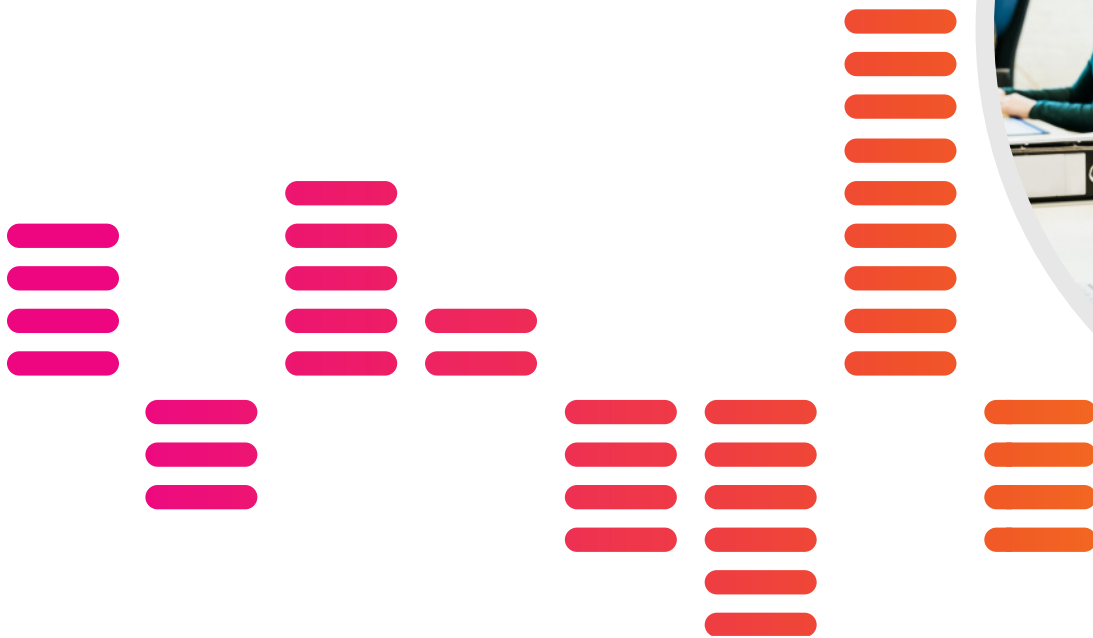


# The SIEM Buyer's Guide for the Public Sector

Strengthen your agency's cybersecurity with a modern, data-driven solution





# Table of Contents


<b>What's a SIEM?</b> .....	<b>3</b>
What does a SIEM do, exactly? .....	4
Legacy SIEMS are dinosaurs.....	4
What else is out there? .....	6
The evolution of a data-driven SIEM .....	6
<b>Modern SIEM Essentials</b> .....	<b>7</b>
Five essential capabilities of a modern SIEM.....	7
Seven must-have SIEM strategies.....	8
<b>Enter Splunk</b> .....	<b>13</b>
Splunk for the public sector .....	13
Splunk as your SIEM.....	14
Uplevel your SIEM .....	14
Build on a strong foundation.....	16
Let's talk real-world ROI.....	17
Future-proof your SIEM.....	21
Tap the power of data for the public sector.....	21



It's a new and challenging era for securing the public sector. Technology is changing at record speed, cyberthreats are constantly evolving, and demands on government agencies for seamless digital services, innovation and technological integration have grown exponentially. Digital transformation has gone from priority to imperative, and modernization strategies for IT and cybersecurity are now mission critical for federal agencies as well as state and local governments. What's fueling the most critical innovations? Accelerated cloud and hybrid technologies and the power of data.

Now more than ever, citizens depend on the government for critical services — from COVID-19 testing and vaccinations to protecting against cyberattacks to administering benefits and more. These critical services require digital systems that both generate and rely on a huge amount of data, data that must be kept secure and managed effectively. If harnessed, this data can also be a strategic asset for the public sector.

To thrive in the hybrid world, organizations of all kinds need solutions that are powerful, flexible and fast — solutions powered by data. With a strong data and technology foundation, government agencies can respond quickly to whatever comes their way, secure their organizations from ever-evolving threats and use their data to innovate.



Yet many organizations and government agencies struggle to fully tap the power of their data, because of four major challenges:

- **Data volume and complexity:** The sheer volume of data and increasingly complex digital interactions fueled by hundreds of backend microservices, often with legacy systems, can quickly become unmanageable.
- **Data silos:** With too many tools within and across teams and agencies, data is often fragmented and hard to see, which leads to inefficiency and vulnerabilities.
- **Lack of visibility across processes or agencies:** Without contextual data, it's difficult to track operational processes end to end, making it harder to get to root causes and find ways to optimize.
- **Security and compliance regulations:** Constantly changing security, privacy and compliance regulations, especially critical for government agencies, make it difficult to make sure the right data is accessed at the right time, with the right governance.

As a consequence, agencies have difficulty drawing insights from and acting on their data. It's just too time-consuming and resource-intensive.

**But there's a solution:** Organizations of all kinds, including those in the public sector, can meet these challenges, strengthen cybersecurity, and tap the power of data by employing the right security information event management (SIEM) solution, one that's cloud-based and data-driven.

# What's a SIEM?



A SIEM solution is like a pilot's radar system. Like pilots, the analysts who help pilot your security operation center (SOC) need a radar to safely navigate what's around them, what's ahead and what might be hidden out of view. A SIEM solution is a security platform that helps SOC analysts see across enterprise IT and spot security threats hiding in the corners of the systems they protect. Without it, they're flying blind.

While security applications and network security and system software do catch and log isolated attacks and anomalous behavior, today's most serious threats are distributed and can't be caught with these tools alone. Hackers attack in unison across multiple systems and use advanced evasion techniques to avoid detection.

Attackers also take advantage of stressful situations to exploit weaknesses — situations like, say, an immediate shift to remote work during a global pandemic. In the middle of that urgent transition, SOC teams were tasked with keeping systems secure, but without in-person access to the security tools and processes they'd come to rely on.

Situations like these are why a modern SIEM solution is more important than ever. Without the right SIEM, cyberattacks can fester and turn into catastrophic incidents that even the best SOC analysts can't see coming. And by the time they discover the vulnerability, like a ransomware or supply chain attack, all they can do is damage control — and start the search for a new CISO.

In this buyer's guide, we'll take a deep dive into what exactly a SIEM solution is, what it does, how it's different from other tools, and how to find the right SIEM solution for your organization.





