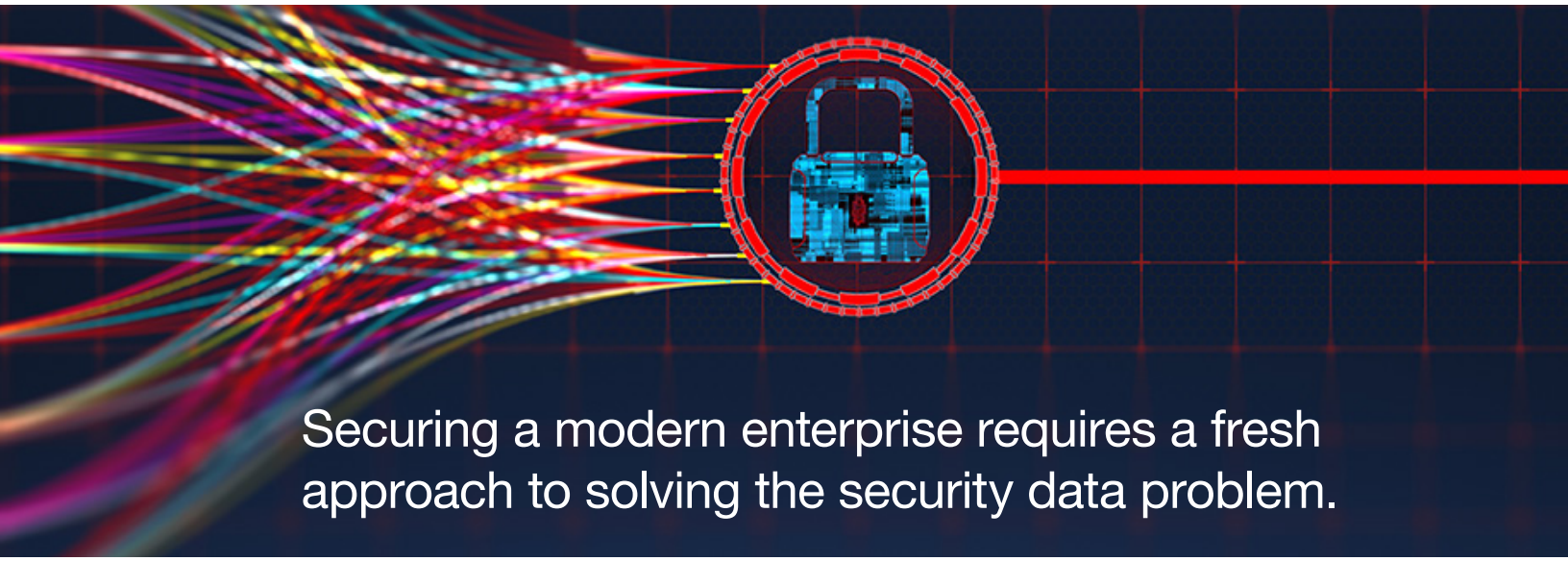
# How security data fabric is weaving a new era of cybersecurity

SPONSORED BY

DataBee™
COMCAST TECHNOLOGY SOLUTIONS

sdxcentral®



# Securing a modern enterprise requires a fresh approach to solving the security data problem.

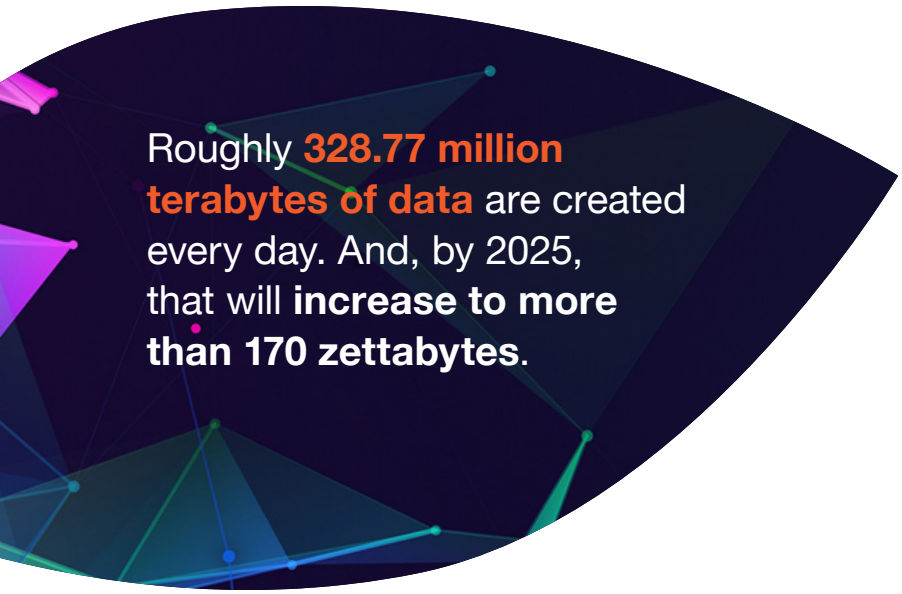
Attackers are increasingly cunning and pervasive, and security tools are sprawled all over the place. Organizations struggle to gain visibility and use their data — in the order of quintillions of bytes — to make tactical, informed decisions about cybersecurity.

