WHITE PAPER

ENHANCE AWS SECURITY WITH SPLUNK® SOLUTIONS

An AWS and Splunk White Paper

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.

According to IDC, security is still a top concern for enterprises that are deciding whether or not to move to the cloud. In fact, in the IDC whitepaper, "Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment*," they cite a recent CloudView Survey, stating that organizations named security concerns as, "the number 1 inhibitor regarding the adoption of cloud technologies and services." In that survey, nearly 50% of responding organizations identified security as a concern, while reliability and compliance garnered 33% and 30% (respectively) of respondents identifying them as concerns.

The IDC, "Security Solutions: Security in the Cloud**," goes on to say that the truth is your organization's workloads can be more secure on the Amazon Web Services (AWS) Cloud. AWS provides a robust infrastructure and a world-class team of security experts that are monitoring AWS systems 24 hours per day, 7 days per week to protect its infrastructure around the globe. Building on this solid foundation of infrastructure security, with Splunk, an AWS Partner Network (APN) Security Competency Partner, you can enhance your level of data security through end-to-end visibility and achieve security standards on the cloud that would be difficult and cost prohibitive to achieve in an on-premises environment.

Understanding Cloud Security Models

Many individuals have the misconception that the cloud is not secure, primarily based on hearing occasional news quips and an incomplete understanding of the cloud. Additionally, there is a perception that moving to shared resources and using more externalized management means an increase in security risk.

However, the concept that risk inherently increases described in the aforementioned situation doesn't accurately portray the complete cloud security story. Most of the concern over the security of the cloud came to be when Infrastructure-as-a-Service (IaaS) was in its infancy. As enterprises started considering IaaS as an option, the viability of these new IT architectures had to be considered from a security point-of-view.

When examining security, it's important to look at it from within the context of risk management. That is, to what extent a given security system mitigates risk. From a risk management perspective, risk is a function of probability (the likelihood that a negative outcome occurs) and magnitude (the severity of the impact of the negative outcome). Unlike on-premises datacenters, the AWS Cloud is designed to be resilient to server failure, data corruption or even natural disasters. With this in mind, a technology risk manager must assess this risk in the context of the main factors that affect the risk of a breach: threat and vulnerabilities (increases risk) and controls (mitigates risk).

The area with the largest differences between on-premises and cloud datacenters is controls. The previously mentioned IDC whitepaper states that since on-premises datacenters already have established sets of controls in place, it can be difficult for organizations to compare different deployment models within them. Cloud architectures, on the other hand, provide great opportunity to "rethink, renew, and reinforce controls that are more likely to match the highly distributed, loosely coupled, component-oriented application architectures being developed today." In other words, much of the modern IT world is designed for flexibility. A lot of modern applications are designed to be rapidly launched and scaled, removing much of the time-consuming installation and integration process commonly found in older applications. This means they can be quickly integrated and used with little to no delay—and that you need an equally flexible security solution, like the one available from Splunk, that is capable of seamlessly scaling to protect these new applications as they are added to the cloud.

To meet these needs, Splunk has closely aligned with AWS to deliver solutions that offer real-time visibility into your cloud applications, infrastructure and AWS account. With solutions from Splunk, you can monitor your AWS deployments as well as deploy Splunk software as an AWS-based cloud service. Legacy security systems struggle to meet the need for flexibility and the task of setting them up to cover new applications is often time consuming and expensive, slowing down innovation. The nature of the cloud allows it to rapidly adapt to meet this level of necessary elasticity and innovation.

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 datacenter. To achieve the level of versatility required by modern application architectures, customers can leverage capabilities from Splunk and AWS. By doing so, you can gain greater security capabilities spanning segmentation, encryption, authentication, and logging and monitoring when compared to legacy architectures.

The necessary level of segmentation can be achieved with Amazon Virtual Private Cloud (Amazon VPC). Amazon VPCs are logically isolated sections of the AWS Cloud 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 datacenter.

