netskope

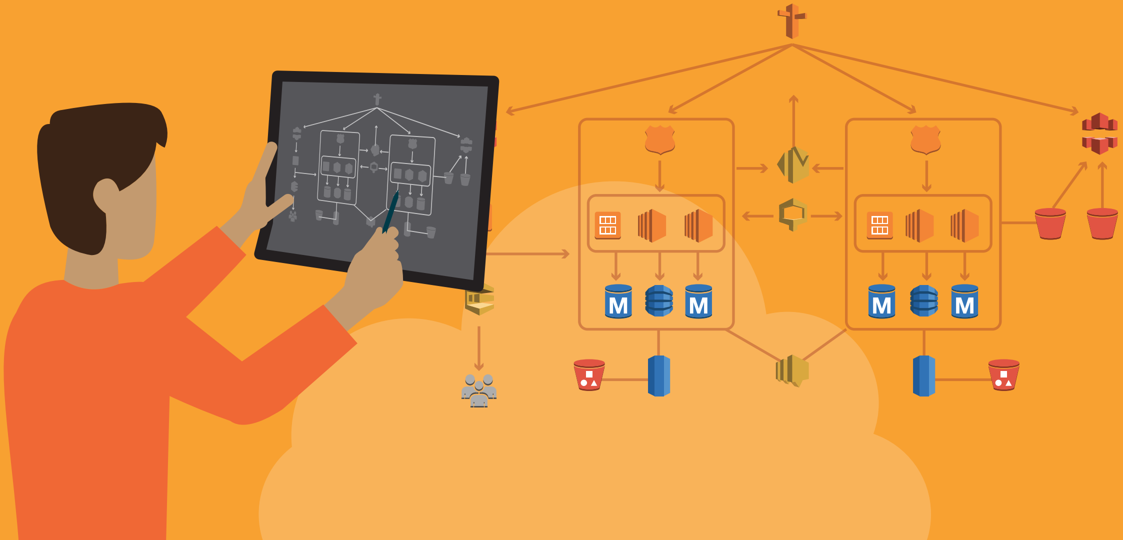
5 Steps to Boost Your Security Posture on Amazon Web Services

How to deliver AWS security that guards data everywhere and stops elusive attacks

This eBook contains 5 steps you can follow to boost your AWS security posture and shows how Netskope can help you implement them.

Step 1:
Get an understanding of your risk posture

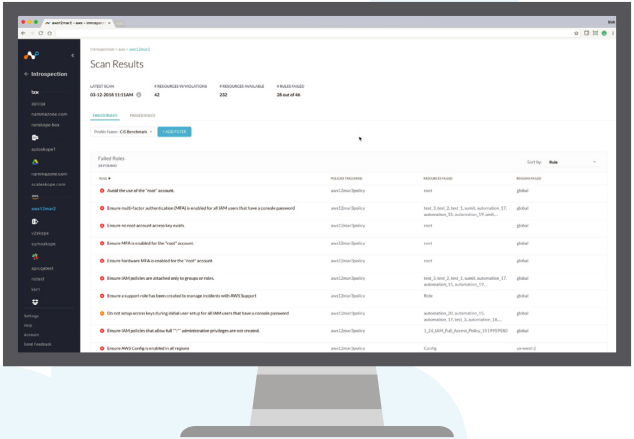
You need a snapshot of where you stand with regards to sensitive data in AWS S3 and misconfigurations in AWS that can leave you vulnerable to attacks.



Get an understanding of your risk posture

With Netskope, you can:

Get an ongoing assessment that helps you identify and remediate compliance and security risks within your AWS environment. Find unauthorized use of AWS and stop unauthorized accounts from access.Follow cloud-specific security and compliance frameworks to inform your security posture. You can start with the CIS AWS Foundations Benchmark, which provides a framework for AWS security best practices. For organizations doing business with the federal government, Netskope incorporates the NIST Cybersecurity Framework. There are different compliance guidelines for payments and many other that can be the foundation you measure against. This will help guide how you secure your configurations.



