Turn Down the Noise, Turn Up the Value

How data management fuels digital resilience

splunk>
a CISCO company

What makes a good rock song? Music is anything but objective, so the answers will vary. A catchy melody that sticks in your brain. An epic guitar solo à la “Free Bird” that stirs emotion. The unique quality and strength of the vocals. The rhythmic, thumping beat of percussion.

In reality, a good rock tune needs all of the above. Every element of the music must come together to create a powerful symphony of sounds. But contrary to what a rock musician may tell you, music isn’t created with magic or serendipity, or in a space-time continuum. It requires a good producer to organize every component of sound into a harmonious composition. That’s what sets apart a noisy, amateur garage band from a polished rockstar.

Without a data management strategy, an organization’s data can also be deafening rather than harmonious. By 2028, **Gartner predicts** that large enterprises will triple their unstructured data capacity across on-premises, edge, and public cloud locations. All that data has to go somewhere, whether for immediate analysis and investigation or to be stored away for compliance reasons.

With this growth comes a tricky dichotomy: Data is a powerful tool for digital resilience. But data without orchestration leads to chaos. It can also pigeonhole organizations into sacrificing convenience and accessibility for cost savings.
A strong data management strategy, on the other hand, lets organizations realize the value of their data for security and observability use cases — even over time — and maximizes cost savings. It’s a beautiful harmony.

What drives the data dilemma

Let's break down some of the biggest contributors to data chaos.

Data volumes are overwhelming. It's not exactly a secret that organizations have been accumulating a stockpile of data for decades. We're talking about multiple cloud providers, IoT devices, internal systems, remote systems — and that's just the tip of the proverbial iceberg. As organizations embrace AI and the accompanying massive workloads, the data situation will become even more complex.

Maintaining visibility over a lot of data isn't the only problem. Dispersed data makes it difficult to determine not just the what, but the where. Seventy-six percent of respondents cite data sprawl as a barrier to addressing downtime in Splunk's The Hidden Costs of Downtime report. This barrier is especially problematic considering the enormous cost of downtime: $400 billion annually across the Global 2000.

Compliance requirements are tightening. All eyes are on compliance. Eighty-four percent of CISOs say boards equate strong security with regulatory compliance, rather than security best practices and metrics, according to Splunk's CISO report. A wave of new and stringent regulations, such as OMB M-21-31 that requires organizations to store data for extended periods, presents them with a conundrum: "How can we ensure our data is both easily accessible and stored cost-effectively?" Data sovereignty practices require organizations to access data from secure repositories rather than from a central location, which forces organizations to strike a delicate balance between enabling on-demand access to data and maintaining compliance.

Data costs are hard to control. Managing a lot of data and maintaining its compliance is expensive. Higher volumes of data translate to more cloud storage, backup, and data center assets. Extracting value from that data requires investments in analyst tools, machine learning, and technical resources. Plus, a plethora of à la carte costs, including the data egress fees that incur when moving data from archived storage, can force organizations to choose cost savings over common sense.

Organizations aiming to deliver excellent customer experiences, maintain reliability and uptime, and build digital resilience can't afford to endure chaotic data management. The stakes are high. Poor data visibility creates blind spots that lead to costly cyberattacks, unplanned downtime, and compliance violations. Mismanaged data becomes a burden — something that security and IT teams need to sort through and decipher — or worse, a liability for compliance.

On the flip side, properly managed data is an incredibly useful asset for security, ITOps, and engineering teams. Context-rich data helps teams make sense of their complex environments, enabling them to find and fix issues faster. And when teams can access the right data quickly, they can get ahead of an incident before it becomes costly.

Signs that your data is working against you

- ☐ Frequent alert storms for SecOps, engineering, and ITOps teams
- ☐ No way to cost-effectively store low-value data while being able to search it on demand
- ☐ Incident investigation involves long virtual war rooms
- ☐ Security events lack context

Conduct a data symphony

A music producer's role is especially pivotal in the studio, where time is ticking and wallets are shrinking by the second. Along with scheduling recording sessions, coordinating equipment, and conducting sound checks, a producer must maximize each musician's time in the studio to prevent draining resources.

Without a data management strategy, data is just noise. Even worse, it's expensive noise. Organizations can lean on three critical strategies to turn their data from noise into insights.

1. Tailor your data flow to focus on what matters

Recording a live, full-band performance requires a massive amount of coordination to capture every guitar lick, cymbal crash, and bass riff. A producer can isolate the instrumentals and vocals to meticulously craft each component into a harmonious whole.

The same goes for data management. The amount of data that the average organization generates daily is astronomical. Nearly every interaction generates a log: When network traffic exceeds a certain threshold, when a system shuts down unexpectedly, when a customer makes a purchase, or when someone attempts to log in to the network. The list goes on and on.

Not all of that data is relevant for incident investigation. In fact, too much of it can slow down that process. For example, a site reliability engineer doesn't need all app logs to fix a critical bug on their point-of-sale application. They probably do, however, need to see all the errors associated with the app.