In today's enterprise environment, data should talk, but it's difficult to hear above the noise.

This requires new, innovative approaches and tools that weave and join data together and finally tell a story.

## We are in the 'zettabyte era'

**HUMANITY ENTERED THE SO-CALLED "ZETTABYTE ERA" (THAT'S A BILLION TRILLION BYTES) IN 2012.** Untold amounts of data have been collected in the decade-plus since: Roughly 328.77 million terabytes of data are created every day, and by 2025, that volume is expected to increase to more than 170 zettabytes.




This accumulation of data is only accelerating with the rapid evolution and proliferation of artificial intelligence (AI) and machine learning (ML) tools. In its Top Trends in Enterprise Data Storage 2023 report, Gartner states that "by 2028, large enterprises will triple their unstructured data capacity across their on-premises, edge and public cloud locations, compared to mid-2023, a veritable proliferation of unstructured data, such as text, images and videos."

But this mind-boggling amount of "big data" isn't just being collected for the sake of it, nor is it irrelevant to modern enterprises — quite the contrary. It is extremely insightful and critical to an organization's operations, particularly when it comes to cybersecurity.

# A sprawling cybersecurity landscape

**THE CYBERSECURITY LANDSCAPE IS MORE PERILOUS THAN IT HAS EVER BEEN.** The cost of a data breach now sits at $4.45 million, a 15% increase over three years — and that's not counting the unquantifiable cost of reputational harm caused by ransomware or other attacks.


In the face of all this, CISOs have many questions to answer:

- **If their organization was attacked, how long was the threat actor on the network and what information did they take?**
- **Are endpoint detection and response (EDR) tools deployed where they should be? If not, what assets aren't deployed and who owns them?**
- **Do high-risk users have multifactor authentication (MFA) activated? Are there easy workarounds for either verified users or malicious actors?**

To answer these questions, CISOs need data, and lots of it. Up to this point, the "solution" has been to throw more and more tools at the problem, but these noncohesive, point solutions can leave more questions than they answer because data remains disconnected.

# Too many cybersecurity tools clutter the landscape

**IT'S ESTIMATED THAT ENTERPRISES USE ANYWHERE FROM 45 TO MORE THAN 130 SECURITY TOOLS.** These cover everything from data protection, to identity management, to risk and compliance, to network, cloud, app, network and data center security (and more).

Enterprises struggle to understand what kinds of data all these tools generate — and you can't capture what you don't know exists. For security vendors to prove their value in the technology stack, they often provide a security score, but proprietary and black box algorithms leave customers uncertain why or how certain scores are processed.

When security teams bring these scores to the business, you risk arguments within teams because there is no trust in the data that creates these scores.

# SIEM helps, but it's not enough

**SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) ATTEMPTS TO WRANGLE THE MULTITUDE OF TOOLS AND PUT THEM TO WORK.** SIEM platforms collect and analyze log and event data generated by various security tools in an enterprise environment.

While these platforms are important, they are expensive (particularly when it comes to high volumes of data), inflexible and not suited for parallel compute scenarios.

So even with SIEM, security continues to play catch up. And ultimately, SIEMs work great — until they don't.

# Mounting regulatory and compliance pressures


**DEPENDING ON THEIR INDUSTRY, ORGANIZATIONS HAVE TO DEAL WITH A MULTITUDE OF COMPLIANCE REQUIREMENTS AROUND VARIOUS TYPES OF SENSITIVE DATA.** And now, they are also facing increased regulatory pressure.

Notably, in the U.S., new Securities and Exchange Commission (SEC) cybersecurity disclosure rules require public enterprises to report "material" incidents within four business days. (The material phrasing is very much open for interpretation, so it's important to err on the side of caution.)

Also critically, public companies must now outline in their regular Form 10-K their process for assessing, identifying and managing such material risks. They must also describe their board of directors' oversight and expertise.