Introspection > aws > aws12mar2

Scan Results

LATEST SCAN	# RESOURCES W/VIOLATIONS	# RESOURCES AVAILABLE	# RULES FAILED
03-12-2018 11:11AM	42	232	28 out of 46

Profile Name: CIS Benchmark

Failed Rules
28 FOUND

Sort by: Rule

RULE	POLICIES TRIGGERED	RESOURCES FAILED	REGIONS FAILED
Avoid the use of the "root" account.	aws12mar3policy	root	global
Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	aws12mar3policy	test_3, test_2, test_1, sumit, automation_17, automation_15, automation_19, amit,...	global
Ensure no root account access key exists.	aws12mar3policy	root	global
Ensure MFA is enabled for the "root" account.	aws12mar3policy	root	global
Ensure hardware MFA is enabled for the "root" account.	aws12mar3policy	root	global
Ensure IAM policies are attached only to groups or roles.	aws12mar3policy	test_3, test_2, test_1, sumit, automation_17, automation_15, automation_19,...	global
Ensure a support role has been created to manage incidents with AWS Support	aws12mar3policy	Role	global
Do not setup access keys during initial user setup for all IAM users that have a console password	aws12mar3policy	automation_20, automation_15, automation_17, test_3, automation_18,...	global
Ensure IAM policies that allow full "*:*" administrative privileges are not created.	aws12mar3policy	1_24_IAM_Full_Access_Policy_1519959580	global
Ensure AWS Config is enabled in all regions	aws12mar3policy	Config	us-west-2

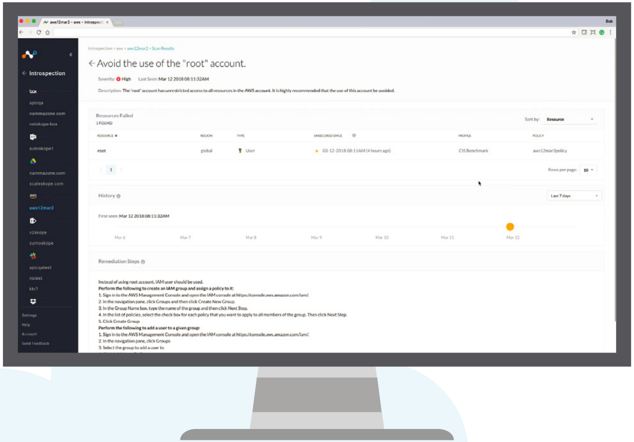
Step 2:
Protect data in S3 buckets

Many breaches have been caused by poorly configured S3 buckets that grant improper access to sensitive data like PII. A good best practice is to review any bucket with permissions granted to "Everyone," especially when sensitive data is involved.

Protect data in S3 buckets

With Netskope, you can:

View a report at any time showing S3 exposure against identified benchmarks and best practices, with recommendations on necessary remediation steps. Scan your S3 buckets for sensitive content and apply cloud DLP policies to prevent unauthorized activity. When a policy violation occurs, coach the application owner, notify the security admin or block certain users from downloading or uploading sensitive files stored in S3 based on location and device used.



Avoid the use of the "root" account.

Severity: High   Last Seen: Mar 12 2018 08:11:32AM

Description: The 'root' account has unrestricted access to all resources in the AWS account. It is highly recommended that the use of this account be avoided.

Resources Failed
1 FOUND

Sort by: Resource

RESOURCE	REGION	TYPE	UNSECURED SINCE	PROFILE	POLICY
root	global	User	03-12-2018 08:11AM (4 hours ago)	CIS Benchmark	aws12mar3policy

Rows per page: 10

History

Last 7 days

First seen: Mar 12 2018 08:11:32AM

Remediation Steps

Instead of using root account, IAM user should be used.

