netskope

WHITEPAPER

Securing your Amazon Web Services with Netskope

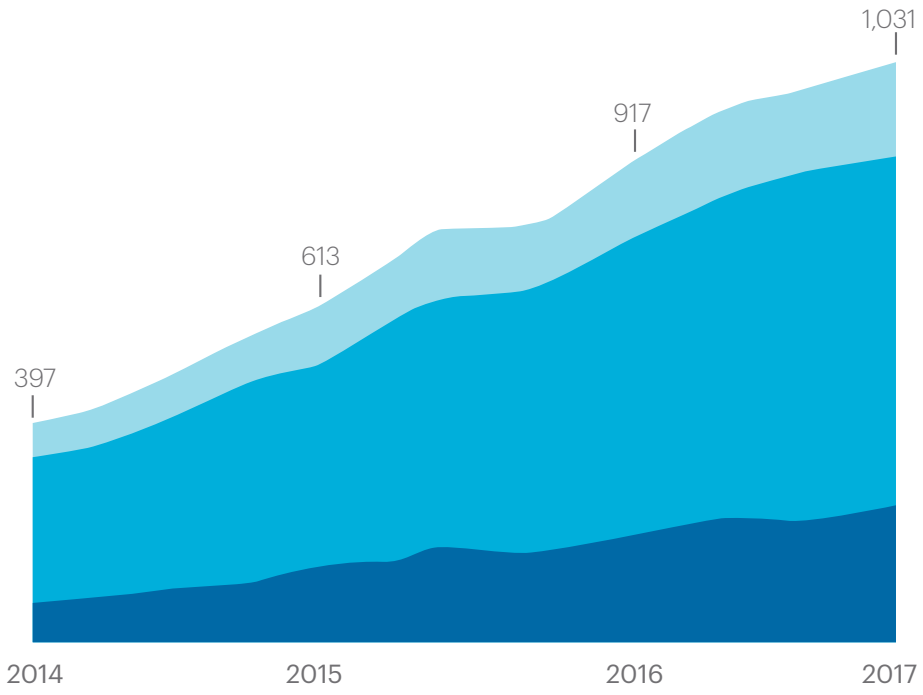
INTRODUCTION

In this whitepaper, read about security challenges organizations face as they move their workloads to Amazon Web Services (AWS), three key capabilities to consider that can improve the security of workloads, and how to establish these capabilities with Netskope.

AWS SECURITY CHALLENGES

The average number of cloud services organizations consume is growing, and the use of infrastructure-as-a-service (IaaS) is a large part of this growth. See Figure 1 for the latest on cloud usage growth based on Netskope research findings. A significant number of organizations are in the midst of migrating most of their applications and workloads to cloud infrastructure or IaaS primarily using three platforms. More than 90% of Netskope customers use IaaS services like AWS, Microsoft Azure, and Google Cloud Platform, and use is increasing.[1] AWS is consistently a leading choice for enterprises. As more organizations move to AWS, they are not willing to compromise on security. Poor cloud security practices have lead to the most recent AWS data exposures. A recent Verizon data breach exposed millions of customer records accessed through an unprotected Amazon S3 storage server.[2]

FIGURE 1 | Average number of cloud services in use, Netskope Cloud Report 2014-2017



[1]https://resources.netskope.com/i/771630-january-2017-worldwide-cloud-report/4?
[2]http://money.cnn.com/2017/07/12/technology/verizon-data-leaked-online/index.html

Even though security is a top priority, many organizations across many industries have not done the heavy lifting to implement cloud security policies and controls that align with their evolving business, security and compliance requirements. In some cases the IaaS platform has been procured and implemented outside the control of IT. In addition, in many instances, users and administrators have made false assumptions about the out-of-the-box security capabilities of IaaS platforms. When evaluating the security of a cloud service, security teams also need to understand their part in the shared responsibility security model. While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems, and networks, no differently than they would for applications in an on-site data center.[3]

What's important in your cloud security agenda right now? What are some characteristics of a security strategy to protect your IaaS environment, and AWS specifically?

