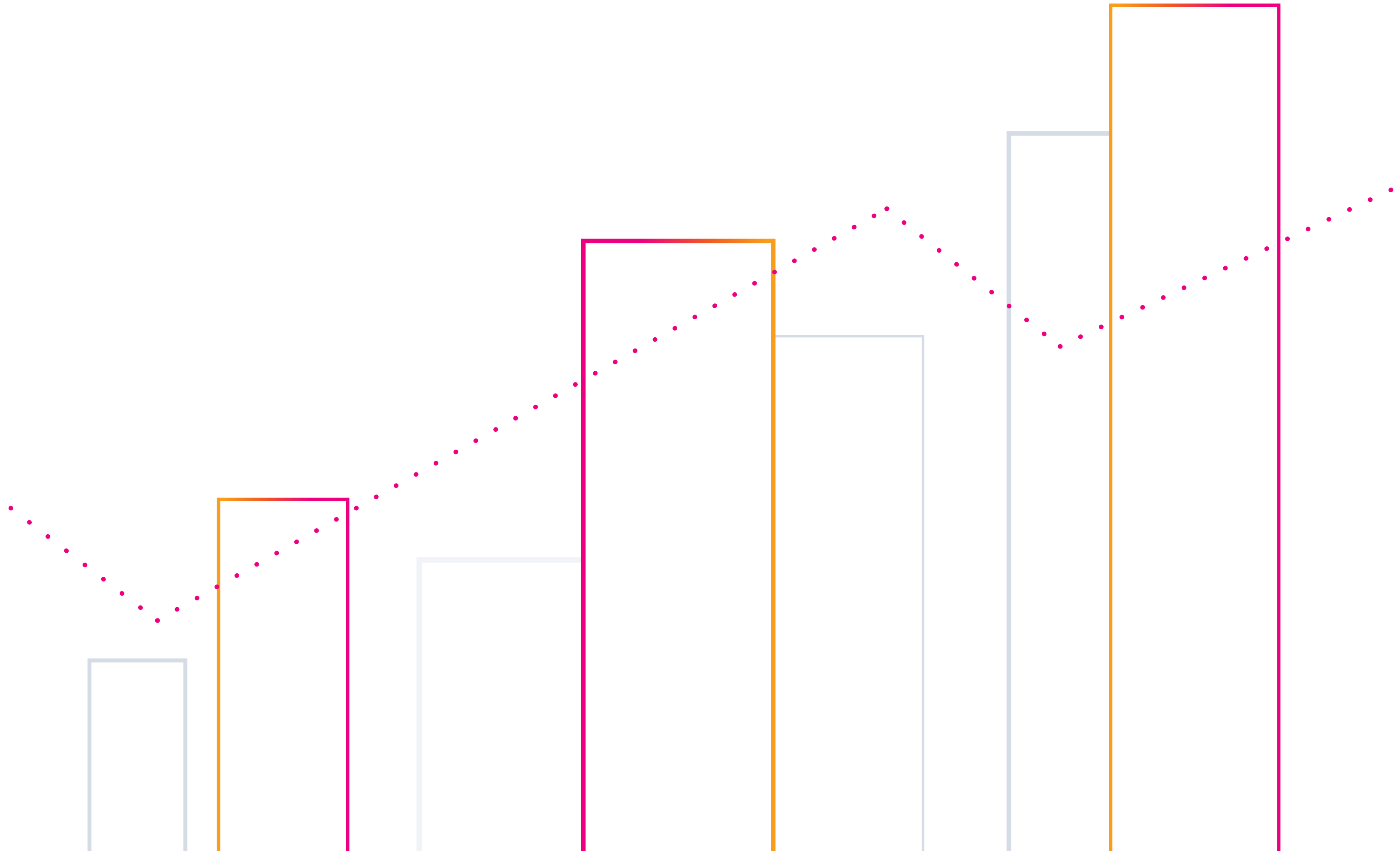
WHITE PAPER

Taking Your SIEM to the Cloud

Simplify and strengthen security management with cloud-based SIEM



Situation Overview

A security information event management (SIEM) solution is like a radar system that pilots and air traffic controllers use. Without one, enterprise IT is flying blind. Although security appliances and system software are good at catching and logging isolated attacks and anomalous behavior, today's most serious threats are distributed, acting in concert across multiple systems and using advanced evasion techniques to avoid detection. Without a SIEM, attacks are allowed to germinate and grow into catastrophic incidents.

