Data Management for Security Teams

Seamlessly search, analyze, and manage data wherever it resides.

splunk>
a CISCO company

“Now where did I put that 2x2 bracket…”

Wingspread is a lesser-known Frank Lloyd Wright located a stone’s throw from Lake Michigan in Racine, Wisconsin. Tours book out far in advance. Do it. It’s the only way to see its interior — every roof tile, wall, and walkway rendered in Wright’s favored palette of ochres, browns, and rust-reds. There’s a 30-foot-high chimney, a retractable dining table, and a glass-enclosed “crow’s nest” lookout, which Wright designed for no other reason than to give the owner’s children a place to hide during epic games of hide-and-go-seek.

In a small second-story bedroom next to one famously favored by frequent houseguest Eleanor Roosevelt, tours pause at a 5x5-foot LEGO® model of Wingspread itself. It took over 500 hours and 50,000 pieces to create. “Along the way, this has been so many things to me,” **builder Jameson Gagnepain explained**, “constant frustration, a continued locus of contemplation, an immense challenge of my abilities.”

…sound familiar? SecOps teams, tasked with securing enterprises, organizations, and nations of every size, might share those exact same sentiments. And just as organizing and categorizing every brick and piece is a critical process step in creating a toy brick model of that scale, Security practitioners need an effective data management strategy that can bridge the gap between data chaos and actionable insights, empowering SOC teams to make faster, more informed decisions that measurably improve visibility and security posture.

How much is a zettabyte, again?

The sheer volume of data that SecOps teams need to see, organize, and make sense of is mind-boggling — and since global data creation is projected to grow to more than 394 zettabytes by 2028, it's not a challenge that's going away.

Want to put that number into perspective? A 1X1 toy brick is about 0.95 centimeters tall. If you stacked 394 zettabytes worth of those bricks — that's 394 followed by 21 zeroes — you'd have a tower that reached about 15% of the way to the Andromeda Galaxy about 2.5 million light years away. Given the fact that approximately 90% of all the world's data has been created in the past two years, we might be able to construct that imaginary interstellar bridge sooner than we think.

This means it's going to get even harder to gain the unified visibility and insights necessary to take control of incident response (and, importantly, costs).

Higher stakes than a toppled toy brick tower

Data overwhelm and decentralization

Organizations deal with vast and growing amounts of structured and unstructured data from many diverse sources: cloud providers, IoT devices, internal systems, and remote users. Add to the mix the astronomical growth of AI workloads, the immense volume of data that organizations capture, store, protect, and analyze is placing pressure on existing systems. Also, the volume and variations in data require herculean efforts for standardization and transformation.

With data increasingly decentralized across different tools and storage locations, SecOps teams struggle to gain context and pull insights to protect digital systems. Also, unoptimized data storage can lead to high levels of data duplication. This means it's hard to follow data back to its original source and teams can't evaluate the completeness, accuracy, and relevancy of available data — risking skewed decision-making.

Slow MTTx

Signals of an attack can come from anywhere in the organization. Since important insights across IT, security, and the organization can lie hidden, SecOps teams rely on high volumes of log data to detect potential threats and vulnerabilities. During an investigation, a security analyst needs to be able to quickly get their hands on all relevant data — and not fret about the associated costs for adding new data sources. This way they can follow where an investigation leads them.

Without an effective data management strategy, security teams face slower time to detect, investigate and respond and greater overall risk exposure.

Skyrocketing costs

Managing increasing amounts of data and maintaining regulatory compliance for privacy and protection involves additional costs. As data volumes grow, organizations must expand cloud storage infrastructure, workload capacity, compute performance, data center assets, and of course the teams tasked with managing it all. Extracting value from that data requires investments in tools, machine learning, and technical resources — adding more volumes and varieties of data to the scores that teams need to wrangle.

Even though cybersecurity teams need access to timely data, most organizations find that it's simply too expensive to keep all data in an easily accessible location. Although organizations are realizing the economical benefits of cloud and hybrid storage, without a strategic approach to data management, costs to ingest and analyze data can be unpredictable.