- Do you have multiple AWS accounts? How do you manage access to your AWS accounts and mark them as sanctioned vs. unsanctioned?
- What tools do you use to monitor your Identity and Access Management (IAM) configuration policies?
- Can you track the activities of your admins to catch rogue events?
- Does the data in your S3 bucket contain confidential information? Are you making sure confidential information is being properly secured?
- How do you detect malware in your S3 bucket?

ADDITIONAL CONTROLS NEEDED TO SECURE YOUR AWS ENVIRONMENT AND HOW NETSKOPE CAN HELP

Security capabilities needed to increase an organization's security posture within AWS environments include:

- Adaptive access control
- Network configuration and compliance assessment
- Data security

ADAPTIVE ACCESS CONTROL

Access control concerns have a lot to do with ensuring only the right people can access or change resources. In many cases customers are concerned who can stop, start or create new EC2 instances in their AWS environment. Organizations need to enable safe and secure access for users. They need visibility and control across the AWS environment, to govern users with access control, and to prevent risky activities.

[3]https://aws.amazon.com/compliance/shared-responsibility-model/

STEP #1: IMPLEMENT ADAPTIVE ACCESS CONTROL WITH NETSKOPE

- Control access for sanctioned corporate accounts while blocking unsanctioned or personal accounts with access control policies
- Allow AWS Identify Access Management (IAM) access from only managed corporate devices but block access from unmanaged devices like a home PC
- Detect when two separate users log in using the same userID with Netskope's built-in anomaly detection
- View and control IAM activities (like edit, create, delete)
- Enforce restrictions on root user
- Prevent users from deleting S3 buckets or EC2 instances

NETWORK CONFIGURATION AND COMPLIANCE ASSESSMENT

In heavily regulated industries, organizations are concerned with complying with regulations and relevant laws and ensuring there is an audit trail to go along with it. For example, they may need to maintain a detailed audit trail of all admin activity across multiple instances of AWS being used by different lines of business, or monitor and track all activities and changes to resources for compliance reporting.

STEP #2: ENABLE COMPLIANCE ASSESSMENT WITH NETSKOPE

- Through the AWS CloudTrail service, Netskope provides the granular visibility into AWS audit logs for reporting and forensics. Admins can query and look at events specific to all AWS instances through an easy to digest readable format of event logs, highlighting User, App, and Activity
- Create reports on root user activity across all instances in your environment
- Investigate audit trails for non-compliant activities and run real-time reports to monitor network configuration changes to S3, EC2, and other services. Get a complete audit trail of IAM, EC2, and S3 and ELB, Route53, Lambda
- Monitor roles, permissions and policy changes in IAM
- Monitor for the creation of new user and groups and whether best practices are being followed like enabling Multi-factor Authentication (MFA)

DATA SECURITY

It isn't only SaaS services that hold sensitive information. IaaS provides a richer environment for data exfiltration and malware. Understand your exposure, then mitigate the risk. Your security program should address your cloud data loss prevention requirements.

STEP #3: ENFORCE DATA LOSS PREVENTION WITH NETSKOPE

- Scan the data in your S3 bucket for confidential information like PII, PCI, or PHI data that should not be there
- Scan a file (in real-time) being uploaded to an S3 bucket containing malware
- Build custom DLP profiles and apply policies to real-time activities, such as uploads to and downloads from S3 and data at rest already residing in S3. Select S3 buckets in any region and have those files scanned for DLP violations
- When a policy violation occurs, coach the user, notify the admin, or block a subset of users from downloading or uploading sensitive files stored in S3

This is only a start. There are additional security concerns and controls that organizations need to consider when implementing IaaS. Learn more about Netskope for AWS at https://www.netskope.com/platform/netskope-for-aws/

Netskope is the leader in cloud security. Using patented technology, Netskope's cloud-scale security platform provides context-aware governance of all cloud usage in the enterprise in real-time, whether accessed from the corporate network, remote, or from a mobile device. This means that security professionals can understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work today. With granular security policies, the most advanced cloud DLP, and unmatched breadth of workflows, Netskope is trusted by the largest companies in the world. Netskope — security evolved.

To learn more visit, https://www.netskope.com.