## What does a SIEM do, exactly?

**Gartner** defines a SIEM solution as “a technology that supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources.”

Basically, a SIEM solution helps SOC analysts do their jobs better. It's a security platform that ingests event logs and gives them a single view of their data, with more insight.

### **With a modern SIEM, analysts can solve three major security challenges:**

- A lack of visibility into the real-time status of your organization's security — often referred to as security posture.
- Trying to reduce the amount of false positive security alerts analysts see, prioritizing them, and then increasing the speed of their detections and investigations.
- A lack of flexibility or support for different types of deployment environments, technology tools and threat intelligence.

So how are organizations trying to solve those challenges today without a SIEM solution? Historically, they've used “legacy” solutions, various point solutions, and tools like extended detection and response (XDR) — with mixed results. Let's briefly explore those options, then focus on the more effective solution, a modern SIEM.



## Legacy SIEMs are dinosaurs

Okay, not literally, but legacy SIEM technology just isn't built to keep up with today's evolving security challenges. With a closed environment and limited data they can ingest, they're slow at queries and investigations, and they don't scale to meet business and mission needs.

Many enterprise IT organizations that invested in SIEM platforms discovered this the hard way. They learned — after spending a lot of money — that it takes a long time to ingest all their data into a legacy SIEM, and that the underlying data system used to create the SIEM tends to be static. Though there are a myriad of software options on the market for collecting, storing and analyzing security-only data, only a few can turn that data into actionable intelligence, and a legacy SIEM isn't one of them.

Then there's the issue of speed. Your SOC analysts can't afford to lose precious time when there is a security alert, and a legacy SIEM solution can't keep up with the pace at which they need to investigate data.

Worse yet, legacy SIEMs can only provide insights into security data, which makes it difficult to correlate security events with what's happening across the rest of an IT environment. That might have worked a decade ago, but not in our hybrid world, where some employees work remotely, others bring their own devices to the office, and everything in between is connected and generating data — all of which is crucial to security.

Especially with today's rapid adoption of cloud services, which continues to expand the threat vectors, today's organizations need to monitor user activity, behavior and application access across key cloud and software-as-a-service (SaaS) solutions, not just on-prem services, to determine the full scope of potential threats and attacks.



## Seven Reasons to Replace Your Old SIEM

Organizations are often tied to the dated architectures of traditional SIEMs, which typically use an SQL database with a fixed schema. These databases can become a single point of failure or suffer from scale and performance limitations.

<b>1. LIMITED SECURITY TYPES</b>	By limiting the type of data that is ingested, there are limits in detection, investigation and response times.
<b>2. INABILITY TO EFFECTIVELY INGEST DATA</b>	With legacy SIEMs, the ingestion of data can be a massively laborious process or very expensive.
<b>3. SLOW INVESTIGATIONS</b>	With legacy SIEMs, basic actions, such as raw log searches, can take a significant amount of time – often many hours and days to complete.
<b>4. INSTABILITY AND SCALABILITY</b>	The larger SQL-based databases get, the less stable they become. Customers often suffer from either poor performance or a large number of outages as spikes in events take servers down.
<b>5. END-OF-LIFE OR UNCERTAIN ROADMAP</b>	As legacy SIEM vendors change ownership, R&D slows to a crawl. Without continuous investment and innovation, security solutions fail to keep up with the growing threat landscape.
<b>6. CLOSED ECOSYSTEM</b>	Legacy SIEM vendors often lack the ability to integrate with other tools in the market. Customers are forced to use what was included in the SIEM or spend more on custom development and professional services.
<b>7. LIMITED TO ON-PREMISES</b>	Legacy SIEMs are often limited to on-premises deployments. Security practitioners must be able to use cloud, multicloud, on-premises and hybrid workloads.



## What else is out there?

The truth is out there ... But let's start with the truth about point solutions versus platform solutions. Point solution vendors are lying if they tell you they can do what a modern SIEM solution can. They typically do one or two things really well, but they can also create additional complexity in the SOC. Point solutions require additional configuration and management, and they'll likely need to integrate with your existing technology stack. And without a centralized way of making sense of the organization's data, your SOC analysts are flying blind.

Then you have XDR — an emerging solution generating a lot of (marketing) buzz. But you can't always believe the hype. XDR is an evolution of endpoint detection and response (EDR), which has traditionally served as an additional data source for a SIEM solution — not a replacement for it. Though XDR can be used in tandem with a modern SIEM, XDR alone won't cut it.

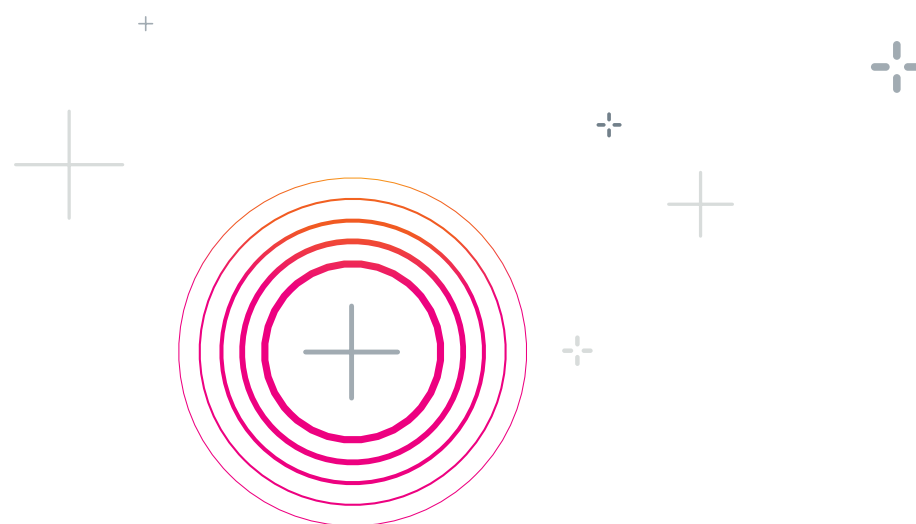
Not being able to see into a company's security posture makes the job of your SOC analyst almost impossible. And the last thing you want to do is make the life of your SOC analyst harder, because there just aren't enough good SOC analysts to go around. Let's face it, the eternal security skills shortage **has only gotten worse** since the pandemic started.