The importance of a SIEM solution to today's enterprise is magnified by the growing sophistication of attacks and the use of cloud services that only increase the surface of vulnerability. As more businesses evolve their infrastructure into the cloud, security strategies and technology must also adapt. Organizations increasingly are turning to SIEM deployed in the cloud or as software-as-a-service (SaaS) to strengthen security management while reducing the resources required for protection.

SIEM: What's Inside?

Enterprise security teams must use a SIEM solution that not only solves common security use cases, but also advanced use cases as well. To keep up with the dynamic threat landscape, modern SIEMs are expected to be able to:

- Centralize and aggregate all security-relevant events as they're generated from their source
- Support a variety of reception, collection mechanisms including syslog, file transmissions, file collections and more
- Add context and threat intelligence to security events
- Group correlation searches into clusters of events to enhance visibility and responsiveness with focused threat detection and accelerated incident investigation
- Correlate and alert across a range of data
- Detect advanced and unknown threats
- Profile behavior across the organization
- Ingest all data (users, applications) and make them available for use — monitoring, alerting, investigation and ad hoc searching
- Reduces risk by enabling faster detection and incident response to newly discovered and ongoing threats with ready to use relevant content
- Provide ad hoc searching and reporting from data for advanced breach analysis and track potential attackers' actions
- Investigate incidents and conduct forensic investigations for detailed incident analysis
- Assess and report on compliance posture
- Use analytics and report on security posture

Although primarily gathered from servers and network device logs, SIEM data also can come from endpoint security, network security devices, applications, cloud services, authentication and authorization systems and online databases of existing vulnerabilities and threats.

But data aggregation is only half of the story. SIEM software then correlates the resulting repository looking for unusual behavior, system anomalies and other indicators of a security incident. This information is used not only for real-time event notification, but also for compliance audits and reporting, performance dashboards, historical trend analysis and post-hoc incident forensics.

Given the escalating number and sophistication of security threats, along with the increasing value of digital assets in every organization, it's not surprising that adoption of SIEM continues to grow as part of the overall IT security ecosystem. Gartner pegged the growth for the SIEM market at 12.5 percent in 2015 and expects the double-digit growth to continue in 2016 and beyond.[1]

A SIEM solution is like a radar system that pilots and air traffic controllers use. Without one, IT is flying blind.

[1] "Magic Quadrant for Security Information and Event Management," by Kelly Kavanagh, Oliver Rochford, Gartner, July 20, 2015, ID G00267505, **http://www.splunk.com/goto/SIEM_MQ**

Key Benefits of Taking SIEM to the Cloud

Running SIEM in the cloud or as SaaS can help solve the problems many organizations have with security intelligence, yet many IT leaders still distrust cloud security and reliability. Before eliminating cloud-based SIEM, know that the security practices and technology at most large cloud services can be far more sophisticated than those in the typical enterprise. SaaS is already widely used for business-critical systems like CRM, HR, ERP and business analytics. The same reasons that SaaS makes sense for enterprise applications — fast, convenient deployment, low-overhead operations, automatic updates, usage-based billing and scalable, hardened infrastructure — make the cloud a great fit for SIEM.

Cloud-based solutions provide the flexibility to use a wide range of data sets from on-premises and cloud. As more enterprise workloads move to infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and SaaS, the ease of integrating with third-party systems shows that SIEM in the cloud makes even more sense.

