that have existed for some time but are taking on new significance because of the way these next-generation applications and tools are architected and designed with Snowflake as the underlying data platform.

LEADERS

Application Security

SNYK

Snyk empowers the world's developers to build secure applications and equip security teams to meet the demands of the digital world. Snyk's Developer Security Platform seamlessly integrates with a developer's workflow and is purpose-built for security teams to collaborate with their development teams. Snyk Reporting and Analytics Powered by Snowflake further bridges the gap between security and development teams and decreases the time-to-value of data, providing customers with the flexibility to look at data however they want. In addition, Snyk brings a unique approach to AI with DeepCode AI, combining developer security workflows with a hybrid AI security engine, securing AI-generated code as soon as it meets your application. With Snyk Reporting and Analytics Powered by Snowflake, developers can code with confidence by leveraging AI-powered security from Snyk in the Data Cloud.

Bot Detection

HUMAN

HUMAN is a cybersecurity company that protects organizations by disrupting digital fraud and abuse across the buyer's journey. Leveraging 2,500 dynamic network, device and behavioral signals through 350 algorithms (technical, statistical and machine learning), HUMAN verifies the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, helping organizations win against cybercriminals. Integration with Snowflake provides HUMAN the speed of decision making necessary to protect programmatically traded media in milliseconds. HUMAN's Snowflake integration lets customers access the full scope of data collected by HUMAN, including pre-bid IVT predictions as well as post-bid detection and analysis. Visit our website: *humansecurity.com*.

Email Security

MATERIAL SECURITY

Material Security is a unified cloud office security suite that provides real-time visibility, intelligent defenses and right-sized controls to reduce risk in Microsoft 365 and Google Workspace environments. Leveraging the power of AI along with innovative threat research, Material helps customers thwart large volumes of sophisticated email-based attacks, understand and mitigate risky user and partner behaviors, and minimize the likelihood and impact of regulated data exposure. The underlying data platform, Powered by Snowflake, continually transforms unstructured cloud office data and events into a structured data model of people, content and communications enriched with metadata and context. Together with Snowflake, Material allows customers to pinpoint and understand security gaps, supercharge threat operations and forensics investigations, and drive business intelligence via their Snowflake security data lake. Your cloud office isn't just another application, it's critical infrastructure — let's treat it as such. Learn more at ***material.security.***

ETL

DASSANA

In a world where businesses invest in numerous security tools, Dassana seamlessly brings all security data into Snowflake's Data Cloud to provide a unified view of security risks. This empowers customers to measure the efficacy of their security tools, get answers in minutes, stand behind their reporting with high-quality data and find the top priorities across distributed teams to focus on what matters most. Snowflake's Data Cloud serves as the foundation, enabling customers to take full ownership of their data. Dassana further enhances this capability by collaborating with other Snowflake ecosystem vendors to bring existing data to life through gen AI normalization. This collaborative approach ensures organizations can harness the power of their data while streamlining security operations, adhering to compliance standards like SEC 106 for 10K and 4K, and transforming cybersecurity into an efficient and effective strategy. Learn more about this partnership at ***dassana.io***.

ETL

MONAD

Monad builds data infrastructure to ingest and model enterprise-scale security data. Customers can use Monad to extract data from their most important security tools, transform it into a format that fits their needs (e.g., OCSF, Monad Object Model, custom model), and deliver it directly to their Snowflake Data Cloud for analysis. This reduces complexity and enables teams to focus on creating sophisticated security analytics. It's never been easier to build your security data lake using Monad and Snowflake. Learn more at ***monad.com*** and start using Monad today for free at ***app.monad.security.***

Identity

OORT (ACQUIRED BY CISCO)

Oort (acquired by Cisco) analyzes telemetry from your core identity and access management (IAM) systems to discover your workforce identities, protect them with best practices, and continuously detect and respond to identity threats. The platform, Powered by Snowflake, enables security teams to gain comprehensive visibility into identities and detect anomalies across enormous datasets. Visit ***oort.io*** to learn more.

DATA ENRICHMENT

Data enrichment is the process of pairing security event data with non-event data and deriving useful information to translate raw data into meaningful and actionable insights to improve an organization's security. This process gives security analysts more context about the data their security tools are ingesting and what's happening in their environment.