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 you solve this 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 data uploaded to the AWS Cloud 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 (Amason 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.

Logging and Monitoring

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, and Amazon CloudWatch—and Splunk can draw from 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.

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.

Working with the AWS Shared Responsibility Model

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, you are responsible for the security of your workloads on the cloud. This means that AWS takes responsibility for securing the network and physical infrastructure of the cloud, but you are responsible for securing your application data and virtual environment that resides on it. Splunk solutions can help you meet your security responsibilities on the AWS Cloud.

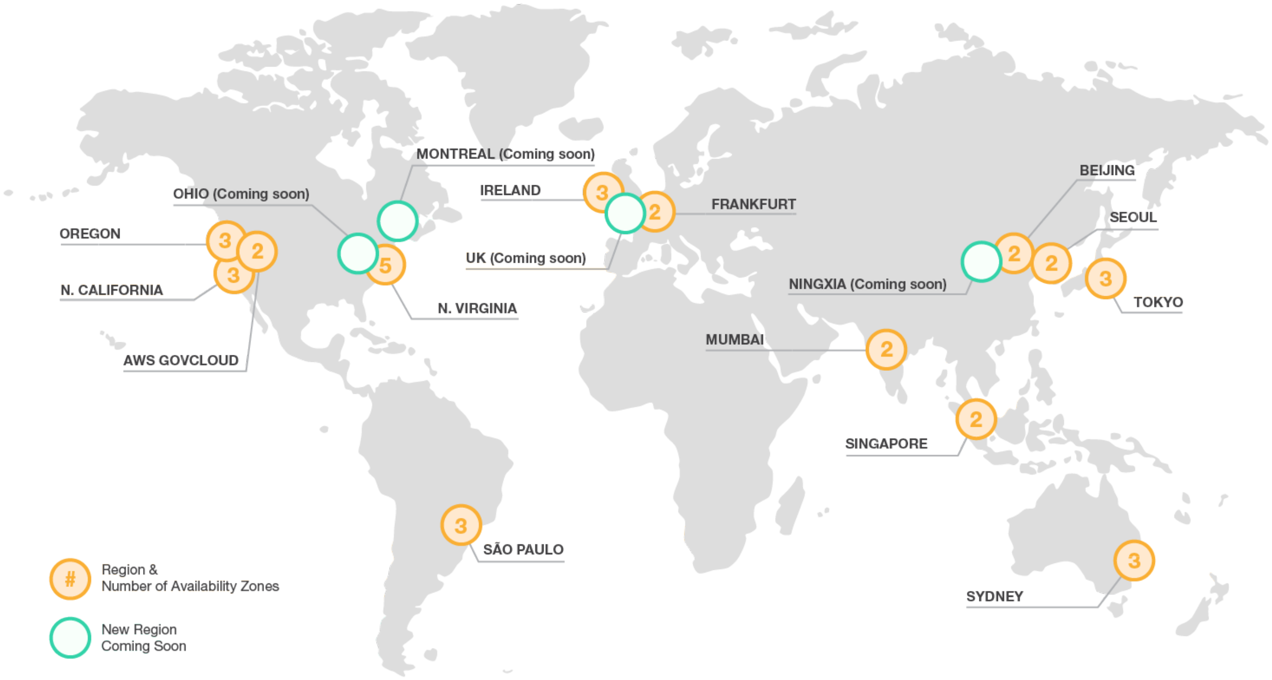


Figure 1

As of July 2016, AWS's global infrastructure footprint consists of 13 Regions and 35 Availibility Zones (AZs) with 4 more Regions and 9 more AZs coming online by Spring 2017 (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 Cloud Security doesn't just include geographic dispersion. Within each datacenter in each region, 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.

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.

It is important for organizations to make security one of their first considerations when building any IT environment, and the cloud is no different. Organizations need to make sure their environments maintain compliance and match the needs of modern applications. Maintaining adequate controls to protect environments from any threats and mitigating any vulnerabilities is also of utmost importance.

