aws | splunk>

WHITE PAPER

ENHANCE AWS SECURITY WITH SPLUNK® SOLUTIONS

An AWS and Splunk White Paper

Executive Summary

Cloud security has evolved well beyond what most people remember from the early days of cloud computing. Using AWS and Splunk, organizations can directly address security risks that have traditionally been of concern, related to moving to a shared resource model with externalized management.

Introduction

Many organizations are moving to the cloud to take advantage of the benefits it provides, such as increased levels of performance, accessibility, and easily scalable storage and computing power that is difficult for on-premises environments to match. While organizations of all sizes have increasingly looked to the cloud to provide the storage and computing power needed for their business applications, many are still hesitant to make the switch.

The concerns with security in the cloud have morphed considerably as adoption has increased. For example, in 2010, according to the Cloud Security Alliance (CSA), key top concerns included abuse and malicious use of cloud services, as well as potential exploit of vulnerabilities within the shared technology components that are used in cloud infrastructure.

Fast forward to today – and similar to on-premises environments, data breaches are the top concern.

Generally speaking (for cloud and on-premises alike), data breaches and associated data loss are costly – globally, the average total cost of a data breach was $3.86 million (up 6.4% from 2017) and the average cost for each lost record was $148 (up 4/8% from 2017), according to the "**2018 Cost of Data Breach Study: Global Overview**", published by the Ponemon Institute.

A critical point from the study is that when it comes to data breach, the faster a threat can be identified and contained, the lower the costs – that is, the faster the organization can detect a priority issue that could result in a breach, and respond accordingly, the greater the chance that the cost of the breach will be less damaging.

In this paper we'll take a look at some concepts that are key to implementing better cloud security and that help minimize the risk of a breach. The result is an overall improvement to security posture, accuracy of threat detection, and operational efficiency.

Throughout we'll provide key insights into how AWS and Splunk, an AWS Partner Network (APN) Security Competency Partner, can help.

Physical Security

The IDC Report, "Security Solutions: Security in the Cloud**," states that workloads can actually be more secure in an AWS deployment than they would be within an on-premises environment. AWS provides a robust infrastructure and a global, world-class team of security experts that are monitoring AWS systems 24 hrs per day, 7 days per week, all year round, to protect AWS infrastructure around the globe.

As of July 2018, AWS's global infrastructure footprint consists of 18 geographic Regions and 1 Local region around the world, with 55 Availability Zones (AZs) (figure 1). Each Region consists of at least 2 AZs, which consist of one or more discrete datacenters, each with redundant power, networking and connectivity, housed in separate facilities. This infrastructure footprint enables AWS to provide reliable service around the globe. In addition, geographic redundancy of these datacenters means your AWS workloads can be online in the face of most failure scenarios, even natural disasters.

AWS Security doesn't just include geographic dispersion. Within each Availability Zone, AWS networks are secured with firewalls and other boundary devices placed to monitor and control communications at the external boundary of the network. Networks are also protected by strategically placed access points to the cloud. These access points, called API endpoints, allow secure HTTP (HTTPS) access and use Transport Layer Security (TLS), a cryptographic protocol designed to protect against eavesdropping, tampering, and message forgery, to establish a secure communication session with your storage or compute instances within AWS.

Figure 1.

The security provided by a geographically dispersed network, secure access points, plus the added security services and tools available through AWS and Splunk create a level of security that is difficult and costly for most organizations to match in an on-premises environment.

Securing Cloud Infrastructure

In addition, there are several key areas where AWS infrastructure provides enhanced security without compromising on the necessary elasticity required to accelerate innovation. Organizations can leverage capabilities from AWS and Splunk to gain greater security capabilities spanning segmentation, encryption, authentication, and logging and monitoring when compared to legacy architectures.

Data Segmentation

Creating the needed level of segmentation to protect an organization from catastrophic data loss (e.g. from a server failure or breach) can be very resource intensive in an on-premises environment. To achieve the level of versatility required by modern application architectures, organizations can leverage Amazon Virtual Private Cloud (Amazon VPC). Amazon VPCs are logically isolated sections of AWS where you can launch resources in a virtual network you design and control. Through the use of Amazon VPCs and built-in firewalls, AWS is able to segment data with less resources and at a much lower cost than an on-premises environment.