As a stark indicator of how serious federal agencies are getting about cybersecurity, the SEC recently charged software giant SolarWinds and its former CISO Timothy G. Brown with fraud stemming from the insidious Sunburst software supply chain attack that began in 2019 (and whose full effects are still unknown).

The costs of falling out of compliance can be steep, and now cybersecurity missteps can lead to criminal charges for CISOs and other individuals, too.

# Introducing security data fabrics

**A NEW APPROACH HAS EMERGED TO HELP COMBAT THESE ISSUES:** Security data fabric.

What is it and how is it different from the multitude of other cybersecurity tools? Those familiar with data engineering and infrastructure will recognize the term “data fabric.” The concept has been around for some time and has been used effectively for non-security data consumers and applications.

A data fabric centralizes, normalizes and correlates data from disparate sources to produce a connected dataset that yields comprehensive business answers. Through its composable and flexible architecture across hybrid and multi-cloud environments, the fabric makes data ready for multiple applications by data consumers across an enterprise.

Data fabrics are an efficient approach to modernizing data integration and management because they address data challenges such as un-actionable data analytics results, and rising costs for storage and compute.

Security data fabrics apply this concept directly to security, where data has been notoriously difficult to parse, understand and use. Multiple data users can use a security data fabric to reveal business-relevant security data connections.

Analyst firm Gartner describes data fabric as “an emerging data management design for attaining flexible, reusable and augmented data integration pipelines, services and semantics.”

The firm also predicts that by 2024, data fabric deployments will quadruple efficiency when it comes to data usage, and will cut human data management tasks in half.

# Getting data ‘right’ upstream

**TRUE TO ITS NAME, DATA FABRIC TAKES “THREADS” OF DATA AND WEAVES THEM TOGETHER.** Applying this concept to security involves discovering business and security relationships by weaving together traditionally separate and disparate data sources continuously.

Datasets, data sources and logs from various security tools across a data stack are combined into a single fabric. Those are then standardized and made shareable and searchable for analyses, monitoring and reporting.

Weaving together business logic with security data in an automated and continuous fashion allows for critical context and quick (and more accurate) action. This enables enterprises to get data “right” upstream and solve problems that many other tools (including SIEMs) fail to do.

Security data fabric platforms can help address issues with visibility by converging data from dissimilar or competitive solutions.

Regardless of where an analyst is, they can access and collaborate on a dataset to answer critical cybersecurity questions. This can help enable a global data strategy, with users across a system answering questions with context.

# Key use cases for security data fabric platforms

**SECURITY DATA FABRIC COMBINES ALERTS FROM DIFFERENT SIEMS SO THAT THEY AREN'T OVERLOOKED OR OUTRIGHT MISSED.** This provides cleaner data and creates a more distinct, complete picture of the cybersecurity landscape.

Notably, a security data fabric platform's robust and modular architecture offers data consumers multiple use cases like compliance.

When choosing a security, risk and compliance data fabric, companies should make sure they can accomplish the following:

- **Weave together asset owner information and security logs with IT data, business policies and organizational hierarchy.**
- **Gain visibility into data health.**
- **Prepare data for advanced analytics and reporting (without manual intervention).**
- **Tackle challenges around vulnerability management.**
- **Meet compliance requirements, such as for continuous controls monitoring (CCM) and payment card industry (PCI).**
- **Prepare data for AI applications.**

# Gaining a comprehensive understanding of users and device timelines

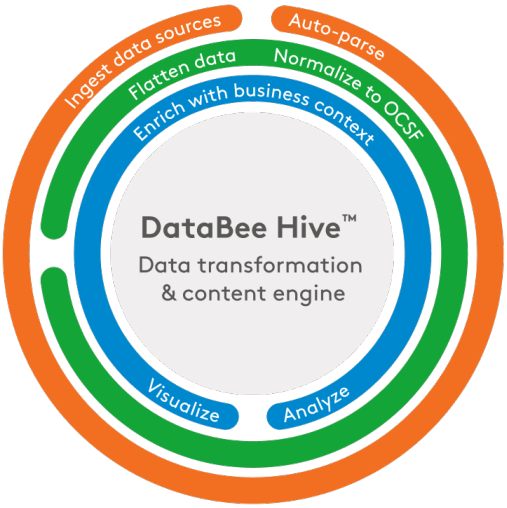
**IN TODAY'S COMPLEX IT LANDSCAPE, IT CAN BE DIFFICULT TO KNOW WHO'S DOING WHAT AT ANY GIVEN POINT ON A NETWORK.** With a security data fabric platform, physical-digital access logs, which can also include IT and OT, are integrated to provide a full view of user activities throughout their workday. Any issues that arise can be quickly pinpointed.

