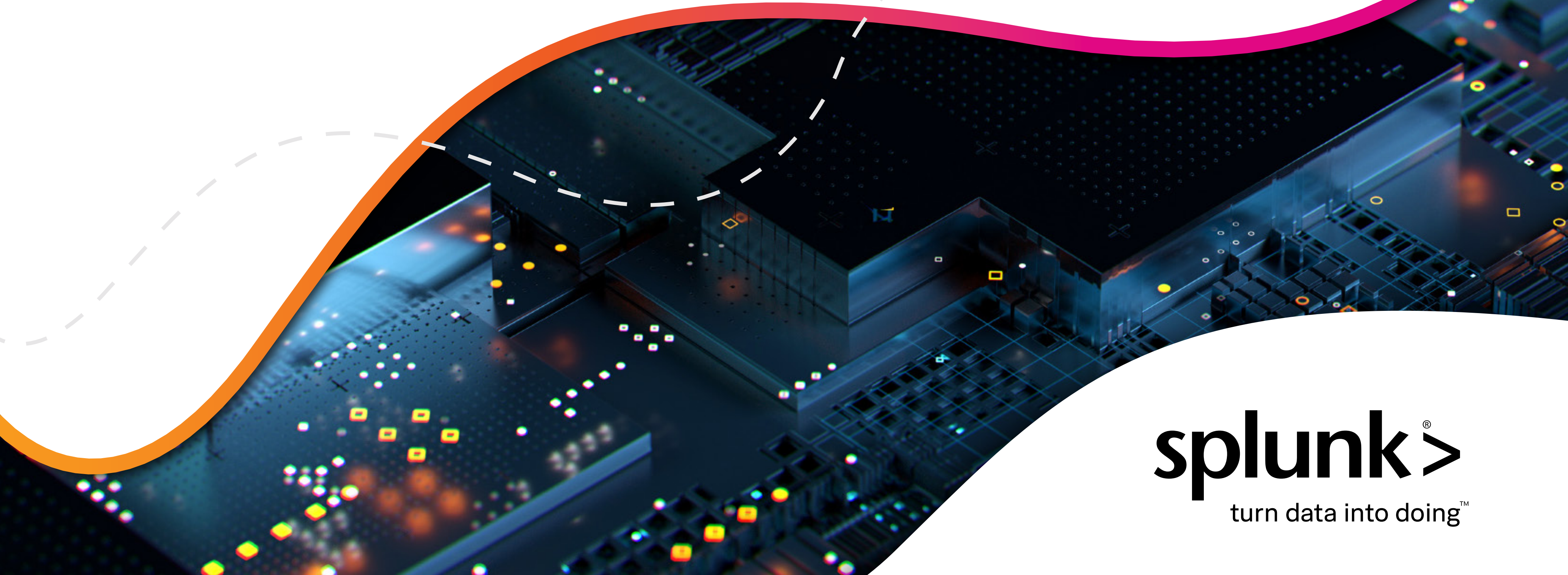
5

Top 5 Things to Consider When

Replacing a Legacy SIEM



splunk>

turn data into doing™

In the decades since security information and event management (SIEM) technology entered the market, the underlying technology has grown by leaps and bounds.

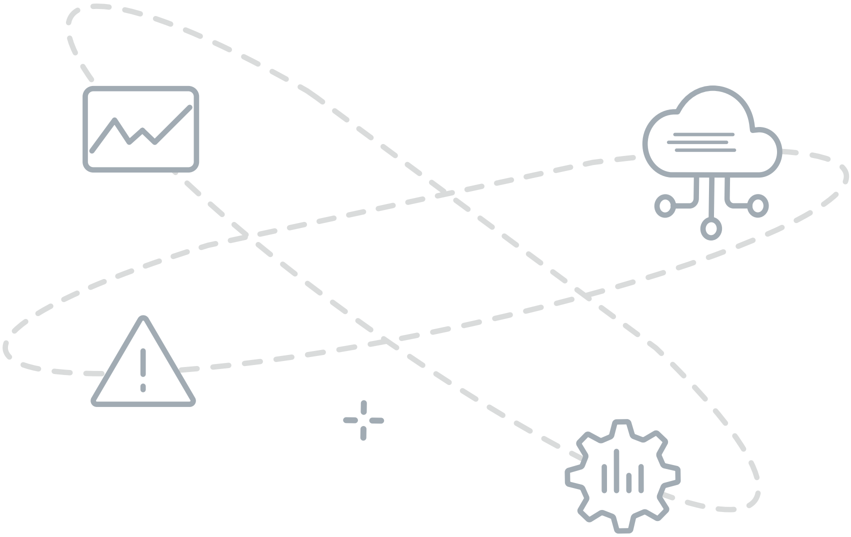
Companies running legacy SIEM solutions can't keep pace with the frequency and sophistication of today's cyberattacks, particularly with the rapid growth of digital transformation and migration to the cloud. Today's security leaders are using analytic-driven SIEMs in the cloud and on premises to quickly detect, investigate, and respond to attacks, and focusing more on information and threat management, in addition to legacy SIEM use cases like compliance and general monitoring.