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, you are responsible for securing the following on your 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 you architect 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.

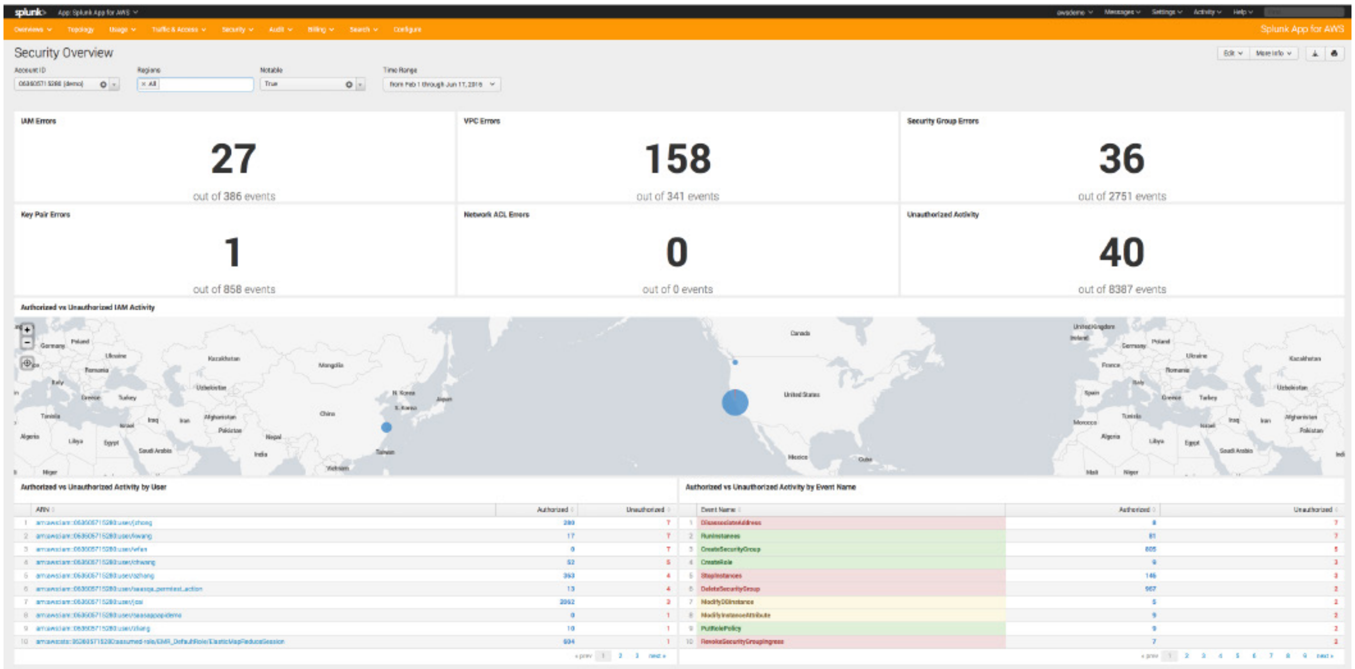
Finally, phase 4 is the performance of validation activities. You create your products by importing AWS CloudFormation templates. These templates define the AWS resources required for the product, the relationships between resources, and the parameters that the end user can plug in when they launch the 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 Infrastructure 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, and Amazon CloudWatch 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 is a leader in enterprise security and 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, and other AWS services to collect and index machine-generated data and deliver real-time security visibility.



