AT&T Cybersecurity

AT&T Business

Beginner's guide: AWS security monitoring

Introduction

Organizations around the world are embracing the benefits of shifting their workloads, apps, and services to Amazon Web Services (AWS) and other popular cloud infrastructure-as-a-service (IaaS) providers. Gartner predicts that of the global enterprises already using cloud today, over half will have an all-in approach to the cloud by 2021[1].

At the same time, cloud security concerns continue to rise. According to a 2018 Cloud Security Report from Cybersecurity Insiders,[2] 91% of respondents are concerned about cloud security, an increase of 11% over last year's report. While security concerns haven't slowed down the migration of workloads to the cloud, by examining these in detail, we can learn how to avoid making costly mistakes that leave our data exposed.

The truth is the top 3 biggest security concerns are all based on operational error. The bad news is, left exposed, these mistakes provide huge gaps an attacker can walk right through. Because of that, continuous security monitoring of your AWS assets, configuration, and infrastructure is essential. The good news? You can fix these, and we'll tell you how.

1. Cloud Computing Enters its Second Decade https://www.gartner.com/smarterwithgartner/cloud-computing-enters-its-second-decade/
2. 2018 Cloud Security Report

Top 3 AWS security concerns

Platform misconfiguration

Experience is one of the best ways to gain knowledge. As enterprises move their critical workloads into the cloud, many gain experience via a steep learning curve. One that may also result in a few configuration errors along the way. The hope is they realize the error of their ways before an attacker does. In the meantime, security monitoring will catch it in near-real time.

AWS offers a number of security features, from identity and access management (IAM) to security zones to multi-factor authentication to encryption (just to name a few). For a new administrator, it may become a bit overwhelming to get all the details completely right. Some organizations have learned by trial and error, and unfortunately, those errors have included leaving S3 (Simple Storage Service) buckets unsecured, exposing sensitive data to the world wide web. Attackers know that stolen PII (personally identifiable information) is valuable and can be sold on the black market to cyber criminals to be repurposed in identity theft, fraud, and other nefarious ways.

Top 3 AWS security concerns

Unauthorized access

No matter how many security controls you may have in place, once an attacker has a set of authorized credentials, they can do a significant amount of damage under the guise of an authorized user.

Credentials have enormous value—especially privileged ones with root and domain levels of access.

Monitoring privileged access and privilege escalation activity within your AWS workloads is essential. By actively monitoring privileged account access and activities, you'll be able to detect abnormal and suspicious behavior, such as direct and frequent downloads from a database housing customer data.

Top 3 AWS security concerns

Insecure interfaces and APIs

Without APIs (application programming interface), it would be nearly impossible to achieve all the benefits that cloud platforms like AWS offer. By automating and enabling data transfer and use among disparate services, these interfaces unlock enormous scalability and efficiency gains.

At the same time, if APIs are not carefully coded and configured, they pose significant security risks in terms of confidentiality, integrity, availability, and accountability.

Continuous monitoring of your AWS workloads and periodic vulnerability scans of your AWS environment will alert you to critical gaps that need attention.

Getting started with AWS security best practices

AT&T Business

Getting started with AWS security best practices

Understand the shared responsibility model

AWS offers significant advantages for many organizations with its innovative technology model. However, one aspect of this innovation that can present unanticipated challenges is its shared responsibility security model.

As Amazon explains[3], "While AWS manages the security of the cloud, security in the cloud is your customer responsibility, as you retain control of what security you choose to implement to protect your own content, platform, applications, systems and networks – no differently than you would for applications in an on-site data center."

That means if you rely on AWS, you need to regularly evaluate the configuration of your network access and security controls. Otherwise, you could inadvertently deploy insecure configurations, putting your instances and assets at risk.