Going back to that radar system: without visibility, security investigations can only scratch the surface of true incident resolution and that leads to more vulnerabilities down the line. The less visibility your organization has, the more vulnerable it is to a high-profile breach, which can cost millions of dollars and its reputation. No CEO wants to see their company's name in a Bloomberg headline — and no CISO wants to explain why that happened.

## The evolution of a data-driven SIEM

Call it survival of the fittest. With legacy SIEMs stuck in the past, and new-fangled solutions only able to solve part of the problem, the modern SIEM had to evolve into a robust, analytics-driven solution to keep up with the sophistication and speed of today's attacks.

What SOC analysts require today is a simple way to correlate information across all security-relevant data. A solution that enables IT to manage their security posture easily. SOC analysts must be able to anticipate what threats might be lurking and put measures in place to limit the vulnerability of their company in real time. For that, enterprises need a data-centric, modern SIEM solution that gives analysts full visibility into the data being generated by their enterprise, one that works with more than just log data and simple correlation rules for data analysis. Leading SIEM solutions now combine long-time storage of event logs with real-time monitoring to provide your team with a holistic understanding of the organization's security posture.



# Modern SIEM Essentials

[Gartner's Magic Quadrant for Security Information and Event Management](#) is practically required reading for anyone exploring the SIEM market. As the report has evolved, it's grown to include open source SIEM vendors and other new entrants in the broader category. So how can you tell if a solution is the real deal?

In the Critical Capabilities for Security Information and Event Management report, [Gartner highlights](#) the five things a modern SIEM can do that others can't.

## Five essential capabilities of a modern SIEM

### 1. Collect security event logs and telemetry in real time for threat detection and compliance use cases.

A modern SIEM solution can collect, use and analyze log data — from across an ecosystem of teams, tools, peers and partners — in accordance with sector-specific mandates around regulatory compliance and reporting, as well as the latest threat detection needs.

### 2. Analyze telemetry in real time, over time, to detect attacks and other activities of interest.

A modern SIEM can collect, use and analyze all event logs and give a unified view into what's going on across the security stack in real time. This gives IT and security teams the ability to manage event logs from one central location, correlate different events over multiple machines or multiple days, and tie in other data sources like registry changes and ISA proxy logs for the complete picture. Security practitioners can also audit and report on all event logs from a single place.

### 3. Investigate incidents to determine their potential severity and impact on an organization or agency.

A SIEM can also determine the severity and likelihood of potential incidents for each issue identified, and use this information to prioritize and inform on corrective actions.

### 4. Report on these activities.

A modern SIEM can also generate reports containing security information about any part of an organization's infrastructure and provide a means for documentation and compliance requirements.

### 5. Store relevant events and logs.

And finally, a modern SIEM solution can store historical log data over the long term, which helps analysts meet compliance mandates and correlate data over time.





## Seven must-have SIEM strategies

That's right, it's another list, because who doesn't love a list — especially one that makes your job easier?

Seven key strategies for securing your organization (and how you can use a modern SIEM to implement them):

- 1. Real-time security monitoring and analysis:** detect and respond to threats fast
- 2. Cloud security:** detect and respond to threats across hybrid, cloud and multicloud environments
- 3. Incident response:** identify incidents when they occur, and track, route and annotate events
- 4. Threat intelligence:** access curated, in-product security research on existing and emerging threats
- 5. Incident investigation and forensics:** optimize threat hunting, reduce the volume of alerts and increase true positives
- 6. Advanced and insider threat detection:** exponentially improve detection success, freeing up time and resources to zero in on complex, high-fidelity threats
- 7. Compliance:** unify the three pillars of compliance — process, technology and people — through greater visibility across systems and processes.



### 1. Real-time security monitoring and analysis

Organizations need to be able to detect and respond to threats in record time — no matter the nature or severity of the attack. But to do this and do it well, security monitoring is a must-have, and luckily, a modern SIEM offers robust, real-time monitoring.

**How does it work?** To pinpoint and identify different types of malicious and/or anomalous behavior, a SIEM retrieves and maintains contextual data around users, devices and applications (e.g., asset and identity data) **from across on-prem, cloud, multicloud and hybrid environments**. All relevant data is then fed into a workflow to assess potential risks.

By monitoring and ingesting machine data from a diverse set of sources across different types of deployments, security teams have a comprehensive view of potential security events — making it that much easier to detect and zero in on bad actors. A leading SIEM should provide a library of customizable, predefined correlation rules, a security event console for real-time presentation of security incidents, and dashboards to provide real-time visualizations of ongoing threat activity.

Security monitoring can also be augmented with out-of-the-box correlation searches that can be invoked in real time or scheduled regularly. These searches can be available via an intuitive user interface that doesn't require analysts or administrators to master a search language. Finally, a modern SIEM will have a local and historical search function to make easy work of searching log data, and reduce the amount of network traffic accessing search data.

## 2. Cloud security

As your organization sprints ahead with digital initiatives, you'll need to pay close attention to both general security requirements and the technical complexities of cloud migration. Inevitably, the journey to cloud nativity presents a considerable increase in risk to the enterprise — especially if the organization is not up-to-date on network controls, access management systems or cloud configuration options. Add an expanding attack surface and a lack of visibility, and you've got yourself a high chance of a breach. So traditional monitoring just isn't enough. Security teams need the capabilities of a modern SIEM to analyze and ingest data from a wide range of sources, across all types of environments, in order to detect the where and why of security events.

**How does it work?** With a leading SIEM solution, you get out-of-the-box cloud security monitoring content that makes it easier to detect and respond to threats across hybrid, cloud and multicloud environments, including sophisticated detection rules for cloud attacks, and tools to help you test and improve cloud detections via attack simulations.

Especially in the age of remote work, you need to be able to capture and analyze all cloud and endpoint data — regardless of volume, variety and velocity. Ultimately, by monitoring the uptime, availability and activity across multiple cloud deployments with a modern SIEM, you'll have full visibility into cloud services, including Amazon Web Services (AWS), Azure and Google Cloud Platform, and all the actionable insights that come with it.



### Slack unlocks data to empower collaboration

When the COVID-19 pandemic hit, Slack had to transition more than 1,600 employees to remote work, all the while continuing to provide a secure, enterprise-grade service to its booming user base. With Splunk, Slack was able to seamlessly transition their workforce to the cloud, bolster security within a zero trust framework, and gain visibility into any and all activity across its cloud services. Slack has also used Splunk to:

- Glean insights into behavioral patterns across critical applications.
- Authorize and authenticate users within a zero trust network.
- Innovate and stay in lockstep with customers while remaining secure.

