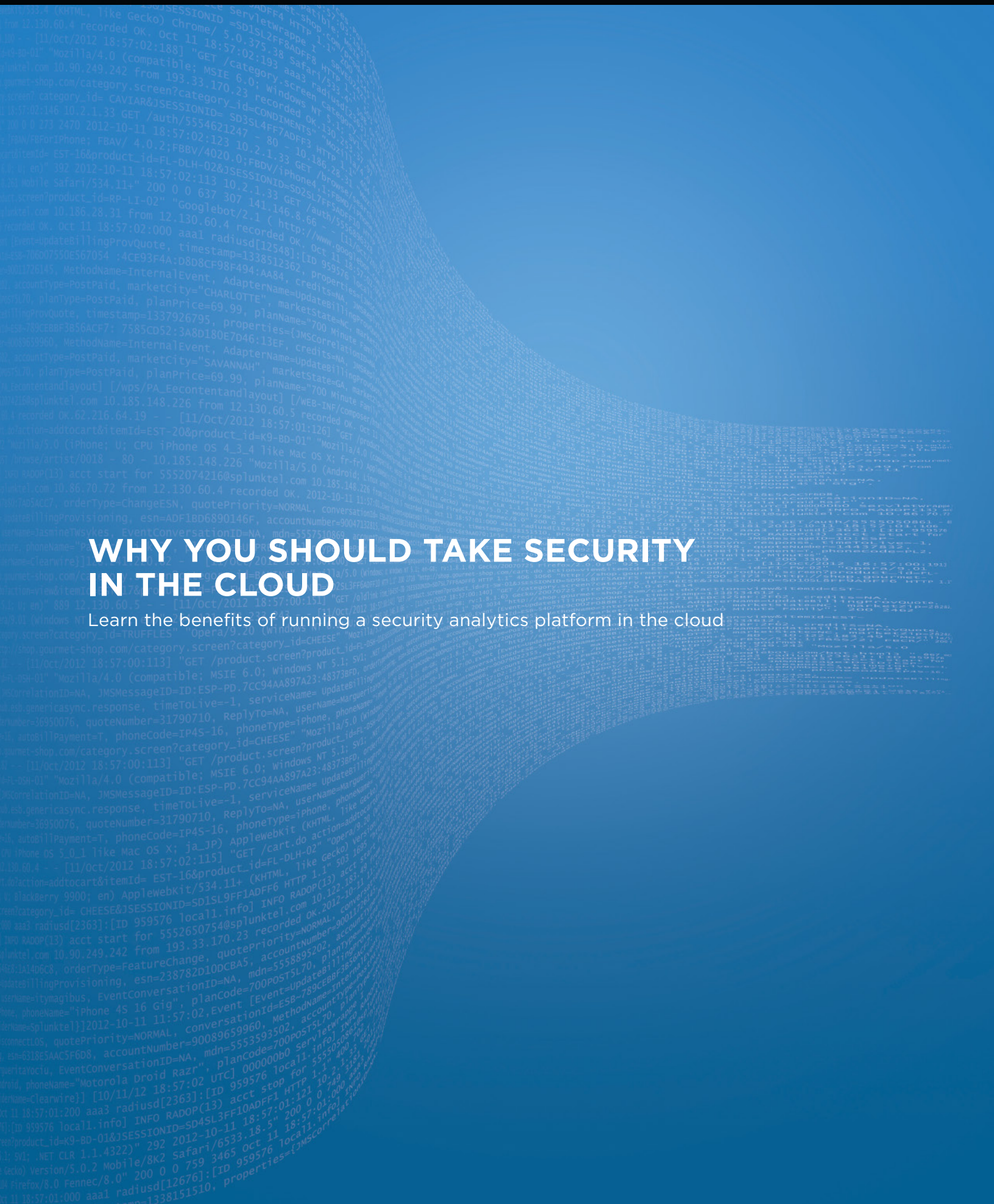
splunk>

WHITE PAPER

WHY YOU SHOULD TAKE SECURITY IN THE CLOUD

Learn the benefits of running a security analytics platform in the cloud



Advanced security threats and attacks are getting harder to detect as hackers are becoming more sophisticated. At the same time, the tools used to defend against cyberattacks keep multiplying and becoming more complex. Companies are also dealing with the challenge of not having enough qualified security staffers to keep the bad guys out.

Cyber Criminals | **Malicious Insiders** | **Nation States**

The time to solve these problems is now and not in the middle of an advanced attack or while investigating a potential breach. Time is the fleeting commodity that security teams cannot afford to spend trying to acquire skilled staff, hardware or deployment capabilities, especially in the middle of a potential threat investigation.

To get ahead of advanced attacks and threat actors, security teams need the ability to conduct ad hoc analysis across all cloud and on-premises data – from the network, endpoints, identity and threat intelligence as well as non-traditional security data — in near real time.

100% Valid credentials were used

99 Median # of days before detection

67% Victims notified by external entity

Organizations also need the ability to monitor and report in real time on threats, attacks and other abnormal activity from across all security-relevant data with business context. With advanced analytics, customers realize accelerated threat detection and rapid incident response across an entire security ecosystem.