If you're ready to replace your legacy SIEM, consider which new capabilities are critical to supporting your organization's business and security objectives. You'll want to strategically plan and design a successful transition to an analytics-driven SIEM taking into consideration the resources you'll need and the potential challenges your organization may face to run and fine-tune it.As you plan to replace your legacy SIEM, here are the top five things to consider:

1. **Your business drivers**
2. **The capabilities you need**
3. **Your people and processes**
4. **Planning and design: how to get there**
5. **Deployment: making it happen**

01

Your business drivers



In the past, enterprise security focused on general monitoring and compliance. Today, as organizations view security as crucial to business, demands for better security and advanced analytics are driving the SIEM market. Spurred on by **digital transformation** and **cloud migration**, data security has become a top business priority, and next-generation SIEM technologies are here to help.

More and more businesses are moving to the cloud, and fast. A new cloud infrastructure demands an upgraded cloud strategy that can be rapidly implemented. Amidst the technical challenges and time pressure of cloud migration, security requirements often get overlooked.

Security teams need to be able to analyze security data in real time and respond to increasingly sophisticated and complex attacks and breaches. With a robust new SIEM solution, you can embark on your cloud migration journey seamlessly and securely. Look for out-of-the-box cloud security monitoring content which makes it easier to detect and respond to threats across hybrid, cloud and multicloud environments. This should also include cloud attack detection rules and a vast cloud attack range.

Enterprises in the midst of digital transformation and migrating their most critical applications to the cloud should deploy tools where there is the most data gravity. Planning for successful migration and conversion of data is also crucial. If you have ever had to migrate data in the past, you know firsthand the challenges of normalizing it for your new vendor. Every second of downtime costs money and puts your organization at risk due to lack of visibility.

How Splunk helps

Enter Splunk, which offers market-leading SIEM capabilities with the economic and operational benefits of cloud service. With Splunk Enterprise Security (ES) and Splunk Cloud, customers can migrate their data to a safer location while protecting it with a market-leading SIEM. Splunk also makes data migration easier because it's a schema on-read technology and doesn't require schema at ingestion. And unlike an on-premises SIEM, Splunk Cloud manages the infrastructure for you, so your team can focus on more important things.

02

The capabilities you need

Like many SOC users, you may not be entirely satisfied with the actionable intelligence you receive from your legacy SIEM. You want alerts that are more accurate, prioritized and meaningful. Your security teams need to be able to analyze security data in real time and respond to increasingly complex threats, and new SIEM solutions have the capabilities to meet both business drivers and demands for better security with more effective detection and response capabilities.

Risk-based alerting is a relatively new approach to threat identification that reduces alert fatigue and false positives while also increasing true positives, as well as finding more sophisticated attacks that traditional searches often miss. This frees up your team's time and resources to focus on remediating actual threats and more effectively hunting for new ones.

Of course the right SIEM solution depends on the particular needs of your organization, and whether you need an on-premises, cloud or hybrid solution. You may have specific requirements for threat intelligence, database or application monitoring, vertical-specific content, and compliance reporting.

Threat detection rules are also something to consider, depending on how frequently rules are updated and how easy they are to customize. Enterprises with mature security operations capabilities should consider a single-vendor SIEM platform with native endpoint, network and UEBA modules, as well SOAR capabilities, and support for analytics, forensics/hunting and reporting/compliance.

How Splunk helps

Splunk offers **real-time, advanced analytics** that solve a wide range of security and operations use cases, with a single dashboard that provides comprehensive security-specific views of data so you can detect threats faster and optimize your incident response. Splunk's risk-based alerting dramatically reduces false positives while improving coverage of complex threats. It gives you the ability to correlate across all domains, supports ad-hoc analysis and provides actionable intelligence so you can prioritize incidents and take action. Splunk also offers end-to-end detection and response capabilities in one security solution, with the option for managed services as well as unified protection of both on-premises and cloud.