Compliance risk

Enabling on-demand access to data while maintaining security and compliance is a delicate balance. The compliance landscape is continuously evolving, with mandates placing additional burdens on technology teams to securely store data for varying time periods. Teams consistently have to evaluate their data governance policies to protect sensitive information and comply with stringent regulations.

As cyberattacks become more widespread and regulations evolve, proof of cybersecurity compliance becomes increasingly important. Also, organizations need to track the flow of data through its lifecycle — gaining a complete record of where the data comes from, what changes are made to it, and where it's going — for validation, as well as investigating potential disruptions or threats.

The building blocks of the SOC of the future

With a unified data management strategy in place, SecOps teams are empowered to gain rapid insights from an organization's data — no matter where it resides — to take control of incident response, costs, and compliance without compromising security posture.

Seamless visibility

Digital resilience requires complete visibility so SecOps teams can understand what's happening, where it's happening, and have all the information they need to respond to and remediate security events quickly. Without an effective data management strategy, SecOps teams face slower time to detect, investigate, and respond — and greater overall risk exposure. Splunk breaks down data silos and integrates data from diverse sources and security data repositories to provide a unified view that helps teams make fast, more informed decisions that strengthen and deepen an organization's risk posture.

Flexibility and choice

With growing data usage volumes and increased storage complexity, it's getting harder to strike that balance between the needs of the security team and the cost of a solution. Organizations need solutions that simplify the data management experience while retaining control of how their data is shaped, stored, and accessed to reduce overall expenditures and maintain high performance. Splunk's unique ability to conduct TDIR wherever it resides via federated analytics and search gives organizations flexibility to select the best storage scenario with no compromise to detection and response efficiency.

Predictable costs

Not all data is created equal. With the Splunk Platform, teams can pre-process data to have more control over what data will be ingested and what is routed to colder storage. This way they maintain a focused view of security events and operational data while keeping an eye on budget. With economical access to all security-relevant data — no matter where it lives — teams have what they need for comprehensive TDIR (and don't waste time sifting through data they don't need at that moment) and also have data within arm's reach if a compliance audit lands at their desk.

Filter and route data efficiently based on its value to your enterprise

- **Real time:** prevention, detection and monitoring
- **Ad-Hoc:** incident investigations, and threat hunting
- **Archive:** longer term needs like forensics, audit, and compliance

The right data at the right time — click!

Splunk data management includes key tools that help you gain seamless, organization-wide visibility into massive volumes of data — giving you flexibility and choice of where you store them without compromising your organization's cybersecurity posture.

Splunk helps you:

- **Aggregate** data smoothly across complex multi-cloud, hybrid environments
- **Normalize** data and consolidate alerts
- **Generate** insights into log and metric data with powerful search language and rich visualizations
- **Optimize** data to accelerate detection, investigation, and response
- **Mask, filter, and transform** data to normalize results, anonymize sensitive information, manage noisy data volumes, and accelerate investigation and response
- **Break down** data silos and integrate data from diverse sources to provide a unified view that facilitates quicker and more informed decision-making and TDIR
- **Eliminate** data duplication and uncover insights with advanced indexing, powerful search capabilities, and comprehensive analytics
- **Optimize** storage, processing costs, and data value with intelligent data tiering and summary indexing
- **Adhere** to regulatory mandates around data retention and privacy

There's always a sense of excitement, anticipation, and just a little trepidation that accompanies pulling apart the first plastic baggie of toy bricks before embarking on a new model. But often that fear starts to dissipate once you begin to categorize and sort all the blocks and pieces on your table — you realize you have everything you need, right there in front of you.

To help you build and power the SOC of the future, Splunk unifies data management so your SecOps team can improve visibility and gain insights while optimizing costs. With Splunk, teams can eliminate data silos, control the flow of data, and expand data access through federation to gain choice and efficiency without sacrifice.

Get started today with data management.

splunk> a CISCO company

25_CMP_ebook_data-management-for-security-teams_v4