Key benefits of taking your SIEM to the cloud include the flexibility of a hybrid architecture, automatic software updates and simplified configuration, instant, scalable infrastructure, and strong controls and high availability.

Flexible, Hybrid Architecture

The enterprise use of cloud services is accelerating and many organizations now have a hybrid environment with data and applications both on-premises and in the cloud. That means regardless of where a SIEM product is deployed, it must be able to collect data for both environments.

Taking a SIEM to the cloud gives enterprises more flexibility. With a hybrid cloud deployment, a SIEM can be deployed in a company's private data center but still aggregate data from on-premises and cloud services — and also be used as a cloud service that can pull security data from anywhere.

Automatic Software Updates and Simplified Configuration Management

The rapidly changing threat landscape, with increasingly complex and effective attacks, makes it hard for security professionals and their tools to keep up with the state of the art. A SIEM system should help, not hinder their efforts. However, because many legacy SIEM vendors place constraints on the data schema, hard-coding threat and log event formats or attack signatures, they might miss the latest exploits.

A SIEM product is only as good as its ability to evolve with the threat environment. A cloud-based SIEM leverages its flagship big data architecture to create dynamic schemas-on-the-fly to catch threats that can escape hard-coded threat definitions.

A cloud-based SIEM is flexible, easier to manage, scalable and highly available.

Robust and Scalable Infrastructure

In addition, provisioning and operating infrastructure for an on-premises based SIEM requires time and operational effort.

Security systems must adapt to both data growth and the diversity of sources. SIEM in the cloud allows organizations to instantly deploy and easily scale according to their data needs. Consolidating all relevant security information in a single repository, ensuring that it's protected, indexed and analyzed, is the best way to improve security-related decisions.

Strong Controls and High Availability

Enterprise services, particularly for something as critical as SIEM, must address common concerns around cloud services security, controls and performance.

- **Data and system security:** SaaS providers often run on one of the major IaaS platforms like Amazon Web Services (AWS), Google Cloud Platform or Microsoft Azure. These leading cloud infrastructure providers operate secure data centers with audited security policies that are capable of achieving SOC 2 Type II and ISO 27001 certifications. A best practice for SIEM services is to logically separate customer data by assigning each to dedicated virtual servers and customer-specific storage. Customer data in transit must be encrypted using SSL and optionally at rest using AES-256 with unique keys that are regularly rotated.
- **Data sovereignty and residency requirements:** Using a hybrid cloud architecture is a good option for SIEM since it means data subject to locally-specific privacy, handling or regulatory requirements can stay on-premises or in a local region from an IaaS provider. By hosting at a major IaaS provider, organizations have the option of deploying in regions around the world. AWS even provides a FedRAMP-certified region for U.S. federal users with AWS GovCloud (US).
- **Service control and customization:** Moving to the cloud shouldn't mean losing control over important application settings and security policies. A SIEM cloud service must provide users control over application-level governance while insulating them from infrastructure-level details. And that allows organizations to retain control to meet internal and external requirements.

Fairfax County Protects Data With Splunk Enterprise Security In The Cloud

Fairfax County, Virginia employs 12,000 people across more than 50 agencies and serves more than 1.1 million citizens. Its government is regarded as a leader in many areas when it comes to cybersecurity and IT, enabling it to serve the needs and protect the data of its IT-savvy and high profile citizens. Since deploying Splunk Enterprise Security (ES) with Splunk Cloud as its SIEM platform, Fairfax County has seen benefits including:

- Proactively supporting more than 50 county agencies and protecting citizens' data
- Reducing security reporting from two weeks to real time
- Increasing focus on strategic initiatives by leveraging cloud services

According to Mike Dent, chief information security officer (CISO) for Fairfax County, 210 IT professionals support more than 50 county agencies, each with unique business and security requirements. Some agencies, such as the Health Department, are governed by regulations like HIPAA, while others must comply with payment card industry (PCI) regulations. Ultimately, the county requires reliable and secure access to data so it can make the best decisions to support county citizens.