Embrace the Cloud

Luckily there is light in these seemingly dark times. In fact there is an opportunity for security teams to improve their security and intelligence operations at the same time. Security teams need to adopt a cloud-based analytics-driven security solution to secure their cloud workloads and existing on-premise systems together.

A cloud-based analytics-driven security solution is defined as a platform that empowers organizations to stay ahead of ever-changing cyberthreats and quickly remediate breaches when they happen, while still being able to focus on critical business needs.

The flexibility of the cloud also makes an analytics-driven security solution accessible to organizations of all sizes because of the cost-savings involved with not having to hire extra staff or buy expensive on premises hardware.

A cloud-based analytics-driven security solution scales while securing an organization's journey to the cloud. It also provides deep insights into the cloud and hybrid security ecosystem and applications. This often helps companies realize value within hours of embracing the cloud.

More specifically, an analytics-driven security solution based in the cloud can be used to detect advanced malware, investigate advanced threats and for rapid response. The cloud-based solution also helps organizations gain and maintain compliance quickly, while protecting sensitive IP and critical assets.

The Cloud With Significant Benefits

Some still question the safety of running a security solution in the cloud. But protecting a security solution in the cloud is no different than securing many other software-as-a-service (SaaS) solutions organizations already rely on every day. A cloud-based security solution can solve the problems many organizations have with security intelligence.

Before eliminating a cloud-based security solution, 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. SaaS is also relied on to deliver commonly used software

such as Microsoft Office 365, Salesforce.com, Okta, Box, ServiceNow, AWS and more.

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 security.

Cloud-based security 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 security in the cloud makes even more sense.

Key benefits of taking your analytics-driven security solution to the cloud include the flexibility of 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 security solution is deployed, it must be able to collect data for both environments.

In fact, a **recent report found** that IT executives believed the cloud and SaaS will be the second **most disruptive technology** over the next 3 to 5 years. This is why 1 in 3 of those executives are also expecting to increase spending on the cloud in the next year. This while the industry **is planning to decrease** spending on hardware and legacy systems in the next year.

Taking a security solution to the cloud also gives enterprises more flexibility. With a hybrid cloud deployment, a security solution 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.

Robust and Scalable Infrastructure

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

Security systems must adapt to both data growth and the diversity of sources. An analytics-driven security solution 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 must address common concerns around cloud services security, controls and performance. Including:

Data and system security: SaaS providers often run on one of the major IaaS platforms like 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 security 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 security solutions 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 cloud-based security solution 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.

Application performance and availability: Running on a major IaaS provider like AWS allows a security 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.

Enter Splunk

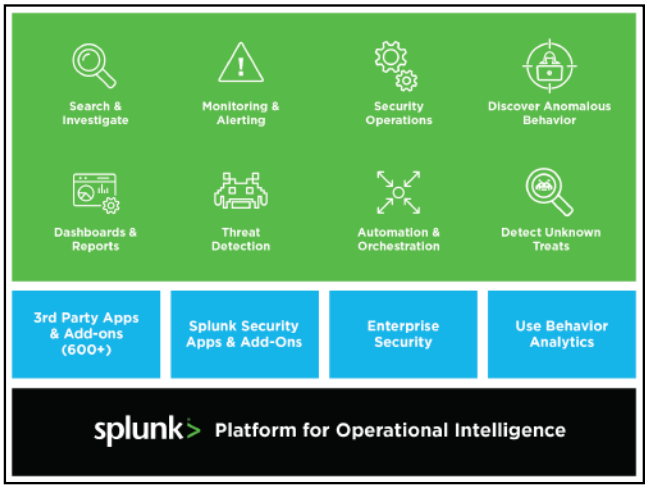
The Splunk cloud-based analytics-driven security portfolio consists of **Splunk Enterprise** (the software as a service solution is Splunk Cloud), **Splunk Enterprise Security** (ES) and Splunk UBA, which works to bring multiple IT areas together to enable collaboration and implement best practices to address modern cyberthreat challenges.

Splunk Enterprise **is deployed** on Amazon Web Services (AWS). It is self-contained and can be easily deployed on any EC2 instance, and it also scales horizontally, making it ideal for an AWS deployment

With the Splunk platform as your nerve center, security teams can leverage statistical, visual, behavioral and exploratory analytics to drive insights, decisions and actions.

The Power of Big Data Analytics and Cloud-Based Security

Running your security solution in the cloud has many benefits, but combining it with a big data analysis platform, such as Splunk delivers log analysis and reporting for all system and application metrics. Such a symbiotic combination provides end-to-end application monitoring, troubleshooting and security analytics plus a full-featured analytics-driven security solution.



The best security analytics 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.

Combining a security solution 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 security deployments. Building a security platform 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.

Try Splunk Enterprise Security now. Experience the power of Splunk Enterprise Security – with no downloads, no hardware setup and no configuration required. The Splunk Enterprise Security Online Sandbox is a seven day evaluation environment with pre-populated data, provisioned in the cloud, enabling you to search, visualize and analyze data, and thoroughly investigate incidents across a wide range of security use cases. You can also follow a step-by-step tutorial that will guide you through the powerful visualizations and analysis enabled by Splunk software. **Learn more**