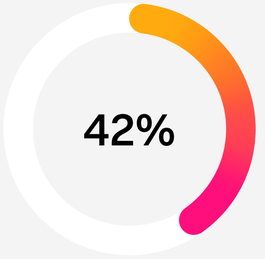
Filtering, redacting, and routing data helps security and observability teams focus on what matters while controlling costs. You can filter out or redact noisy data to control volumes and transform data into the right shape and structure for your use case. Then, you can route your data to a location that hits the sweet spot for cost-effectiveness and accessibility. Data transformation and redaction is so effective that 91% of observability leaders say these techniques are either important or critical when it comes to controlling operational costs, according to Splunk research.

It's a classic win-win. SecOps, ITOps, and engineering teams spend less time sorting through data, and more time innovating. And when businesses can store data in the most cost-effective location, leaders can focus budgets on strategic initiatives, not data storage.

OpenTelemetry: Another tool in the data management toolbox

Standardized, consistent data makes filtering, redacting, and routing a much easier process. As services and applications generate telemetry data, engineering and ITOps teams are forced to instrument all of those services' frameworks and libraries across different programming languages. OpenTelemetry simplifies data management by:

- Standardizing how telemetry data is collected and transmitted.
- Providing a common format of instrumentation.
- Breaking down data silos that make troubleshooting difficult.
- Reducing vendor lock-in by eliminating the need for proprietary agents



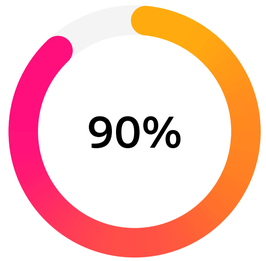
of ITOps and engineering leaders say they've reduced observability costs by using OpenTelemetry

2. Access data where it lives

SecOps, ITOps, and engineering teams need high-value data at their fingertips to quickly detect threats. A unified platform such as Splunk makes critical data visible in real time so that teams can spot a security incident or outage with a short turnaround. Because we know that when it comes to unplanned downtime, every second counts. If downtime costs Global 2000 companies $400 billion annually, when you break it down, that's $9,000 per *minute*.

But not all data needs to live in Splunk. Data like VPN logs, for example, is important for incident investigation but can be accessed on an ad-hoc basis. Audit and compliance data that needs to be accessed less frequently should go in cold archival storage. This practice of storing different types of data based on their usage is called data tiering.

Moving these types of data whenever they need to be accessed is inefficient and expensive. Instead, teams can access data where it resides through federation. Data federation brings search and analytics capabilities to data that resides outside of a security and observability platform, whether it's stored in a data lake, data warehouse, cloud provider, or some other location.



of observability leaders say data tiering is either important or critical for controlling ongoing costs

How data federation empowers smart decisions

At its core, data federation enables organizations to manage and access data in a way that's aligned to their use cases. They can make these decisions based on what makes sense from all angles — convenience, accessibility, security, compliance — and not just cost.

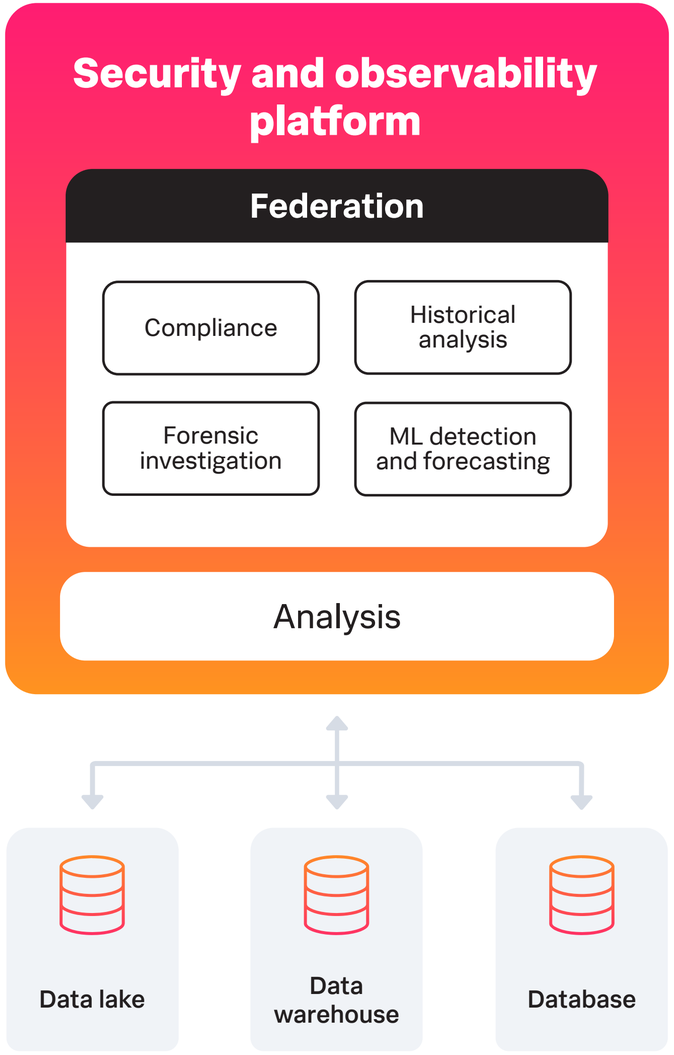
Here's how data federation encourages smart decision-making with your data:

Search and analyze data from any environment. Searching for a particular piece of data across multiple cloud services, databases, data lakes, or on-premises storage can be difficult. Data federation enables organizations to surface relevant, high-quality data from any environment.