Data Encryption

Data encryption is something that often gets neglected by organizations with on-premises environments. To make matters worse, as the amount of data stored grows and becomes more complex, it becomes more difficult to encrypt. Using Splunk Cloud helps this problem by utilizing standard SSL encryption for data in transit, plus optional AES 256-bit encryption for data at rest. Additionally, AWS gives you the ability to encrypt uploaded data using either your own 256-bit AES key through an Amazon service that automatically encrypts data uploaded to it, such as Amazon Simple Storage Service (Amazon S3), Amazon Glacier, and Amazon Elastic Block Store (Amazon EBS); or by utilizing a master 256-bit AES key through AWS Key Management Service (AWS KMS). AWS KMS is a service that helps you easily create and control your encryption keys, adding a level of simplicity to your data encryption needs.

Authentication and Access Management

To control access to your services and resources, AWS provides the AWS Identity and Access Management (IAM) service. Using IAM, your organization can create and manage AWS users and groups, and set permissions to allow and deny their access to AWS resources. IAM allows users to federate into their AWS environment with their current identity provider (such as Active Directory). It also adds the ability to use AWS Multi-Factor Authentication (MFA), a best practice that adds an extra layer of protection on top of a username and password. With MFA enabled, when a user signs into an AWS website, they must enter their username and password, then provide an authentication code from their AWS MFA-enabled device.

Central Logging and Monitoring Security Posture

With Splunk on AWS, you can enhance your logging and monitoring capabilities. AWS provides a suite of services you can use to monitor your environment including AWS CloudTrail, AWS Config, Amazon

Inspector, Amazon CloudWatch, Amazon Kinesis Data Firehose, and Amazon GuardDuty — and Splunk can draw from any or all of these services to analyze logging and monitoring data all in one place.

AWS CloudTrail supports your cloud security by recording API calls for your account and delivering logs to you. It records information including the identity of the API caller, the time of the call, the source IP address of the caller, the request parameters, and the response elements returned by the AWS service.

AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration, history and configuration change notifications, enabling you to achieve better security and governance. With Config Rules, you can create rules that automatically check the configuration of AWS resources recorded by AWS Config.

Amazon Inspector helps you improve the security and compliance of applications deployed on AWS through an automated security assessment service. Amazon Inspector is designed to automatically assess applications for vulnerabilities or deviations from best practices and produces a detailed list of security findings prioritized by level of severity.

Amazon CloudWatch is a monitoring service that collects and tracks metrics, collects and monitors log files, sets alarms, and automatically reacts to changes in your AWS resources.

Amazon Kinesis Data Firehose is the easiest way to reliably load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Splunk, enabling near real-time analytics with existing workflow and dashboards you're already using today.

Amazon GuardDuty provides intelligent threat detection by collecting, analyzing, and correlating billions of events from AWS CloudTrail, Amazon VPC Flow Logs, and DNS Logs across all of your associated AWS accounts.

Splunk enhances the value of these services by analyzing and delivering real-time insights from these data sources in one centralized view. With Splunk solutions, you can easily drill down into the data from the above services to rapidly identify correlations and determine root causes of unusual activity, enabling you to quickly address and mitigate risks.

Logging gives you the ability to gain operational insight into your organization's workloads and identify potential vulnerabilities before they become issues. Together, Splunk and AWS provide the necessary services to gain the full operational visibility needed to help keep your IT infrastructure secure.

Threat Detection

Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance attempts by attackers.

Enabled with a few clicks in the AWS Management Console, Amazon GuardDuty can immediately begin analyzing billions of events across your AWS accounts for signs of risk. GuardDuty identifies suspected attackers through integrated threat intelligence feeds and uses machine learning to detect anomalies in account and workload activity. When a potential threat is detected, the service delivers a detailed security alert to the GuardDuty console and AWS CloudWatch Events. This makes alerts actionable and easy to integrate into existing event management and workflow systems.

Using Splunk, you can ingest GuardDuty events and perform correlation searches with other data sources, such as AWS Config data, VPC Flow data, AWS CloudTrail data, or other data sources, to verify a threat or to find associated activities, or investigate root cause and determine remediation steps. For example, if there is indication of a data breach, you can use Splunk with GuardDuty data and other data sources to help quickly gain key insights into affected or compromised accounts and users, instances and other resources affected, which regions, how an attack might have initiated, whether or not it resulted in data exfiltration, and other key evidence you would need to collect as part of your standard incident investigation and response procedure.