#### Running a secure ecosystem

With a massive surge in demand due to the pandemic, Slack had to make sure its security program was working effectively and — with the welcome help of Splunk — launched a new application programming interface (API), as well as fortified a zero trust network.

By integrating an analytics API with Splunk, users had an easier time keeping a finger on the pulse of the organization. The API integration helped customers get the information they needed and for leadership to stay connected. All of Slack's critical applications were sending logging content into Splunk, bringing data into one place, and offering insight into an array of behavioral patterns.

Operating in a zero trust network — where users are authenticated and authorized — also strengthened Slack's security posture. "Splunk is a key part of Slack's ability to operate a zero trust network," Ryder says. "Because Splunk gives us visibility into all the activity that's happening across all of our cloud services."

**"Splunk is how we verify that our security program is operating across our entire fleet and across our corporate applications the way we expect it to, the way we must to assure the integrity of our company." [Read more.](#)**



### 3. Incident response

Today's organizations also need an up-to-date incident response strategy, and a modern SIEM can help you identify incidents when they occur, and provide a means for tracking, routing and annotating events.

**How does it work?** A SIEM can manually or automatically aggregate events, support third-party systems and vendors (allowing for the easy ingestion of data to and from a diverse set of sources), and provide up-to-date threat intelligence and auto-response capabilities (like playbooks) that preempt or disrupt cyberattacks either right before or right after they emerge.

In order to do all of this, a SIEM solution should be the hub around which an incident response workflow is customized and crafted. Since security events have different levels of urgency attached to them, potential threats can be identified, categorized and triaged via dashboards, then assigned to analysts for review. By identifying, triaging and auditing notable events based on the fidelity of the threat, a modern SIEM makes the start of the remediation process more reliable, equipping your teams with the contextual awareness they need to determine next steps.

To expand or reduce the scope of their analysis (which can be vast), your SOC analysts can use a SIEM to apply filters to the sea of log data, then place events, actions and annotations into a timeline to see everything that's going on. They can then review and codify these timelines as a repeatable kill chain methodology to deal with specific event types.



### 4. Threat intelligence

Threat intelligence is another must-have strategy. But threat intelligence is often too noisy, with your security analysts having to manually curate data to make use of it. With manual input, context gets lost during the investigation process or the data becomes too disparate, while enrichment in playbooks is too clunky. Making it even harder for your analysts, the most valuable security data is often locked inside silos in and across companies. With more integrations coming online that are generating more data needing to be secured and stored, this problem isn't going away.

Fortunately, thanks to the rapidly growing intelligence marketplace, modern SIEM solutions can integrate threat intelligence into every stage of the incident response flow, as well as across an ecosystem of teams, tools, peers and partners.

**How does it work?** Threat intelligence transforms internal and external sources of security intelligence for informed, actionable automation across ecosystems of teams and tools and helps with intelligence sharing with internal and external stakeholders. Your team can preempt attacks and create complex pipelines without ever having to write or maintain scripts in the backend. Threat intelligence comes integrated into most modern SIEM solutions or as cloud-native SaaS that integrates seamlessly with a modern SIEM platform.

The intelligence provided usually includes indicators of compromise (IOCs), adversary tactics, techniques and procedures, alongside additional context for various types of incidents and activities. This makes it much easier to recognize abnormal activities, as your analysts have all the information they need to assess the risks, impact and objectives of an attack — no matter how cunning — and respond appropriately.

Threat intelligence data can be integrated with machine data to create watchlists, correlation rules and queries for better detection and response to attacks. This information can be automatically correlated with event data and added to dashboard views and reports, or forwarded to devices that can then remediate the vulnerability in question.



## 5. Incident investigation and forensics

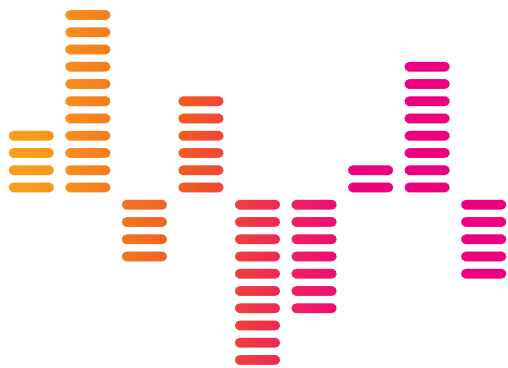
Chances are, your security team spends too much time investigating low-value alerts with too little context. Incidents based on narrowly defined detections can lead to a high volume of false positives and a lot of extra noise, quickly overwhelming and overburdening anyone on the front lines. That's why you need a strong incident investigation and forensics strategy powered by a modern SIEM.

**How does it work?** A modern SIEM visualizes and correlates data by mapping categorized events against a kill chain, or creating heat maps to better support incident investigations by providing important insight into which tactics have been used by an adversary that map to a particular industry framework.

Risk attribution can also help optimize threat hunting and reduce the volume of alerts — thereby increasing true positives — while surfacing more sophisticated threats, like low and slow attacks that most correlation searches traditionally miss. This frees up time and resources to hone in on actual (often complex) threats, aligning operations to industry-standard cybersecurity frameworks.

**Bottom line:** freeing up your analysts to focus on high-value tasks means they're better positioned to respond quickly and efficiently in the event of a security breach — and who wouldn't want that?

Plus, your team can make better informed decisions and gather forensics evidence with the comprehensive collaboration and reporting capabilities integral to a modern SIEM investigative workflow.



## 6. Advanced and insider threat detection

Security threats continue to evolve, mutate and find ways to evade standard security procedures — and the more sophisticated the attack, the harder it is for your team to detect and remediate it. Between the changing threat landscape and the crafty nature of new and emerging threats, advanced and insider threat detection strategy has never been more important.

Most traditional security tools can't meet the challenge. They rely on existing rulesets and signatures, and can only detect straightforward, well-known threats, so they fail to address the complexity of advanced security threats, like insider threats, zero-day attacks, laterally moving malware and compromised accounts.

**How does it work?** Fortunately, a modern SIEM can adapt to these threats by stitching together anomalies and correlating them as part of the incident response workflow, as well as implementing capabilities like endpoint detection and behavioral analytics.

By establishing multi-dimensional behavior baselines and dynamic peer group analysis — ideally in tandem with unsupervised machine learning — compromised or misused accounts can be detected.