LEADERS

IPINFO

IPinfo helps convert internet traffic data into intelligence for thousands of customers globally, across industries, from Fortune 500 enterprises to nonprofit organizations. Cybersecurity teams and enterprise SOC departments can leverage this highly contextualized IP address data to gain comprehensive insights into the functioning, security and optimization of their organization's assets across the internet ecosystem. With datasets easily accessible in Snowflake Marketplace, forward-thinking security professionals use IPinfo's scalable data to fuel their apps and operations running on the Snowflake Data Cloud. Learn more at: *ipinfo.io/integrations/snowflake*

ONES TO WATCH

KELA

KELA partners with Snowflake to help joint customers fortify their defenses against potential threats by proactively identifying and remediating risk. KELA's technology collects and analyzes diverse cybercrime data, and KELA's Technical Intelligence automatically extracts and catalogs potentially compromised IPs and domains from cybercrime sources. By monitoring the latest compromised network assets, KELA is able to identify critical elements that threat actors exploit for cyberattacks. KELA thoroughly investigates closed forums, illicit markets, and automated cybercrime shops to provide invaluable insights and intelligence. This intelligence, available on Snowflake Marketplace in a structured, machine-readable format, ensures that organizations can effortlessly integrate and deploy this robust defense mechanism across their security apparatus to help organizations safeguard their digital landscape.

PANORAYS

One of the key challenges that today's CIOs and CISOs face is how to make security data more approachable and actionable to make risk-aware decisions. Third-party cyber-risk management is an intertwined security program with other business processes. Organizations must ensure third-party cyber-risk data is available and able to integrate with multiple business processes, such as vendor onboarding. In the sourcing process, organizations should include third-party risk data to ensure vendors with bad security posture are flagged early on. It's also critical to combine third-party security risk data with vendor financial health and legal compliance status, and alert business stakeholders to improve the effectiveness of proactive vendor relationship management. Last, by combining external vendor risk data, such as reputational monitoring and internal vendor risk data, and questionnaires and risk reviews, organizations can accurately qualify and quantify vendor risk and prioritize risk-mitigation efforts. Panorays has partnered with Snowflake to provide access to Panorays' third-party cyber-risk data through Snowflake Marketplace.
Learn more at ***panorays.com***.

SECURITY SCORECARD

Organizations across the globe rely on security ratings to understand how a company's cybersecurity posture correlates with the likelihood of sustaining a data breach. SecurityScorecard helps security teams measure their own security posture and the posture of their third- and fourth-party vendors. SecurityScorecard collects 100B+ vulnerabilities each week across 12M+ companies and uses an AI-based model to calculate breach likelihood calibrated to A-F letter grades. SecurityScorecard's easy-to-understand scores increase confidence, awareness and visibility to prove the value of a security program. Customers use Snowflake Secure Data Sharing to share SecurityScorecard security ratings directly with vendors and customers to their Snowflake account. This enables data-driven narratives on cybersecurity with benchmarks showing the impact of security risks. All this data is accessible by the "call" function within Snowflake, ensuring data remains in the customer's environment. SecurityScorecard has thousands of customers, including 70% of the Fortune 1000. Learn more at ***SecurityScorecard.com***.

CUSTOMER ADOPTION

The following section showcases examples of security teams deploying applications that connect to their data lake.

Read more customer stories here.

Figma

Figma is a cloud-based design platform that helps teams brainstorm, design and build better products together — from start to finish.

CHALLENGE

Figma's success has been fueled by multiple factors, including its commitment to data security and protecting the organization from cyberthreats. "Figma aims to be the core tool for many designers, thinkers, and project managers, and so people need to trust us to keep their data safe and available," Figma's Staff Security Engineer, Max Burkhardt, said.

Sustained growth at Figma led to the rapid expansion of customers, users, employees and security data. Security teams need proper context from a variety of security logs and business contextual data to obtain high-fidelity alerts and effectively investigate security events. However, security data is often fragmented, with data coming from identity platforms, cloud providers, SaaS applications and more.

Additionally, the costs of ingesting and retaining data in traditional SIEM solutions across the industry, forces security teams to silo security data in cold storage. This siloed data architecture ultimately limits the visibility of a security analyst. And as a result, adversaries are often identified months to a year after they have already infiltrated the organization's systems.

While fragmented logs and disjointed data lakes make it hard for teams to combine data and collaborate, for Figma's Head of Security, Devdatta Akhawe, staying ahead of security risks required a single, unified view of data. "Teams need to be able to use security tools at scale and quickly respond to security incidents," Akhawe said.

"Snowflake's ecosystem of modern security tools and programming languages enables us to do really novel, creative investigations that were previously impossible."

—Devdatta Akhawe, Head of Security, Figma

Figma

SOLUTION

Seeking to build a modern security data program, the security team discovered their data science teams at Figma had already been using Snowflake. By connecting Panther, a cloud-native SIEM tool, with Snowflake as their security data lake, Figma can store high volume datasets from multiple sources and easily query the data for further automated detections and alerts.

Snowflake empowers the security team's philosophy of "fearless logging." According to Akhawe, "Most legacy security tools would not be able to handle the growth we experienced in a way that scales reliably. Snowflake as the core of our security data program allows us to ingest all the disparate logs without worrying about scale or cost."