One of the major challenges Dent and his team faced was centered around the numerous disparate systems from which it pulled event logs. What's more, its previous SIEM tool could not keep up with the more than 3.9 petabytes of data the county must control, access and secure. Dent explains that after comparing the Splunk data analytics platform to several other products, the county partnered with Splunk's professional services team to conduct a successful proof of concept, and then moved forward with an implementation that was easy on his staff.

"Previously, reporting to leadership was difficult because everything was manual. My staff would spend countless hours, probably two weeks' worth of work, to get me a summary report of our cybersecurity stance," Dent says. "Now, with the Splunk platform, I have real-time access and can give an overall security posture to my leadership to let them know when we have issues."

- **Application performance and availability:** Running on a major IaaS provider like AWS allows a SIEM service to provide state-of-the-art system availability at a reasonable price. For example, the service can be architected to span multiple cloud availability zones or regions, which means that the service stays up even if an individual data center goes offline.

The Power of Big Data Analytics and SIEM in the Cloud

Running SIEM in the cloud has many benefits, but combining it with a big data analysis platform delivers log analysis and reporting for all system and application metrics. Products that are built on an Operational Intelligence and log analysis platform allow security-related data and operational logs to be combined and correlated, allowing businesses to make optimal security decisions. Such a symbiotic combination provides end-to-end application monitoring, troubleshooting and Operational Intelligence plus a full-featured SIEM.

The best Operational Intelligence platforms are designed to consume, collect and make sense of log records from myriad systems and is a time-tested platform used in organizations large and small. These platforms deliver real-time data collection, search across all data with a rich query language, data visualization and statistical analysis features that can feed real-time information dashboards. For SIEM, these platforms should add support for external threat intelligence data feeds including STIX/TAXII formats such that multiple threat intelligence sources can be aggregated, and weighted to build a range of security indicators.

City Of Los Angeles Integrates Real-Time Security Intelligence Across 40+ City Agencies

Los Angeles is a vast metropolis with critical infrastructure like airports, seaports, and water and power, as well as 35,000 employees and over 100,000 endpoints generating 14 million security events daily. The city's departments had their own security tools, requiring it to gather and manually correlate logs from each agency for broad views of its network security — an untenable process that was cumbersome, imprecise and slow to address threats. To better protect its digital infrastructure, Los Angeles sought a scalable cloud-based SIEM to identify, prioritize and mitigate threats, gain visibility into suspicious activities and assess citywide risks.

After considering available solutions, Los Angeles chose Splunk Cloud and Splunk Enterprise Security for its extraordinary scalability and 100 percent uptime SLA. "Splunk Cloud was fast to deploy and easy to tailor, whereas customizing competing products required two full-time employees," says Timothy Lee, chief information security officer for the City of Los Angeles.

Since deploying Splunk Cloud and Splunk Enterprise Security, the city has seen benefits including:

- Creation of citywide security operations center (SOC)
- Real-time threat intelligence
- Reduced operational costs

Splunk's real-time situational awareness and timely threat intelligence is enabling the city to securely lock down its digital assets. By anchoring its integrated SOC with the rich SIEM functionalities of Splunk Cloud and Enterprise Security, Los Angeles met its mayor's directive by transforming its patchwork of security measures into a cohesive, all-encompassing cyber security strategy. "For municipalities that are decentralized into many departments, the Splunk platform is a comprehensive yet cost-effective security solution," says Lee.

Combining SIEM with a big data platform that can pull data from any system allows businesses to achieve a unified view of the most important operational, application performance and security metrics. By deploying it as a cloud service, organizations derive value immediately without lengthy setup and learning curves or high up-front expenses, yet are still able to collect and analyze data from all environments — including both cloud and on-premises systems.

With sources of relevant security information and overall data volumes exploding, a cloud service is a perfect solution for SIEM deployments. Building SIEM upon a proven data aggregation and analysis platform like Splunk leverages the same rich features designed to improve IT operations for security management all in one package.