Security data fabrics using real-time data streams can continuously identify assets (including those previously unknown or orphaned) and automatically fill in insights. This helps plug potential entry points for bad actors or insider threats.

This also helps prevent unintentional compliance violations. Compliance leaders can see trending metrics and self-defined KPI values for continuous reporting and can manage any gaps while identifying users, devices or services that are out of compliance.

Furthermore, security data fabric enhances existing investments in SIEMs and modern data lakes. Security data fabrics can ingest and process high-volume and underutilized logs that often drive up cost for SIEMs and can divert them to modern data lakes in a raw and optimized format for analysis at a later time. Storage and compute are decoupled from SIEMs to improve indexing and query results.

# Introducing DataBee™




**DATABEE, FROM COMCAST TECHNOLOGY SOLUTIONS, IS THE FIRST CLOUD-NATIVE SECURITY, RISK AND COMPLIANCE DATA FABRIC PLATFORM,** and is inspired by Comcast's own internal cybersecurity and compliance teams. It allows you to establish a sustainable, long-term foundation for your evolving global data strategy.

DataBee sees the future as vendor-agnostic and embraces a world where data is the shared language.. The platform is designed with a modular, open-ended architecture to make onboarding data easy and delivers a single, shared dataset transformed to Open Cybersecurity Schema Framework (OCSF) schema with proprietary extensions and Sigma rules applied for detections.

Here's how it works:

- **The system pulls together disparate data from a multitude of feeds.**
- **It then standardizes and normalizes that data, enriches it with business policy context and applies patent-pending entity resolution technology to create a unique entity identifier.**
- **It processes and analyzes data in memory and applies active detection streams, including Sigma rules, to high-volume data sources. Data that triggers a DataBee  inding, or alert, is sent to SIEMs or other destinations for further analysis.**
- **It transfers a full-time-series dataset to a modern security data lake of the organization's choice.**
- **Instead of learning yet another visualization tool, users can access pre-built dashboards that use their enriched data directly in Tableau and Power BI.**

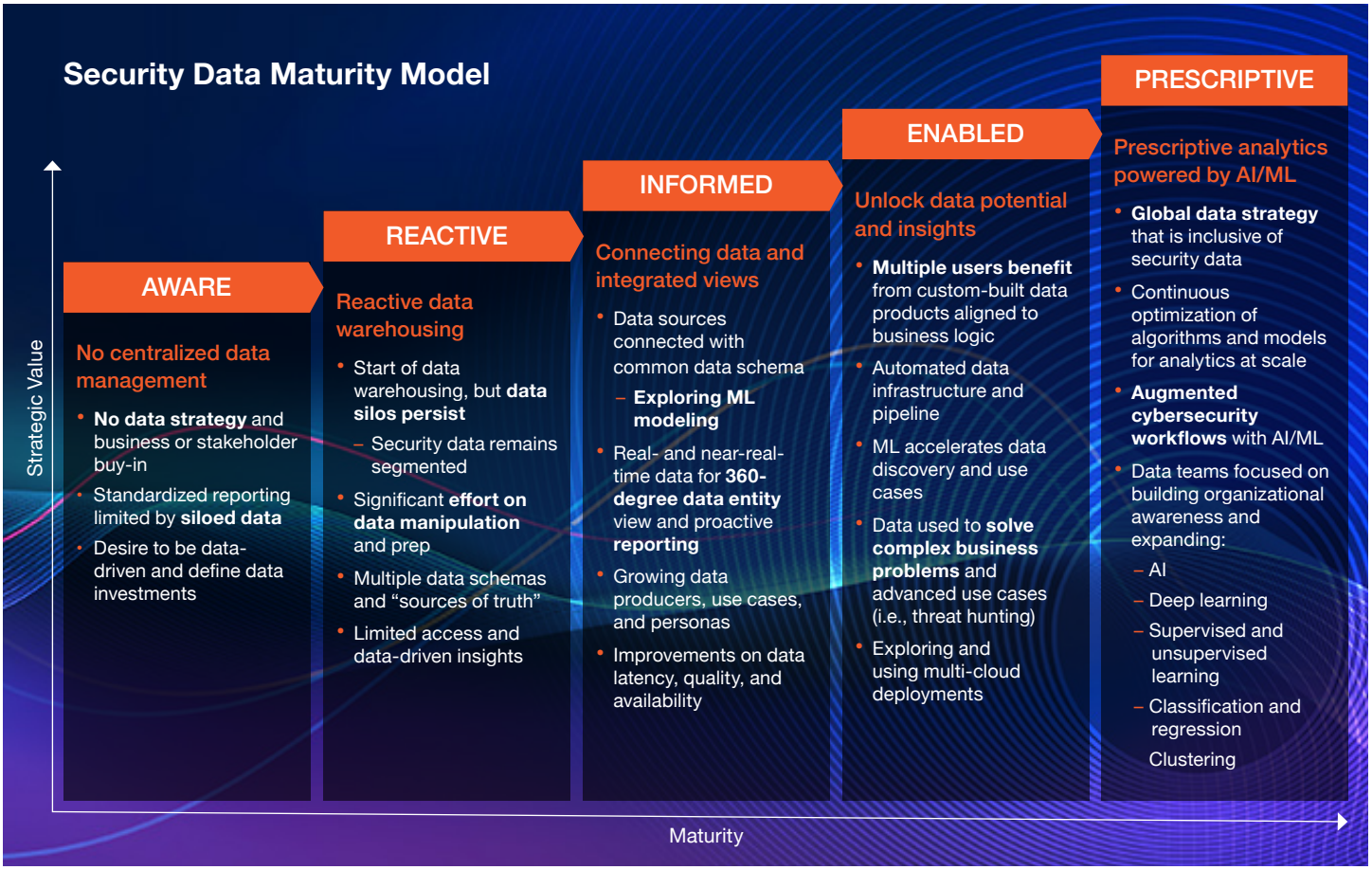
This process provides a unified view of critical security data with business context. Threat hunters, data scientists, security operations center (SOC) analysts, compliance specialists and many others across an organization can quickly identify security issues, derive valuable insights and manage compliance without the need for manually accessing security control data.