Working with the AWS Shared Responsibility Model

Gartner predicts that through 2020, 95 percent of cloud security failures will be the customer's fault. This prediction is an indication that in general, most concerns about cloud providers' ability to deliver on their security responsibilities have been largely alleviated by the cloud providers' direct attention to prioritizing security for their customers.

The fact that cloud providers have stayed highly motivated in addressing security concerns is not surprising, given the massive potential of cloud computing. Nonetheless, not all responsibilities lie with the cloud provider, thus there is a need for a clear delineation of security responsibilities in a cloud services environment.

The **AWS Shared Responsibility Model** is the set of guidelines established by AWS to determine with whom a given security responsibility lies. While AWS takes responsibility for the security of the cloud, customers are responsible for the security of their workloads on the cloud. This means that AWS takes responsibility for securing the network and physical infrastructure of the cloud, but customers are responsible for securing their own application data and the virtual environment they run within that infrastructure. Splunk solutions can help meet security responsibilities in an AWS environment.

AWS provides much of the security needed, but before an organization begins deploying their applications on the cloud, it is important that they have a clear understanding of their role in keeping their data secure. While the AWS infrastructure is designed for security, reliability, and compliance, the organization is responsible for securing the following within their own AWS environment:

- Customer Data
- Platform
- Applications
- Identity & Access Management
- Operating System
- Network & Firewall Configuration
- Client-Side Data Encryption & Data Integrity
- Authentication
- Server-Side Encryption
- Network Traffic Protection

Security by Design

To help with architecting a secure environment, AWS provides a set of templates, reference architectures, and best practices called **AWS Security by Design (SbD)**. SbD provides a pre-validated architecture that takes key security considerations into account, and is a great way to get your security quickly set up. SbD is a security assurance approach that formalizes AWS account design, automates security controls, and streamlines auditing. SbD encompasses a four-phase approach for security and compliance at scale across multiple industries, standards and compliance capabilities for all phases of security. It allows organizations to design everything within their AWS environment, to include permissions, logging, trust relationships, encryption enforcement, mandating approved machine images and more.

SbD helps customers build their AWS environment for security by suggesting a four-phase approach.

- **Phase 1** – Understand your security requirements
- **Phase 2** – Build your "secure environment" based on a pre-packaged security template
- **Phase 3** – Enforce the use of your template with Service Catalog
- **Phase 4** – Perform validation activities

The first phase entails understanding your requirements. This means outlining your policies, documenting what controls you inherit from AWS, and documenting the controls you own and operate. Once you have established your policies and controls, the last step of phase 1 is to decide what rules you want to enforce in your AWS IT environment.

Phase 2 involves building an environment that fits your security requirements and needs. After defining the security configuration you need, you can find a pre-packaged security template (in the form of AWS CloudFormation Templates) that matches your needs and provides a more comprehensive rule set that can be systematically enforced.

The third phase involves the enabling of AWS Service Catalog to enforce the use of your template from phase 2 in the catalog. This step enforces the use of the security rules set up by the template used in phase 2 and prevents anyone from creating an

environment that doesn't adhere to your security rules. This effectively operationalizes the remaining customer account security configurations of controls in preparation for audit readiness.

Finally, phase 4 is the performance of validation activities. You create your products by importing AWS CloudFormation templates. These templates define the AWS resources required for the product, the relationships between resources, and the parameters that the end user can plug in when they launch the product to configure security groups, create key pairs, and perform other customizations. Then, the rules defined in your template can be used as an audit guide. AWS Config allows you to capture the current state of any of your environments, which can be compared with your environment security rules, enabling audit evidence gathering.

Splunk is an SbD program partner. As an SbD Partner, Splunk can help you use the data generated by AWS Config to help enforce controls and identify potential security and control vulnerabilities. Additionally, Splunk can help identify errors in security templates when validating your security design and rules. When used together with AWS Service Catalog and AWS CloudFormation templates, Splunk can help create an audit-ready environment.