Security Overview

Account ID: 063605715280 (demo) | Regions: × All | Notable: True | Time Range: from Feb 1 through Jun 17, 2016

IAM Errors: 27 out of 386 events

VPC Errors: 158 out of 341 events

Security Group Errors: 36 out of 2751 events

Key Pair Errors: 1 out of 858 events

Network ACL Errors: 0 out of 0 events

Unauthorized Activity: 40 out of 8387 events

Authorized vs Unauthorized IAM Activity

Authorized vs Unauthorized Activity by User

	ARN	Authorized	Unauthorized
1	arn:aws:iam::063605715280:user/jzhong	280	7
2	arn:aws:iam::063605715280:user/lwang	17	7
3	arn:aws:iam::063605715280:user/wfan	0	7
4	arn:aws:iam::063605715280:user/chwang	52	5
5	arn:aws:iam::063605715280:user/szhang	363	4
6	arn:aws:iam::063605715280:user/saasqa_permtest_action	13	4
7	arn:aws:iam::063605715280:user/jcai	2062	3
8	arn:aws:iam::063605715280:user/saasappqapidemo	0	1
9	arn:aws:iam::063605715280:user/zliang	10	1
10	arn:aws:sts::063605715280:assumed-role/EMR_DefaultRole/ElasticMapReduceSession	604	1

« prev 1 2 3 next »

Authorized vs Unauthorized Activity by Event Name

	Event Name	Authorized	Unauthorized
1	DisassociateAddress	8	7
2	RunInstances	81	7
3	CreateSecurityGroup	805	5
4	CreateRole	9	3
5	StopInstances	146	3
6	DeleteSecurityGroup	967	2
7	ModifyDBInstance	5	2
8	ModifyInstanceAttribute	9	2
9	PutRolePolicy	9	2
10	RevokeSecurityGroupIngress	7	2

« prev 1 2 3 4 5 6 7 8 9 next »

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).

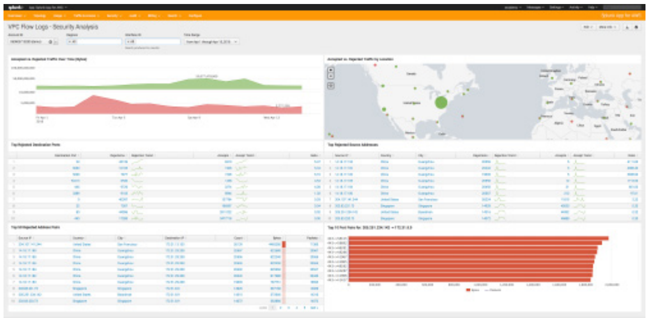
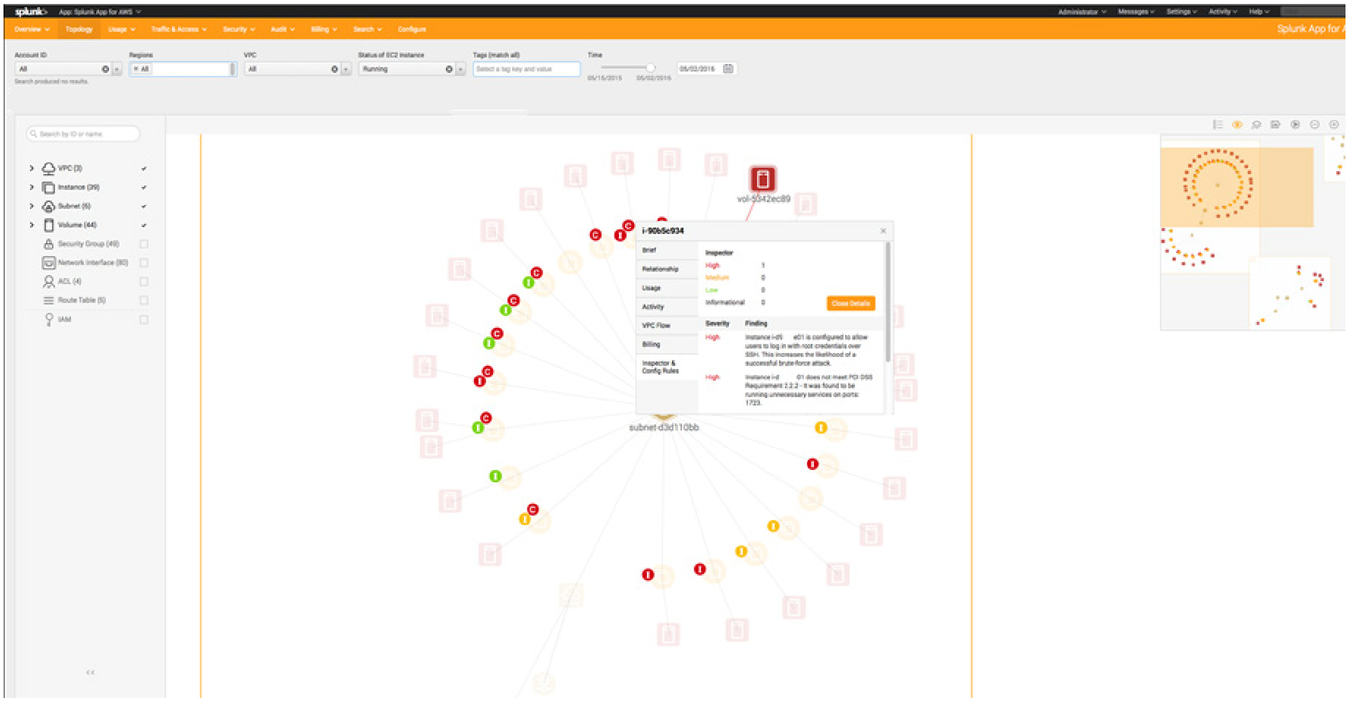