3. Understanding the ASD's Cloud Computing Security for Tenants in the Context of AWS
Link: https://d1.awsstatic.com/whitepapers/compliance/Understanding_the_ASDs_Cloud_Computing_Security_for_Tenants_in_the_Context_of_AWS.pdf

Getting started with AWS security best practices

Identify the most common cloud configuration errors and make sure to avoid them

To avoid common cloud configuration errors and credential mismanagement, follow these key guidelines:

- **Lock down your root, domain, and administrator-level account credentials.** Treat user accounts, especially privileged ones, like toothbrushes—it's never healthy to share them. In fact, it can be dangerous. In addition, periodically reset passwords for privileged accounts and consider using password managers or other tools to protect these credentials. Another goal of locking down privileged account use is to always follow the principle of least privilege: Only use root or administrator level account access when it's absolutely necessary for the job at hand. That way, any mistakes are much more easily contained.
- **Use IAM roles and temporary credentials.** IAM roles can be used to define permission levels for different resources and applications that run on EC2 (Elastic Compute Cloud) instances. When you launch an EC2 instance, you can assign an IAM role to it, eliminating the need for your applications to use AWS credentials to make API requests. This is one of the best tools when it comes to security in AWS. First of all, IAM roles can be very granular; you can control access at a resource level and for actions that can be performed. And when using IAM roles, if your EC2 instance gets compromised, you do not need to revoke credentials.
- **Enable multi-factor authentication (MFA).** By using more than one factor to prove that you are who you say you are (something you have + something you know + time of day/location), it becomes much more difficult for a cyber attacker to impersonate you.

Getting started with AWS security best practices

Identify the most common cloud configuration errors and make sure to avoid them (cont.)

- **Limit administrative access with AWS security groups.** Functioning much like gateway firewalls, security groups enable you to manage and apply access policies to instances that have similar functions and security requirements. For example, by restricting administrative access to only specific IP addresses, security groups helps block attackers who may try to probe your AWS environment.
- **Use virtual private clouds (VPCs).** An Amazon VPC is a virtual network that runs in your AWS account. This virtual network presents some key advantages from a security point of view: The network is isolated from other resources, it is not routable to the internet by default, and you can apply security groups and access control lists to reduce the attack surface.
- **Activate native AWS monitoring tools.** AWS monitoring tools such as CloudTrail, CloudWatch, and VPC Flow Logs provide baseline information about how data flows in and out of your AWS environment. These also store rich data that can be correlated with other event log data from your critical assets to spot intrusions, identify suspicious behavior, and collect indicators of compromise.

Getting started with AWS security best practices

Know the prevailing types of AWS attacks and what activities attackers perform

Unfortunately, cyber attackers don't always use the same tools or techniques in every attack. But there are enough common characteristics in AWS attacks to draw some instructive conclusions. Here are some specific warning signs to watch out for to detect an attack in progress:

- **AWS temporary security credentials with long duration.** Attackers will use temporary credentials with long lives to maintain connection persistence.
- **New AWS user account starting a high number of instances.** While this activity could be a rookie user making an honest mistake, it could also be an attacker cryptojacking your valuable AWS resources or malicious actors attempting to disrupt incident response efforts.
- **New user account used to delete multiple users.** Once an attacker has created a new user account for themselves, they can use it to lock out legitimate users en masse.
- **Multiple instances being started or shut down programmatically.** Attackers like to automate their exploits and this is a clear signal one is in process.
- **CloudTrail log deleted.** This could be an indication that an attacker is erasing traces of their malicious activity by deleting logs.

AWS logs to enable for effective security monitoring

Fortunately, AWS provides extensive logging, giving you detailed visibility into what is happening in your environment. Here's a non-exhaustive list of different types of AWS logs and the purpose each can serve from a security perspective.