Perform the following to create an IAM group and assign a policy to it:

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, click Groups and then click Create New Group.
3. In the Group Name box, type the name of the group and then click Next Step.
4. In the list of policies, select the check box for each policy that you want to apply to all members of the group. Then click Next Step.
5. Click Create Group

Perform the following to add a user to a given group:

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, click Groups
3. Select the group to add a user to

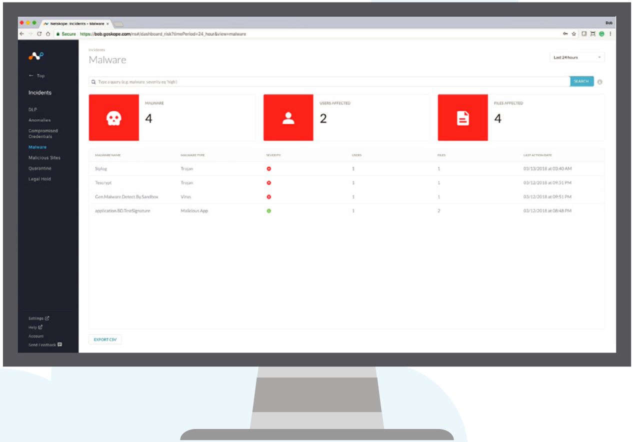
Step 3:
Scan S3 buckets for malware

Protecting the enterprise from cloud-based malware involves gaining visibility into all cloud traffic. Perhaps you can see across your SaaS applications, but cybercriminals can reach far beyond to IaaS applications as well. If your S3 bucket contains files coming in from public sources you are most susceptible to being exposed to malware. Even internal files being stored on S3 may have ransomware or botnets attached. Remember, the Shared Responsibility Model means protection of the data is a customer's responsibility, and this includes protection against malware.

Scan S3 buckets for malware

With Netskope, you can:

Get multi-layered threat protection in your IaaS environment that traditional malware scanning tools do not cover. Netskope uses multiple real-time and deep detection engines to protect against malware en route to and from your IaaS environment. You can scan traffic coming from rogue/unsanctioned accounts and block this activity. This protection extends not only to your corporate managed devices but also to unmanaged devices that may be used to access your IaaS environment.



Malware

MALWARE 4

USERS AFFECTED 2

FILES AFFECTED 4

MALWARE NAME	MALWARE TYPE	SEVERITY	USERS	FILES	LAST ACTION DATE
Siplog	Trojan	🟥	1	1	03/13/2018 at 03:40 AM
Tescrypt	Trojan	🟥	1	1	03/12/2018 at 09:51 PM
Gen.Malware.Detect.By.Sandbox	Virus	🟥	1	1	03/12/2018 at 09:51 PM
application.BD.TestSignature	Malicious App	🟩	1	2	03/12/2018 at 08:48 PM

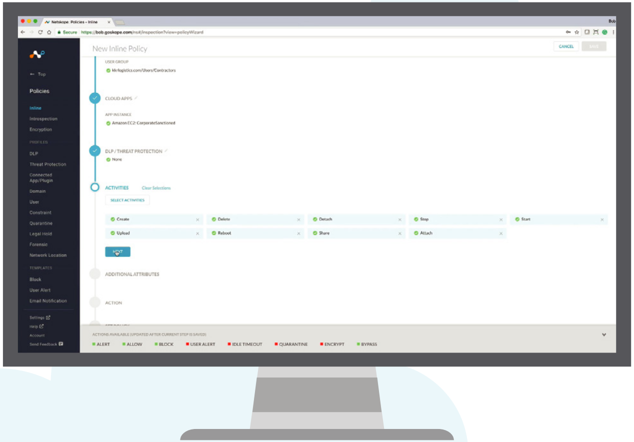
Step 4:
Provide real-time visibility and control of access to AWS Management Console

Users logging into the management console can have unfettered access to functions such as create, delete, start, and stop across AWS instances. This presents an opportunity to do major damage that you can equate to "taking down a data center." You need the ability to achieve real-time visibility and control of activities tied to AWS instances.