With traditional approaches to data management, performing meaningful analysis for forensic investigation can be expensive — which sometimes results in organizations treating them as tabletop exercises or forgoing them altogether. With data federation, organizations can get visibility across security data lakes with scanners or APIs without needing to re-ingest data. This accelerates analysis, enabling SecOps teams to analyze data without going over budget.

Comply with data sovereignty. According to IDC, half of Global 2000 organizations must comply with data sovereignty practices by 2024. These rules dictate that data aligns with the laws and governance of where it is collected. Because of this, it encourages organizations to use scanners and APIs to access the data from a secure repository rather than move it to a central location — making data federation and sovereignty a perfect match.

Innovate with AI. The key to a powerful AI model is data from a variety of disparate sources — which could include customer transaction records in a database, product inventory in a CRM, or sensor data in cloud storage. With data federation, there are no isolated pockets of data across different locations. This means that an AI model can tap into a wide variety of sources and, in turn, deliver more accurate outputs.



3. Harmonize security and observability teams with shared data

In the past, SecOps, ITOps, and engineering teams often operated in silos. The mindset was that dedicated point solutions targeting specific problems would give teams a competitive edge and enable them to focus on the tasks at hand. But that mindset has quickly become outdated due to a very real problem: tool sprawl.

Sixty-nine percent of respondents in Splunk's State of Security 2024 struggle with too much pivoting between disparate security tools and management consoles, which hinders timely investigation and response. But that's starting to change. Nearly half (49%) of respondents say they use the same tools and data across SecOps, ITOps, and engineering to troubleshoot incidents, according to Splunk research.

Bringing security and observability data together gives teams the advantage of collaboration and context. Troubleshooting an incident — whether it's security- or IT-related — requires a frame of reference to uncover patterns, identify anomalies, and ultimately determine the root cause. A cybersecurity attack and IT incident can also look very similar; a spike in network traffic, for example, could be due to a Black Friday sale or signs of a DDoS attack in progress. When ITOps, engineering, and security teams share and reuse data, they can more quickly and easily understand the "why," not just the "what" of an incident.

A unified data management platform that combines security and observability collects telemetry logs, events, metrics, and traces, helping SecOps, ITOps, and engineering teams to surface and analyze data with richer context. Organizations that converge security and observability monitoring tools report a wide range of benefits, including improved MTTR and MTTD (49%), faster time to remediate security vulnerabilities (47%), and streamlined workflows (44%), according to Splunk research.

ManpowerGroup, for example, has all ticket information in Splunk, enabling instant visibility into the SOC. Any team can access the data it needs to quickly mitigate gaps. The audit team, for example, can pull data for policy compliance, or their IT team can issue patches.

> **With Splunk, we're all playing from the same sheet of music.**
>
> — Mike Friedel, Director of Global Information Security, ManpowerGroup

How to make the most of your data

Rock and roll is influenced by modern culture, from politics to religion to fashion and everything in between. Data management is similarly impacted by the times that we live in. AI workloads, for example, generate a massive amount of data. Ninety-three percent of respondents are already using generative AI tools across the business, according to Splunk's State of Security 2024 report. Compliance and regulatory demands are shifting too; 87% say that one year from now, they'll handle compliance very differently, according to the same report. These changes make data management harder.

Data management strategies need to adapt to those seismic shifts. Organizations that work around data silos and make sacrifices due to cost concerns aren't adapting, they're merely surviving.

Adapting means leaning into innovation, and innovation starts with data. Approaches like data federation make it more attainable and cost-effective for SecOps and observability teams to perform more high-performance use cases with their data — all while enhancing digital resilience.

Visibility and cost optimization: A SOC story

Let's say you want to host an application on Windows VMs in the public cloud, like AWS, and ensure that you have visibility over your environment through Windows logs. Windows logs, however, can be chatty and therefore expensive. A cost-effective solution would be to selectively send some of your data, like high-fidelity Windows Defender logs, to your security platform for monitoring and threat detection, and the rest to a long-term storage location like Amazon S3, where you can access them later if needed.

Meanwhile, in the SOC, an analyst discovers a triggered security alert in the Windows Defender logs. It's an instance of deactivated multifactor authentication. To understand what's going on, the analyst needs to look at logs from the surrounding AWS environment. Fortunately, data federation enables the analyst to correlate logs in Amazon Security Lake with data in Splunk. The analyst can review network traffic to track the suspicious account's behavior and confirm that the account was, in fact, compromised.

Learn more about harnessing the full power of data while balancing data, agility, and cost in this **IDC whitepaper**.

And for more executive takes on topics like data management, tool consolidation, and AI, visit **Perspectives by Splunk**.

splunk>
a cisco company

24_CMP_ebook_turn-down-the-noise-turn-up-the-value_v10