Gaining Visibility into Your AWS Environment with Splunk

It is difficult to detect and mitigate threats and vulnerabilities that you can't see. Services such as AWS Config, AWS CloudTrail, Amazon Inspector, Amazon CloudWatch, and Amazon Kinesis Data Firehose provide critical data, however they don't offer tools to cross-correlate and analyze it to gain insights into potential attack vectors. It is, however, still your responsibility to hold up your end of the AWS Shared Responsibility Model, so your organization will need to find a way to gain visibility from the data provided.

Splunk enhances the security of your data on AWS with end-to-end visibility. The Splunk App for AWS can be easily integrated with AWS Config, AWS CloudTrail, Amazon Inspector, Amazon CloudWatch, Amazon Kinesis Data Firehose, Amazon GuardDuty, and other AWS services to collect and index machine-generated data and deliver real-time security visibility, threat detection, and operational efficiency.

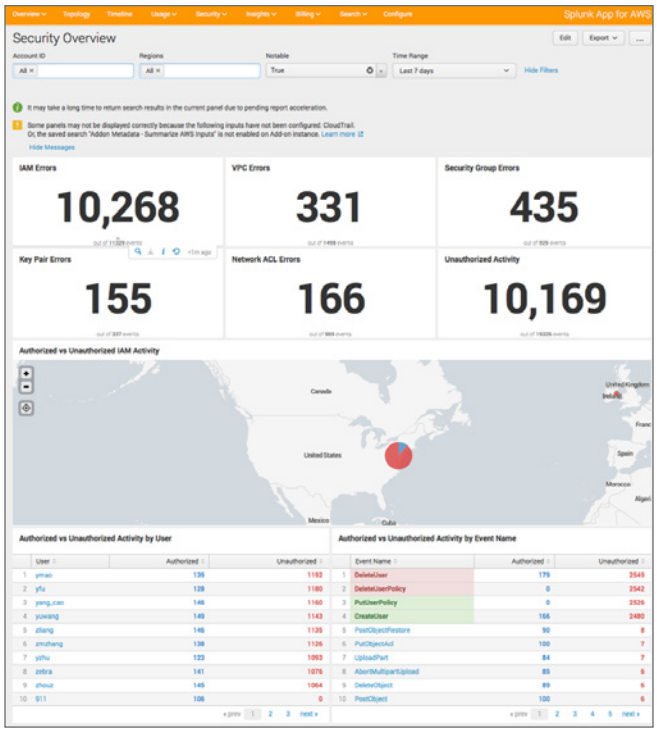

Figure 2.

What Exactly Can You See with Splunk?

The Splunk App for AWS makes it easy to configure data inputs from AWS Config, AWS CloudTrail, Amazon Inspector, Amazon CloudWatch, Amazon VPC Flow Logs, AWS Billing and Cost Management, Amazon S3 and more. The app takes the data from these inputs to create a pre-built knowledgebase of dashboards, reports and alerts that deliver real-time visibility into your environment (figure 2). For example, the Splunk App for AWS provides instant visibility into user administrative actions in your AWS environment, helping you with security and compliance.

Through its consumption of data from AWS CloudTrail, the Splunk App for AWS is able to offer reports analyzing activity in detail, enabling you to instantly gain critical visibility into AWS administration and account activity, including detailed insights into unauthorized access attempts, simultaneous logins from disparate locations, and changes made to access control privileges. Additionally, the Splunk App for AWS monitors all user activity so that you can see who creates, updates, or deletes something within your AWS workload, and it keeps track of who did what and when the event occurred.

The Splunk App for AWS can also show you correlations between AWS CloudTrail and AWS Config data. These correlations allow you to identify trends in existing and deleted AWS resources and changes in AWS Config rules, as well as obtain security analysis that identifies potential issues.

The monitoring function of the Splunk App for AWS also lets customers track inbound and outbound traffic to and from your VPCs and gain insights into network anomalies including rejected network traffic, IP addresses and ports (figure 3).