The goal is to not only detect hidden threats, but also determine the scope of the attack and how best to contain it. For this, your team requires real-time views and reporting capabilities that can be extended to include any number of third-party applications and services.

This type of analytics and behavior profiling in a SIEM can exponentially improve detection success, freeing up your team's time and resources to focus on complex, high-fidelity threats, before it's too late.

## Expo 2020 Dubai mega-event ensures security with Splunk

Securing an event like Expo 2020 is no easy feat — especially in the face of insider threats. And while Expo Dubai had prioritized cybersecurity since its very inception, the time had come for the org to up the ante ahead of their coming six-month event.

To tackle a number of their growing concerns, Expo 2020 required a security platform that could scale quickly, manage operational security for hundreds of different data sources and technology solutions, and be flexible enough to adapt to the evolving cybersecurity needs of the event. Splunk proved to be the best solution to meet these requirements.

Splunk helped Expo 2020:

- Monitor, flag and classify suspicious or anomalous behavior/activity.
- Respond to potential threats immediately and take corrective action.

### Tackling the possibility of insider threats

Mega-events and large-scale organizations deal with a number of security incidents on a regular basis — and insider threats have evolved into some of the most challenging risks these organizations face. To protect its technology ecosystems from potential adversaries, Expo relied on Splunk's real-time monitoring to identify suspicious behavior.

Splunk also helped the Expo team make faster, better data-driven decisions, strengthening Expo's overall cyber resilience, and empowering them to respond to threats immediately with corrective action.

**“Splunk's flexibility meant that we could easily resize the deployment to accommodate Expo's changing needs during the pandemic, especially in terms of adapting to the one-year postponement of the event.” [Read more.](#)**

## 7. Compliance

Whether it's for cybersecurity, forensic analysis, privacy, fraud or risk management, different teams require different views and processes around data in order to guarantee compliance. A modern SIEM can help unify the three pillars of compliance — process, technology and people — by providing you with greater visibility across the board.

**How does it work?** A modern SIEM solution takes a holistic, foundational approach to compliance that not only connects compliance teams, silos and technology fiefdoms, but also streamlines the overall efficiency of compliance-related operations. This means the tedious, time-consuming chore of legally-mandated log review can finally be put to bed. Your analysts can be more productive and maintain the buttoned-up, documented approach to risk management that's expected of them.

With a modern SIEM, organizations can see across the entire security stack for assessments, rankings, investigations and audits, and are no longer dependent on a single department or functional unit for insights. Your analysts can search, alert and report on machine data from an array of sources, meet compliance requirements from audit trail collection and reporting, and generate sector-specific compliance reports in seconds.



# Enter Splunk

**Splunk** offers a data-driven SIEM solution on a flexible data platform. With Splunk, organizations can see across all their data, gain insights quickly, respond with accuracy, confidence and ease — and do it all with one unified, integrated solution. You could say it's the ultimate radar system for SOC analysts.

Splunk can monitor and analyze data from any source and at enterprise scale, and offers integrated solutions that deliver consistent full-stack observability, unified security and myriad custom applications, giving you limitless ways to gain insights from data.

A no-compromise, data-centric security operations platform like Splunk delivers the strength and flexibility needed to meet complex compliance challenges and respond to threats so your organization can grow and innovate — securely.

By working across multicloud and hybrid environments and providing robust tools for investigation, analysis and orchestration, Splunk helps organizations find and remediate threats quickly, and with accuracy.

**Splunk Enterprise** monitors and analyzes machine data to improve your IT, security and business performance. With intuitive analytics, machine learning, packaged applications and open APIs, Splunk Enterprise is a flexible platform that scales from focused use cases to an enterprise-wide analytics backbone.

**Splunk Cloud Platform** is a flexible, secure and cost effective data platform that helps organizations search, analyze, visualize and act on their data. With Splunk deployed and managed securely, reliably and scalably as a service, you get fast, flexible service, powerful and integrated streaming, search, and machine learning, and predictable pricing that aligns with value.

## Splunk for the public sector

Thousands of U.S. public sector organizations trust and rely on Splunk for security, IT and observability solutions. Splunk can help your agency meet requirements for cyber incident response mandated by the **Biden Administration's recent executive order** (OMB M-21-31). Splunk is a trusted federal partner that understands agency mandates and the particular cybersecurity challenges you face in the public sector.

Today's federal agencies are powering their critical digital transformations while operating in highly-distributed multi-public cloud and hybrid cloud environments. Tasked with improving outcomes for security, resilience and innovation, they face daunting complexity and an ever-expanding technology ecosystem and attack surface. To be successful, federal leaders need a new approach to their cloud journey.

Splunk's extensible platform and purpose-built solutions help public sector teams improve security at scale and drive resilience across enterprises. Splunk protects the confidentiality, integrity and availability of data in **compliance** with government security requirements, such as FedRAMP moderate and Department of Defense Impact Level 5 (IL5).

Splunk can also help you meet the zero trust architecture security requirements mandated by **Executive Order 14028**. A zero trust model enhances security by protecting your endpoints and backend applications instead of relying solely on perimeter-based protection. Protection and authentication are continuously applied at the device and user levels for each transaction, ensuring continuous and adaptive authorization.

A zero trust architecture requires robust analytics to ingest and analyze significant volumes and types of sensor and logging data, and Splunk's data-driven solutions provide that and more. With Splunk, you can continuously monitor user, asset and service trustworthiness to increase confidence in access permissions to enterprise resources. Splunk's full-stack visibility into service health, component relationships and infrastructure strengthens performance and availability, and machine learning helps you predict issues before they arise. Last but not least, Splunk saves your team's time and energy, and cuts down on operational costs by automating tasks and orchestrating workflows.

No matter what your agency's security, IT and observability needs are, Splunk is here to help you achieve mission success. Now, let's get down to the brass tacks of Splunk as a SIEM solution.

## Splunk as your SIEM

Today's complex technological ecosystems and constantly changing security threats require modern security operations that effectively balance mission risk with security risk, while also allowing organizations to move quickly.

Splunk security solutions not only meet today's SIEM needs, they help you prepare for what's next. Splunk offers a security operations platform that ingests data from any source for accurate threat detection, investigation and automated response across cloud, on-prem and hybrid environments. And because Splunk embraces an open ecosystem, you have the freedom to select the best tools and build using your existing infrastructure.