Security teams gain a more complete view of user activity with higher fidelity alerts and can conduct multiple investigative queries. The governance, risk management and compliance (GRC) departments can also make important validations when it comes to privacy policy levels. Further, security data fabric can help prevent runaway data ingestion and reduce storage costs.

Other critical DataBee use cases include:

- **Data modeling:** DataBee provides threat detection teams with time-series analytics for AI/ML-based detection.
- **SIEM decoupling:** When SIEMs are used as they're intended — to detect and analyze security events — you can better protect your business. SIEMs, when paired with a data lake and integration is optimized with a security data fabric, are more optimal and performant, and vendor lock-in is avoided.
- **Behavior baselining with anomaly detection:** Data is clean, shareable and usable, allowing security teams to easily understand user and device behavior and quickly respond to anomalies.

From a data maturity standpoint *(see Fig. 1 below)*, DataBee enables enterprises to move from "aware" (that is, with no centralized data management) or "reactive" to "informed," "enabled" and, ultimately, "prescriptive" (optimally leveraging AI and ML-powered analytics).




Source: Comcast Technology Solutions Confidential & Proprietary

With DataBee, modern enterprises can truly "harness their data" — and move beyond just the buzzwords.

# A data-driven approach to security

**CYBERSECURITY IS A HIGH-STAKES GAME.** Breaches are on the rise for a multitude of reasons, among them the fact that organizations have limited visibility into their data, aren't optimally using it (and are missing out on insights from a substantial amount of it) and can't see gaps in their infrastructure — a vulnerability that hackers know how to exploit.

Enterprises need to use their data — and wisely — to bolster their defenses. Security data fabric is a critical step forward, taking enterprise cybersecurity to the next level.

**Interested in learning more about DataBee?**

Request a demo or contact Comcast Technology Solutions today.

COMCAST TECHNOLOGY SOLUTIONS

**About Comcast Technology Solutions**

DataBee is a part of Comcast Technology Solutions, a division of one of the world's leading media and technology companies, bringing Comcast Corporation's proven technologies to an evolving list of industries worldwide. We believe in continuous innovation, always looking for new and better ways to connect with our customers, as well as aggregate, distribute, and secure our own content, advertising, and data. We invest in and test these solutions, so you don't have to — freeing you up to focus on accelerating your business, not your tech stack. Through our portfolio of solutions, we bring these innovations to the global marketplace, enabling our partners to think big, go beyond, and lead the way in media, technology, and cybersecurity. For more information, visit www.comcasttechnologysolutions.com.

**About SDxCentral**

SDxCentral is the leading resource for IT infrastructure knowledge.

IT infrastructure is under more demand and more scrutiny than ever. The way we build networks has fundamentally changed, with new technologies constantly popping up to solve new challenges. At the same time, the role of IT departments and of individuals within the department is changing. While vendors and executives strategize around new technologies, those in the trenches scramble to keep up.

**www.sdxcentral.com**

sdxcentral®