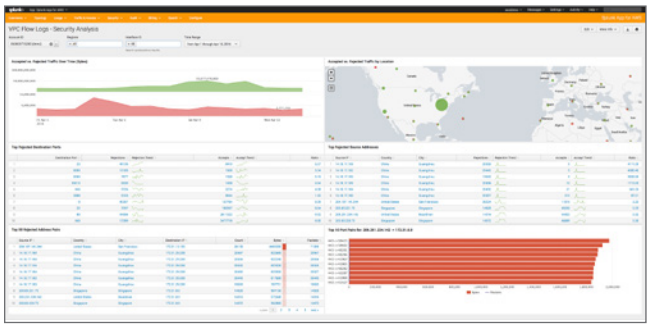

Figure 3.

This, in turn, allows you to use logging and monitoring to track group traffic patterns and network access control that may indicate malicious activity. The Splunk App for AWS also allows customers to monitor the use of cryptographic keys. By doing so, the Splunk App for AWS is able to provide customers with information to help them identify keys that could potentially be compromised.

All of the above, plus the comprehensive analysis of your AWS generated machine data by Splunk allows for greater visibility into your IT environment's potential risk. The reports and dashboards provided by Splunk can help you obtain a better understanding of your risk profile. This expanded knowledge allows you to take action to mitigate the risk identified.

To gain visibility into your automated security vulnerability assessments at scale, the Splunk App can integrate data from Amazon Inspector, making it easier to conduct security tests throughout the development and deployment lifecycle. The Splunk App for AWS gives you a way to consume security data at scale, aggregating Amazon Inspector findings together with insights from AWS CloudTrail and AWS Config to capture a holistic view of vulnerabilities or misconfigurations throughout an organization and react quickly where needed (figure 4).

Another key area that Splunk provides visibility is in data security compliance. Through Splunk's integration with AWS Config and AWS CloudTrail, it is easy to prepare for security audits. Splunk correlates the data from those two sources to help you ensure your organization is adhering to security and compliance standards. The Splunk App accomplishes this by providing a complete audit trail.

Detecting and visualizing threats and associated context, as provided by Amazon GuardDuty, is made straightforward by collecting Amazon GuardDuty events into Splunk via either the Amazon GuardDuty Add-On for Splunk, or via Amazon Kinesis Data Firehose. Custom dashboards can easily support any new or existing workflow associated with triage and investigation of cloud-based threats.

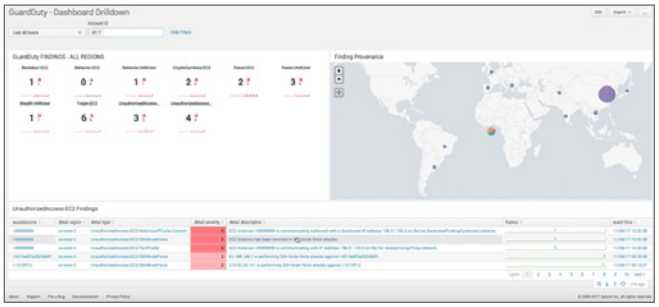

Figure 4.

Overall, AWS provides a secure IT environment and a variety of tools to help keep your data within the cloud secure. Splunk can help you enhance that security by helping your organization gain critical end-to-end visibility and centralized analysis of security events and threat activity across AWS. Through the Splunk App for AWS, you can mitigate security risks stemming from unauthorized access attempts, simultaneous logins from disparate locations, and changes from access control privileges. The App also helps ensure adherence to security and compliance standards, accelerates AWS deployments and helps detect and analyze fraud.

About AWS

For over 12 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 125 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 55 Availability Zones (AZs) within 18 geographic regions and one Local Region around the world, spanning the U.S., Australia, Brazil, Canada, China, France, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. AWS services are trusted by millions of active customers around the world—including the fastest-growing startups, largest enterprises, and leading government agencies—to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit **https://aws.amazon.com**.

About Splunk

Splunk Inc. (NASDAQ: SPLK) turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to discover their "aha" moments with machine data and solve their toughest IT, Internet of Things and security challenges. Use Splunk software in the cloud and on-premises to improve service levels, reduce operations costs, mitigate security risks, enable compliance, enhance DevOps collaboration and create new product and service offerings. Join millions of passionate users by trying Splunk software for free: **www.splunk.com/free-trials**.

Ready to gain end-to-end visibility into your AWS environment? The Splunk App for AWS is available for **free on Splunkbase**.

aws | splunk>

www.splunk.com

WP-Splunk-EnhanceSecurity-AWS-Cobranded-105