The Splunk platform is built to ingest, normalize and provide insights across all of your data so you can get accurate and actionable detections, conduct quicker investigations and reduce time to remediation. Those advanced security analytics provide the valuable context and visual insights your security team needs to make faster, smarter decisions in complex environments.

Along with end-to-end visibility into security, Splunk offers schema-on-read and distributed indexing capabilities that make collecting and analyzing data from any source both quick and easy. Splunk is also flexible, offering several options for enterprises looking to deploy their SIEM or migrate from their legacy SIEM, and the choice of on-prem, cloud or hybrid deployment.

To cover your basic needs, you can use either [Splunk Enterprise](#) or [Splunk Cloud Platform](#). Both core platforms provide collection, indexing, search and reporting capabilities. Many Splunk security customers use one of the two platforms to build their own real-time searches and dashboards for essential security use cases. You can also leverage Splunk-built search and reporting, security and observability solutions as well as the [Splunkbase](#) ecosystem that includes literally thousands of apps.



## Uplevel your SIEM

Need to take it up a notch (or three)? Splunk's next-level SIEM solution, [Splunk Enterprise Security \(ES\)](#) is fast, powerful and flexible, delivering data-driven insights for full visibility into your organization's security posture so you can protect your organization and mitigate risk — at scale. These are just some of the reasons Splunk ES has been the SIEM market share leader the past several years, [according to IDC](#).

With unparalleled search and reporting, advanced analytics, integrated intelligence, and pre-packaged security content, Splunk ES accelerates threat detection and investigation so you can quickly assess the scope of high-priority threats and take action. It combines machine learning, anomaly detection and criteria-based correlation in a single security analytics solution, and runs on Splunk Enterprise, Splunk Cloud or both.

Splunk ES is also flexible and plays well with others. Built on an open and scalable data platform, Splunk ES allows organizations to stay agile in the face of evolving threats and business needs. And Splunk's extensive ecosystem and flexible deployment options ensure your technology investments are working in tandem with your SIEM, while meeting you where you are on your cloud or hybrid journey.

With Splunk ES, you can visually correlate events over time and communicate details of multi-stage attacks. You can also easily discover, monitor and report in real time on threats, attacks and other abnormal activity from across all your security-relevant data. And Splunk ES now offers new, native risk-based alerting and cloud security features so you can investigate real threats even faster, with more insight.

Chances are, your security team is wasting hours on low-fidelity alerts that they ultimately abandon. Risk-based alerting in Splunk ES cuts down on the number of alerts they receive so they can focus on the ones that matter, helping to detect complex threats they might otherwise miss.

Risk-based alerting attributes risk to users and systems and only generates alerts when risk and behavioral thresholds are exceeded, helping you detect more true positives. And unlike other solutions, Splunk's risk-based alerting was also built to improve SOC efficiency and help teams align with their industry-standard cybersecurity frameworks of choice.

For more advanced use cases, Splunk ES offers ready-to-use and customizable dashboards, searches and reports. Splunk ES also includes incident review, workflow functionality and third-party threat intelligence feeds to accelerate threat detection and investigation.

## Five complex problems you can solve with Splunk Enterprise Security

Problem	Solution	How it works	What it helps you do
1. Not being able to see all of your data from different sources (audit, firewall, windows, unix, linux, endpoint or other logs).	<b>Real-time security monitoring and analysis</b>	Puts all of your data into one centralized platform so you can search and make sense of what's going on in your environment.	Get real-time visibility over your security posture paired with the ability to search, analyze, and prioritize if or when potential issues arise.
2. Advanced and insider threats that go unnoticed and hurt your organization's financial well-being and reputation.	<b>Advanced and insider threat detection</b>	Advanced analytics help you find sophisticated threats and malicious insiders that evade traditional detection methods.	Prevent security incidents early and quickly before they do irrevocable damage.
3. Not being able to search through data while performing an investigation can be slow and cumbersome.	<b>Incident investigation and forensics</b>	Gives you the full context of an event, identifies the root cause and provides fast and flexible search and reporting.	Quickly and easily investigate security events, find and analyze data for evidence, and assess potential damage.
4. Lack of centralized data to drill down and search while lack of predictive analytics or machine learning can make hunting for threats slow and arduous.	<b>Threat hunting</b>	Provides in-depth hunting and analysis through flexible searches, machine learning and threat intelligence.	Search proactively for cyberthreats that may otherwise evade detection.
5. Lack of visibility and inability to analyze IT and security controls can lead to compliance violations (and severe penalties and fines).	<b>Compliance</b>	Performs continuous risk assessment, centralizes and analyzes data across the organization, and provides robust reporting to ensure compliance standards are achieved.	Confirm and demonstrate effective adherence to compliance requirements and regulatory frameworks.



## A SIEM in the cloud, for the cloud

Most organizations today are at some stage of their cloud journey. With so many tools to manage across different portals, compliance, migration and service offerings, cloud security monitoring can be tough. Security teams need tools that easily integrate with cloud providers, and Splunk ES gives you cloud security monitoring content designed to make monitoring easy, no matter where your data is located.

Splunk ES has pre-built detections and investigations specific to the major cloud providers, like Amazon Web Services (AWS), the Google Cloud Platform (GCP) and Microsoft Azure. This content helps you monitor both cloud and on-prem data, seamlessly bringing cloud data into your existing detections and investigative workflows. Splunk ES is vendor neutral and can monitor your data no matter the cloud provider, giving you the confidence to choose an IT infrastructure and application provider that makes the most sense for your agency.

And now that practically everything is offered “as a service,” why shouldn't your SIEM be SaaS too? When deployed as a cloud-based SIEM via Splunk Cloud, Splunk Enterprise Security frees your team to focus on high-value activities, instead of backend maintenance. Splunk ES on Splunk Cloud can scale to monitor TBs of data per day, from any source, in any structure, at any time scale, giving you the economic and time-to-value benefits of cloud service with the powerful market-leading capabilities an enterprise organization needs.



## Build on a strong foundation

Splunk ES is a part of a broader Splunk security portfolio that uses Splunk Enterprise or Splunk Cloud as a core data platform and offers a range of security solutions to help your team lower their mean time to detect and respond to incidents:

- **Splunk UBA (user behavior analytics)** uses machine learning to scale advanced and insider threat detection.
- **Splunk SOAR (security operation, automation and response)** accelerates security workflows by automating and orchestrating the incident response process.
- **Splunk Intelligence Management (threat intelligence)** automates data orchestration to centralize, normalize and prioritize intelligence across all stages of security operations.