Figure 3

This, in turn, allows you to use logging and monitoring to track group traffic patterns and network access control that may indicate malicious



Inspector

High	1
Medium	0
Low	0
Informational	0

Severity	Finding
High	Instance i-d9 e01 is configured to allow users to log in with root credentials over SSH. This increases the likelihood of a successful brute-force attack.
High	Instance i-d 01 does not meet PCI DSS Requirement 2.2.2 - It was found to be running unnecessary services on ports: 1723.

Figure 4

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.

Overall, AWS provides a secure cloud 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 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 prevent fraud.

AWS Services	Benefit Added by Using Splunk Solutions	
AWS CloudTrail	Monitor all user activity in your AWS account	Help ensure security and compliance
AWS Config Rules	Monitor all resource activity in your AWS account	Visualize and interact with your AWS Topology
Amazon Inspector	Analyze findings from automated security assessment	Integrated with CloudTrail and Config
Amazon CloudWatch	Visualize and analyze CloudWatch metrics and VPC Flow Logs	Monitor IP traffic to and from VPC network interfaces for anomalies and patterns that may indicate malicious activity
Amazon VPC Flow Logs	Capture information about the IP traffic going to and from the network interfaces in your VPC	Troubleshoot why specific traffic is not reaching an instance, help diagnose overly restrictive security group rules, and monitor the traffic that is reaching your instance

Getting Started with Splunk on AWS

Splunk can help you enhance your overall AWS security posture. Click here to sign up for a free trial.

Learn more about Splunk solutions for AWS.

Citation

*Lindstrom, Pete. "Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment." *An IDC White Paper sponsored by Amazon Web Services*, July 2015, www.aws.amazon.com/security/safer-in-the-cloud-download-report/.

**Richmond, Christina. "Security Solutions: Security in the Cloud." *IDC,* 2016, https://www.idc.com/getdoc.jsp?containerId=IDC_P31286.

About AWS:

For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 70 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 35 Availability Zones (AZs) across 13 geographic regions in the U.S., Australia, Brazil, China, Germany, Ireland, Japan, Korea, Singapore, and India. AWS services are trusted by more than a million 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 http://aws.amazon.com.

About Splunk

Splunk Inc. provides the leading software platform for real-time Operational Intelligence. Splunk software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. More than 12,000 enterprises, government agencies, universities and service providers in over 110 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce costs. Splunk products include Splunk® Enterprise, Splunk Cloud™, Splunk Light and premium solutions. To learn more, please visit: http://www.splunk.com/company.

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

sales@splunk.com www.splunk.com