The key ingredients for a modern security data program include a scalable architecture to consolidate security data and an ecosystem of best-of-breed security applications to run on top of that data. Snowflake provides an all-in-one solution to help security teams focus on what really matters.

IMPACT

- **Faster investigations with greater confidence.** For example, if an employee logs into Figma's internal systems from an unusual IP address, previously that might have been a tedious, manual investigation that involves correlating employee information with security logs. Now, with business data, contextual data and security data all in one place within Snowflake, security engineers at Figma can write a simple query to combine HR employee data with endpoint and login data to determine whether or not this is a malicious attack or an employee authenticating from a new place. A simple query within Snowflake can make event correlations easier and quicker, helping remove false positive alerts.
- **Achieve faster time to value with connected applications.** Figma's security engineers prefer utilizing Snowflake-connected applications, such as Panther, to run on top of their security data lake instead of building and maintaining custom applications. With Panther as a search engine, Figma can write custom detections using SQL and Python to analyze data and correlate events across all of Figma's security data.

Clari

Clari, a revenue collaboration and governance platform, allows every revenue-critical employee to collaborate to stop revenue leak and deliver revenue precision. This enables CEOs to answer the most important question in business: “Are we going to meet, beat or miss on revenue?” In short, Clari is the only enterprise system that provides end-to-end revenue collaboration and governance.

CHALLENGE

Clari faced significant alert noise from their rules-based legacy tools. Their remediation and investigation processes required optimization, and data silos created visibility gaps. With no access to data stored in vendors, they were unable to gather actionable insights.

SOLUTION

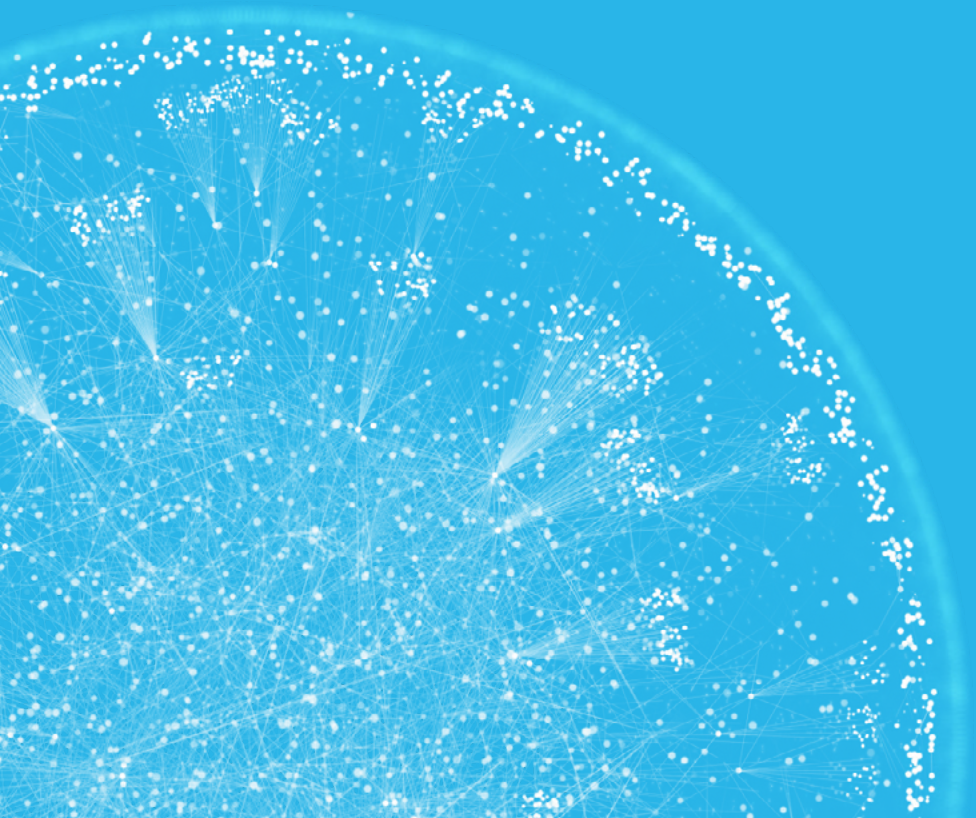
By working with Lacework and Snowflake together, Clari enriched their data and aligned security insights with business outcomes. They were able to receive the right number of context-rich, actionable alerts while gaining visibility into processes running in Java and Python applications. With access to a large library of integrations and easy deployment, both Lacework and Snowflake helped Clari to quickly streamline their security practice.

IMPACT

- Cut alerts from thousands per day to tens
- Streamlined SOC 2 and ISO 27001 compliance processes with data-rich dashboards
- Increased visibility into cloud configurations and applications
- Gained visibility into access and network patterns

THE SNOWFLAKE DATA CLOUD: THE PLATFORM FOR NEXT-GENERATION CYBERSECURITY APPLICATIONS

We've identified the key players behind the next-generation cybersecurity applications by assessing actual usage of applications that are deployed on Snowflake Data Cloud. This shows which technologies have traction among cybersecurity teams fighting against the latest cyberthreats.