### Smarter security with machine learning and automation

With [Splunk UBA](#), Splunk's user behavior analytics tool, you can detect unknown threats and anomalous behavior using machine learning. Advanced threat detection discovers abnormalities and unknown threats that traditional security tools miss. Automatically stitching hundreds of anomalies into a single threat will help your security analysts be more productive. And deep investigative capabilities and powerful behavior baselines on any entity, anomaly or threat will accelerate your threat hunting.

[Splunk SOAR](#), Splunk's security operation, automation and response tool, lets your team work smarter, respond faster and strengthen your organization's security defenses. It automates repetitive tasks so they can focus their time and attention on the incidents and actions that matter most. Splunk SOAR reduces dwell times with automated investigations and reduces response times with playbooks that execute at machine speed. SOAR also integrates your existing security infrastructure so that each part actively participates in the defense strategy and all the parts work together.



[Splunk Intelligence Management](#), Splunk's threat intelligence tool, automates data orchestration to centralize, normalize and prioritize intelligence across all stages of security operations. It breaks down data silos to help align security effectiveness with mission objectives, improving cyber resilience and operational efficiency. With Splunk Intelligence Management, your team can easily select intelligence sources, including open source, premium intel providers and collections of historical events and alerts. They can then apply priority scores, safelists and filtering based on indicator types or attributes and submit prepared data into data repositories or a designated application of choice.

### More ways to secure and integrate

For Splunk Enterprise Security, there's also the [Unified App for Splunk Enterprise](#) and Splunk ES, which helps security professionals analyze notable events and leverage intelligence to quickly understand threat context and prioritize and accelerate triage. Analysts can leverage data in Splunk and enrich against threat intelligence feeds and case management data to gain insight into attack trends.

For more ways to integrate, [Splunkbase](#) offers thousands of security-related apps (and thousands of non-security apps as well) with pre-built searches, reports and visualizations for specific third-party security vendors. These ready-to-use apps, utilities and add-ons can help your team with security monitoring, next-generation firewall, advanced threat management and a lot more.

Along with a myriad of out-of-the-box content for specific security use cases, you can rely on [Splunk SURGe](#), a team of dedicated Splunk security experts, threat researchers and advisors, to provide you with timely research, technical guidance and tactical recommendations on how to detect, investigate and respond to the latest emerging threats.

And with the Splunk data platform as the foundation for Splunk ES, you can use Splunk to gain insight and solve problems outside of security. That same data can be tapped for all kinds of IT, DevSecOps and mission-critical initiatives.

## Let's talk real-world ROI

But a data-centric, modern SIEM solution is really expensive, right? Depends how you look at it. The real expense comes when your organization falls victim to an insider threat, a ransomware attack or another data breach, which are both costly and harmful to your organization's reputation. When you consider the risk of those costs, a data-driven security solution starts to sound like a pretty smart investment.

A modern SIEM provides immediate ROI by helping you avoid a breach and proactively protect your organization from both inside and outside bad actors. But the ROI doesn't end there.

A data-centric SIEM not only meets your security needs, but also supports IT issues such as compliance, fraud, theft and abuse detection. It's also useful for IT operations, service intelligence, application delivery and analytics. With Splunk as your SIEM, your security team can work in concert with other IT functions and gain visibility across the organization, fostering better cross-department collaboration and stronger overall ROI.

But the best way to understand the real ROI of a data-centric SIEM solution is to hear from those who already have one.



## ASU fights fraud, protects payroll – and save \$780k a year

As the largest educational institution in the United States, Arizona State University (ASU) helps set the standard for security in higher education across the globe. Guided by the mission to protect students and faculty against threats like fraud, ASU turned to Splunk to safeguard its systems.

Since deploying Splunk, the customer has seen benefits including:

- Reducing payroll and direct deposit fraud for the more than 14,600 employees on ASU's \$889 million annual payroll.
- Saving the university \$780,000 every year.
- Centralizing key data to improve student and employee experience.

ASU leveraged Splunk for security and another crucial objective: improving the student and employee experience. By using Splunk to centralize key data across campus, the university gained visibility into previously disparate systems and was able to address problems quicker and enhance the entire student experience.

[Watch the video](#) to see how public universities increase efficiency with Splunk.



---

**“Thanks to Splunk, we now have visibility into the student experience and can collect, aggregate and report on data to make business decisions faster than ever before.”**

— Nate Plamondon, Splunk Architect,  
Arizona State University

---



## InfoTeK and Splunk deliver a security intelligence platform for the public sector

Many organizations depend on SIEM software to monitor, investigate and respond to security threats. But at one U.S. government agency its mission was hampered when its legacy SIEM software from HP ArcSight failed to live up to expectations. The agency turned to InfoTeK, a leading cybersecurity, software and systems engineering firm, to replace its SIEM tool.

Since deploying the Splunk Enterprise with Splunk ES, the customer has seen benefits including:

- Deploying in one weekend and stopping an attack the next day.
- Achieving a 75 percent cost reduction to support its SIEM.
- Reducing number of tools required, including log aggregators and endpoint solutions.

With Splunk Enterprise and Splunk ES, the agency has an data-driven SIEM that provides the IT team with actionable security intelligence at an affordable cost. InfoTeK deployed Splunk software over one weekend for the customer.

Starting the very next day, the software proved its value. The IT team was able to search security events and immediately thwarted an attack vector.

[Click here](#) to learn how InfoTek reduced its SIEM costs by 75%.



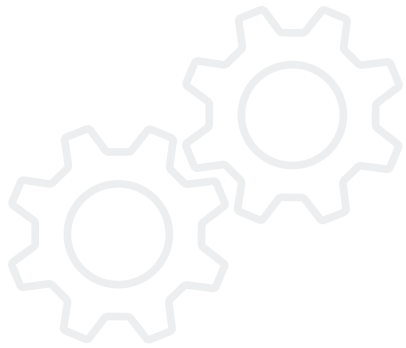
---

**“ Something that used to take hours, days or even weeks with other products or jumping between multiple tools can be done in seconds, minutes or hours with Splunk.”**

**“ We were able to provide a ROI before the product was even fully purchased because the customer successfully stopped a threat that would have required a complete rebuild of the network.”**

— Jonathan Fair, senior incident handler and security engineer, InfoTeK

---



## Heartland Automotive protects brand reputation, secures data with Splunk

Known for its signature oil change, Heartland Automotive Services, Inc., dba Jiffy Lube, is the largest franchisee of quick lube retail service stores in the U.S. Heartland Automotive needed a cybersecurity platform to protect its brand and its most important resource—its data.