03

Your people and processes

Replacing a legacy SIEM will mean new challenges and opportunities for your team and may warrant a reevaluation of processes as well. Does your team currently have the skills they need to deploy, run and fine-tune a new SIEM, or do they need training? On-the-job training conducted while your SIEM is built can help your team hit the ground running. And when evaluating product options, look for one with robust community support and training options.

In addition to your own people, consider the level and type of outside support you may need in terms of planning, product and implementation. Based on your timeline and budget, it may be more cost-efficient to have professional services build the infrastructure components and partner with in-house architecture and engineering, then focus on in-house parallel training specific to your new SIEM tool.

Process is also a key consideration. The tool you pick may require that you redefine some of your processes around alerting, incident management and drill-down analysis. And you may need to align processes across vendors as well as your architecture and cloud implementation teams. Changing processes can be challenging, but the benefits are enormous: with risk-based alerting, less alerts and false positives will free up your team to focus on real threats and other important tasks. And with a legacy SIEM it's time-consuming and resource-intensive to keep your environment running at peak functionality and find ways to optimize storage. Replacing your legacy SIEM with one based in the cloud means you no longer have to manage an on-premises infrastructure.

How Splunk helps

In addition to the benefits of the cloud and risk-based alerting, Splunk supports your people and processes by offering robust training, community support and up-to-date release documentation. Training options include courses tailored specifically for administrators and end-users to help your team learn to install, configure and manage your SIEM solution, and use Splunk to identify security incidents, analyze risks, use predictive analytics and discover threats.

04

Planning and design: how to get there

As you evaluate and plan for your new SIEM, bear in mind scalability and integration. Consider the volume of data that you'll need to ingest per day and how many different sources that data will be coming from. Integration can be a big challenge for enterprise SIEM deployment, so consider what other technologies your new SIEM technology needs to integrate with, such as:

- On-premises and AWS security data
- Endpoint, network and vulnerability scanning logs
- Identity repositories for user authentication
- Enterprise research planning (ERP) solutions, third-party, big data platforms or SOARs
- Existing ticketing and incident management systems
- Streaming data from several security technologies

Experts recommend that you design your SIEM to automate data ingestion across both on-premises and cloud data sources as much as possible. And standardizing the data parsing will ensure your use cases can be built seamlessly and your acceleration can be applied to many use cases for timely incident detection.

How Splunk helps

Splunk's professional services team offers a series of paid planning and design services to help enterprise security customers derive the most value for their investment and support rapid implementation where needed. Offerings include a solutions architect to design and plan around your needs, best practice installation, data onboarding of essential data sources and the implementation of prescriptive use cases.

05

Deployment: making it happen

Your organization’s particular timeline and transitional logistics will depend on how quickly you need to deploy and the complexities of your transition. You’ll want to determine which aspects of your deployment can be automated and auto-scalable. Automating as much of the process as possible will aid deployment and subsequent upgrades.

Most enterprise organizations also face integration challenges in transitioning to a new SIEM. For a seamless transition, you’ll need to maintain both SIEMs, so you’ll need your current systems to continue their processes while you deploy the new one. Transitioning may require integrating streaming data from several security technologies, rule conversion and use case transition, as well as parallel deployments (for example, with enterprise syslog). The aim should be for an invisible transition – one that doesn’t risk visibility and detection.

When it comes to deployment options, many new SIEMs allow for customization as well as automation. Organizations can mix and match appliances, virtual appliances and software to build functional stacks for flexible deployment and horizontal scalability. With a new SIEM, you can also customize existing rules and predefined reports. And new SIEMs can combine on-premises, cloud and hybrid deployments to create a cloud-based SIEM solution that goes beyond mere detection and response.

How Splunk helps

Splunk gives you the scalability, automation and integration capabilities you need from transition through deployment and beyond, as well many ways to customize. And Splunk offers SIEM as a cloud service as well as on-premises and hybrid deployment models, with full feature parity across all deployment models.

Whatever your organization’s business drivers and security requirements, today’s analytic-driven SIEM solutions offer the capabilities you need to support your organization’s business and security objectives. With the right planning, design, training and support, your team can successfully deploy, run and fine-tune a new SIEM that meets your current needs and prepares you for the future so you can leave that legacy SIEM in the past, where it belongs.

Getting started

Ready to retire your legacy SIEM for an integrated, cloud-based service? Discover why you should use Splunk for your new SIEM solution.

Learn More

splunk>®

turn data into doing™