One trend is clear: Snowflake is becoming a formidable application development platform of choice for many data-intensive cybersecurity applications. Many leading cybersecurity providers are choosing to build on Snowflake because the platform streamlines their application infrastructure, reducing operational complexities and cutting costs while helping ensure easy scalability. Cybersecurity providers also want to deliver new features to their customers quickly so they can stay more secure.

Application developers are also leveraging advanced features in the Data Cloud, such as rapid search, AI integration and seamless data sharing. They are tapping into Snowflake's ability to support AI-powered automation in security workflows with ease — whether users wish to automate investigations with AI and ML, or employ text-to-code with large language models (LLMs).

Snowflake's architecture is also designed for security vendors to scale seamlessly, and operates across more than 30 regions and various cloud providers, including Amazon Web Services (AWS), Microsoft Azure and the Google Cloud Platform (GCP).

LEARN WHY CYBERSECURITY PROVIDERS ARE BUILDING ON SNOWFLAKE

APPENDIX:
DETAILED METHODOLOGY

The goal of this research was to identify the technologies that were developed with Snowflake which have achieved the greatest customer adoption. The data covers a 12-month period, from Aug. 1, 2022 to July 31, 2023. The process was as follows:

Identify the full list of technologies for the cybersecurity ecosystem on Snowflake:

- We looked at the full list of Powered by Snowflake technologies that were identified as cybersecurity applications. We also looked at the full list of Snowflake Marketplace data providers that had an active listing under the "Security" filter.
- For each of the five identified categories — SIEM, compliance, cloud security, emerging segments and data enrichment — results only included those companies that were active members of the Snowflake Partner Network (SPN) or had a comparable agreement in place with Snowflake.

Split the five categories of technologies based on their type of Snowflake consumption: The multiple workloads that exist in Snowflake, combined with the optionality of different application deployment models available, means that vendors integrate with the Data Cloud in different ways and for different purposes. To accurately evaluate market leadership and adoption levels, particular metrics were applied to providers based on their type of Snowflake consumption. Specifically, the analysis consisted of splitting the technology providers into two broader categories: technologies that use Snowflake's workloads for data integration, transformation and analysis; and technologies using Snowflake's collaboration workload.

Identify key metrics

- The metrics for technologies using Snowflake's core workloads for data integration, analysis and transformation were:
  - Total number of active customers using the technology on Snowflake
  - Total credit consumption the technology uses on Snowflake
- For technologies using Snowflake's collaboration capabilities:
  - Total number of stable edges that include the technology. Stable edges are the ongoing relationships between providers and consumers of data. A stable edge is defined as a data share that has produced at least 20 transactions in which compute resources are consumed and such consumption results in recognized product revenue over two successive three-week periods (with at least 20 transactions in each period).

APPENDIX:
DETAILED METHODOLOGY

Generate an index based on the type of Snowflake usage that illustrates the level of market penetration achieved by the technology, and complement it with how deep that usage is. The calculation is based on the following weighted criteria:

- Technologies using Snowflake's core workloads for data integration, analysis and transformation:
  - Breadth (50%): number of active customers
  - Depth (50%): total credit consumption
- Data enrichment category:
  - Breadth (100%): number of stable edges, to prioritize measuring collaboration for enrichment purposes rather than size of different organizations' datasets

Rank/select the marketing technologies from 1 to N, where the lower number (ranking) is more favorable. Combine the full list of technologies across both groups and normalize this ranking between 0-100. (A score of 100 would be the technology ranked first across every metric.)

- Leaders represent the top technologies with the highest index in each category. Note that Leaders in the Emerging Segment category did not necessarily have more than 2 technologies in that category, but were selected based on multiple factors, such as strong recent momentum in the market, innovative technology or approach with Snowflake, or having recently demonstrated strong customer capabilities.
- Ones to Watch followed the leaders in their standing in primary categories such as security information event management, cloud security, compliance and data enrichment.
- There are technologies that were evaluated but are not mentioned in the report due to their decision to not participate or they were in adjacent industries such as data security, governance and observability.

ABOUT SNOWFLAKE

Snowflake enables every organization to mobilize their data with Snowflake's Data Cloud. Customers use the Data Cloud to unite siloed data, discover and securely share data, and execute diverse artificial intelligence (AI) / machine learning (ML) and analytic workloads. Wherever data or users live, Snowflake delivers a single data experience that spans multiple clouds and geographies. Thousands of customers across many industries, including 639 of the 2023 Forbes Global 2000 (G2K) as of July 31, 2023, use the Snowflake Data Cloud to power their businesses.

Learn more at **snowflake.com**