Provide real-time visibility and control

With Netskope, you can:

Get real-time visibility of activities taking places against AWS instances and put real-time policy controls in place to block certain activities or restrict based on user, group, or OU. Since Netskope is continuously assessing your AWS environment, you can even see instances that may only be set up temporarily to perform a discrete activity.



New Inline Policy

USER GROUP
kkrlogistics.com/Users/Contractors

CLOUD APPS

APP INSTANCE
Amazon EC2: CorporateSanctioned

DLP / THREAT PROTECTION
None

ACTIVITIES
Create, Delete, Detach, Stop, Start, Upload, Reboot, Share, Attach

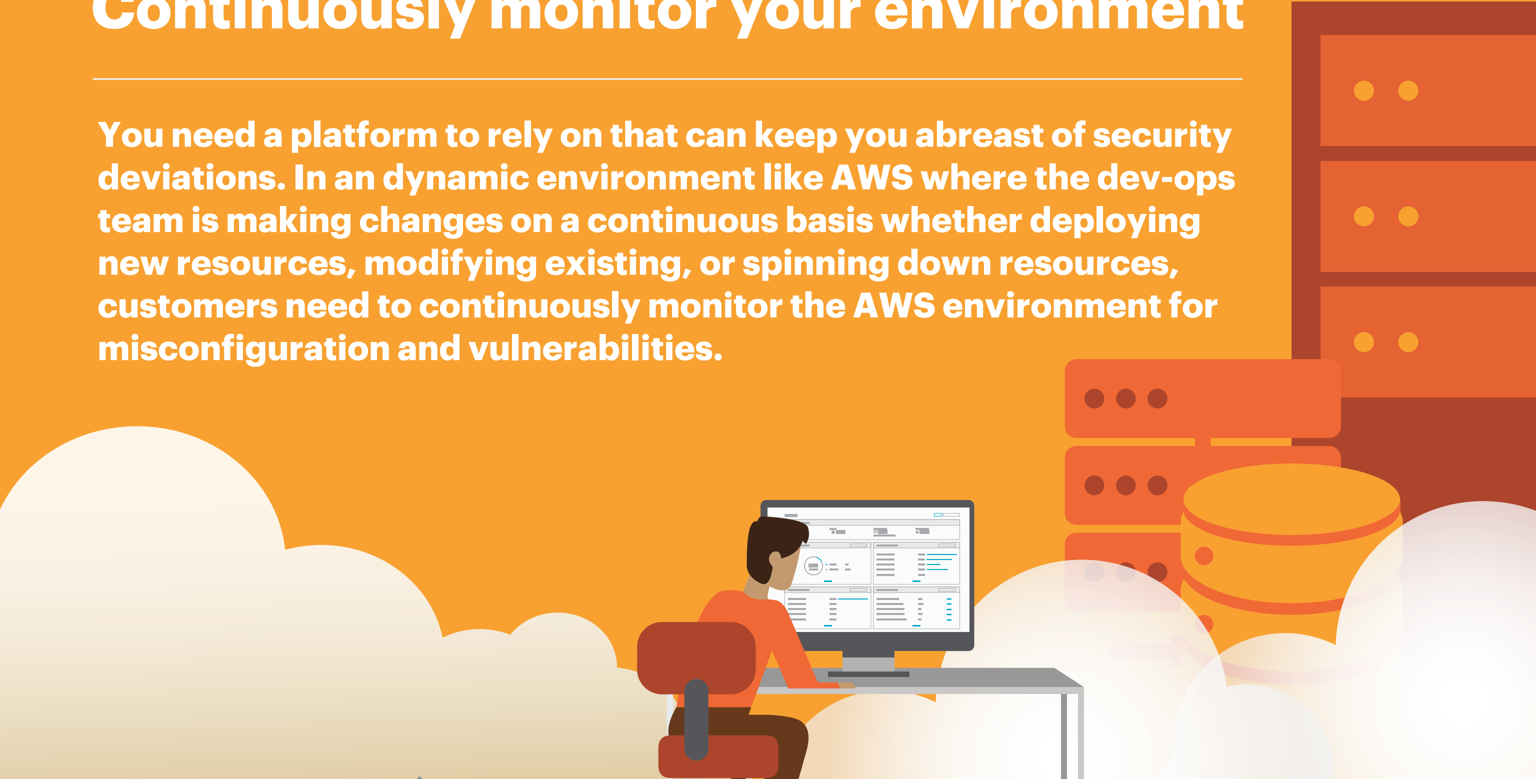
ADDITIONAL ATTRIBUTES

ACTION

ACTIONS AVAILABLE (UPDATED AFTER CURRENT STEP IS SAVED)
🟩 ALERT 🟩 ALLOW 🟩 BLOCK 🟥 USER ALERT 🟥 IDLE TIMEOUT 🟥 QUARANTINE 🟥 ENCRYPT 🟩 BYPASS

Step 5:
Continuously monitor your environment

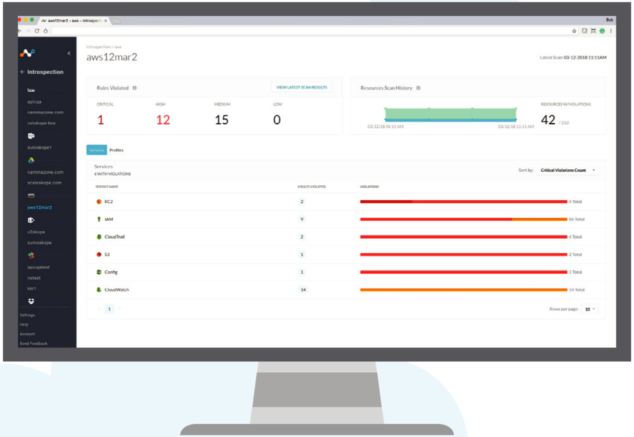
You need a platform to rely on that can keep you abreast of security deviations. In an dynamic environment like AWS where the dev-ops team is making changes on a continuous basis whether deploying new resources, modifying existing, or spinning down resources, customers need to continuously monitor the AWS environment for misconfiguration and vulnerabilities.



Continuously monitor your environment

With Netskope, you can:

Continuously monitor and audit your AWS configuration with Netskope's Continuous Security Assessment. Use the CIS benchmark as a yardstick to make sure you are compliant and to mitigate the risk of misconfiguration. The CIS Benchmark supports many best practices for configuration in your AWS environment such as confirming that two factor auth is enabled, access keys are rotated every 90 days, or least access is enabled for VPCs. If violations are found, these items flagged as Critical, High, Medium, or Low. The admin can find detailed information about each violation and recommended remediation steps.



Introspection > aws

aws12mar2

Latest Scan: 03-12-2018 11:11AM

Rules Violated

CRITICAL	HIGH	MEDIUM	LOW
1	12	15	0

Resources Scan History

RESOURCES W/VIOLATIONS 42 / 232

Services
6 WITH VIOLATIONS

Sort by: Critical Violations Count

SERVICE NAME	# RULES VIOLATED	VIOLATIONS
EC2	2	4 Total
IAM	9	86 Total
CloudTrail	2	4 Total
S3	1	2 Total
Config	1	1 Total
CloudWatch	14	14 Total

1

Rows per page: 10

Secure your AWS workloads today with Netskope

Visit www.netskope.com or call us at 1-800-979-6988 to schedule a demo.

Netskope is the leader in cloud security. We help the world's largest organizations take full advantage of the cloud and web without sacrificing security. Our patented Cloud XD technology eliminates blind spots by going deeper than any other security provider to quickly target and control activities across thousands of cloud services and millions of websites. With full control through one cloud-native interface, our customers benefit from 360-degree data protection that guards data everywhere and advanced threat protection that stops elusive attacks. At Netskope, we call this smart cloud security.

Netskope — smart from the start.

netskope

netskope.com