Since deploying Splunk ES and Splunk UBA as its integrated SIEM platform, Heartland Automotive has seen benefits, including:

- Realizing time to value by implementing a SIEM and insider threat protection solution in only three weeks.
- Gaining a platform to drive innovation with 25% less total cost of ownership (TCO).
- Establishing real-time security investigations and insider threat protection.

SIEM implementations are often complex, as large organizations have many data sources and it may require weeks to configure alerts. According to Alams, the Splunk professional services team made the entire process of identifying the company's data sources, fleshing out the SIEM design and configuring alerts seamless.

[Click here](#) to learn how Heartland Automotive drove innovation using Splunk with 25% less TCO.



---

**“Fast time to value is everything—we were able to implement a SIEM and insider threat detection solution in three weeks in what would normally take three months.”**

**“The chief financial officer and other members of our senior leadership team have been impressed with time to value—to see it one day and almost be implemented the next—increased their confidence in us to deliver quickly.”**

— Chidi Alams, head of IT and Information Security, Heartland Automotive Services

---

## Future-proof your SIEM

Security threats will only keep advancing, and technological systems and circumstances aren't getting any simpler. So why settle for a SIEM that just meets today's needs when you could have one that helps you tackle the challenges of tomorrow?

A data-centric SIEM solution provides a solid foundation for the future with robust capabilities like real-time monitoring, incident response, user monitoring, advanced analytics and more. And by combining a data-centric SIEM with advanced threat detection and SOAR technologies under a single platform, your SOC is even better equipped to protect your organization today and in the future.

A future-ready security operations platform that allows your team to manage security events across the entire event lifecycle — all from a common work surface — will be critical in containing and remediating cyberattacks quickly. Your team will be able to respond quickly to ever-evolving threats and protect your organization by optimizing and modernizing your data, analytics and operation solutions.

Splunk is developing even more new security capabilities and integrations to help you prepare for what's ahead, including integrated threat intelligence, streamlined, cloud-based behavioral analytics and advanced risk-based alerting.

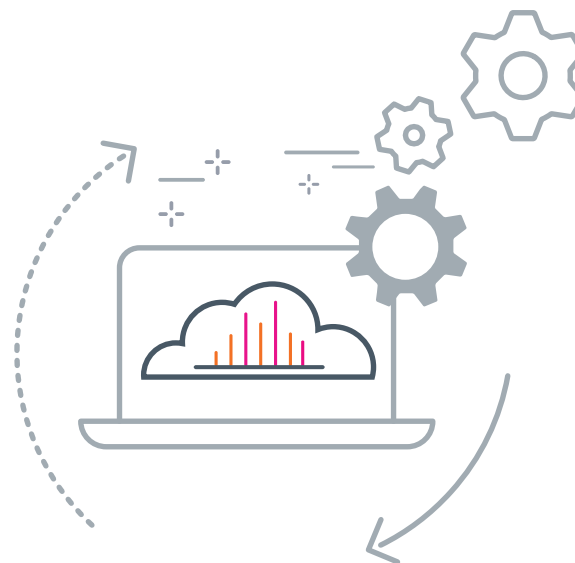
## Tap the power of data for the public sector

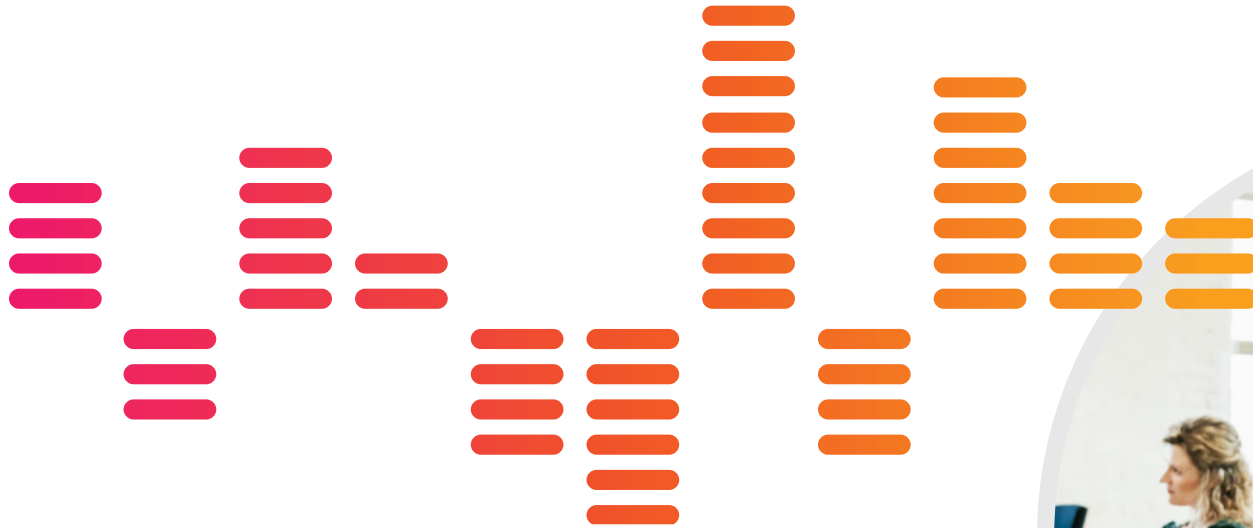
Your job in public sector cybersecurity was hard enough to begin with, and the last few years have made it even harder. It's time to put your data to work. Your agency needs powerful, flexible and fast solutions — solutions powered by data.

With a strong data and technology foundation, organizations of all kinds, including those in the public sector, can respond quickly to whatever comes their way. **Splunk** is *the* data platform for the hybrid world, empowering organizations to unlock innovation, improve security and drive mission success.

With Splunk as your cloud-based and data-driven SIEM, your agency can gain visibility across data sources and processes, keep up with security and compliance regulations, and stay one step ahead of security threats.

Ready to make Splunk your SIEM solution? [Learn more.](#)





# Get Started.

Are you ready to learn more about Splunk's analytics-driven SIEM solution and how it can help improve your organization's security posture? [Speak with a Splunk expert now.](#)