Type of AWS log	Description	Security relevance
CloudWatch	AWS CloudWatch logs let you monitor and troubleshoot your systems and applications using your existing system, application, and custom log files.	Using CloudWatch logs, you can monitor activity, in near-real time, for specific phrases, values, or patterns. Alarms can be triggered if certain suspicious patterns are found. In addition, security analysts can access the original log data for in-depth forensic investigations.
CloudTrail	AWS CloudTrail service enables logging of all account activities on different AWS resources (like IAM console logins). Once enabled, AWS CloudTrail logs are delivered to your AWS S3 bucket.	CloudTrail records important details about all AWS activity, including user accounts making requests, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. With this information, you can easily track changes made to AWS resources to verify compliance, mitigate operational issues, and help reduce risks.
Virtual private cloud (VPC) flow logs	VPC flow logs capture network-level activity and connections among all the nodes on a VPC.	Network flow data provides essential forensic clues for security incident and data breach investigations. Central to your AWS security monitoring program, VPC flow logs empower you to examine and monitor network flow data to verify compliance and detect threats. This network flow data includes: • Inbound network connections from external IP addresses • Traffic produced by traditional services, such as NFS (network file system) file shares, on the internal network • Connections between microservices and APIs
Simple storage service (S3) server access	S3 acts as a central database for your AWS environment.	S3 server access logging provides detailed records for the requests that are made to a bucket, enabling security teams to track down whether API calls are authorized and verify that these access requests don't put sensitive data at risk.
Elastic load balancing (ELB)	ELB provides access logs containing details of requests sent to your load balancer.	You can use ELB access logs to analyze traffic patterns, troubleshoot issues, and investigate suspicious activity. Because each log contains information such as the time the load-balancing request was received, the client's IP address, latencies, request paths, and server responses, you can use these details to build comprehensive security incident timelines.

Getting started with AWS security best practices

Integrate native AWS Security monitoring tools with third-party apps

AWS provides a wealth of logging features and raw audit log data to help you monitor the overall security and compliance posture of your AWS assets. The next challenge is deriving actionable and relevant information from those mountains of event logs. Third party log analysis and event correlation tools apply correlation logic to AWS log data to alert you when emerging threats, as well as AWS misconfiguration and policy violations, expose your AWS assets to risk. Some of these tools can also integrate your on-premises event log data with your AWS log data for a complete picture of your security and compliance posture.

That said, not all log analysis and event correlation tools are the same. Make sure you verify that they will work with your AWS environment as easily as they do within your on-premises environment. A consistent and unified security monitoring program across your environments will help drive rapid and targeted incident response.

Getting started with AWS security best practices

Integrate native AWS Security monitoring tools with third-party apps (cont.)

Use the following questions to inform your log analysis tool evaluation process

Questions to ask your AWS security monitoring partner:

1. How do you detect cryptojacking or cryptomining activities in the cloud?
2. How do you detect AWS misconfigurations or other security exposures?
3. Which of the native AWS log file types do you support?
4. Which cloud-based enterprise apps can you collect logs for? (G Suite, Office 365, etc.)
5. What type of alarms does your tool generate?
6. How does your tool correlate events across disparate data sources and environments?
7. What are your capabilities for long term event log data storage?
8. What type of compliance reports does your tool generate?
9. What other security controls does your tool offer or integrate with (like security automation and orchestration, file integrity monitoring, etc.)?
10. How does your tool automate threat hunting?
11. From what sources do you get your threat intelligence and security research?

How AlienVault USM Anywhere can help

AlienVault® USM Anywhere™ from AT&T Cybersecurity is an all-in-one platform that delivers powerful threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments. Unlike traditional security approaches that try to retrofit their network-centric approach to AWS, USM Anywhere is optimized for AWS. We monitor and alert on an ever-expanding list of AWS services, including support for:

- CloudTrail monitoring and alerting
- S3 access log monitoring and alerting
- ELB access log monitoring and alerting
- CloudWatch monitoring and alerting
- GuardDuty monitoring and alerting
- Config monitoring and alerting
- AWS API asset discovery
- AWS-native cloud intrusion detection
- AWS vulnerability assessment
- AWS infrastructure assessment

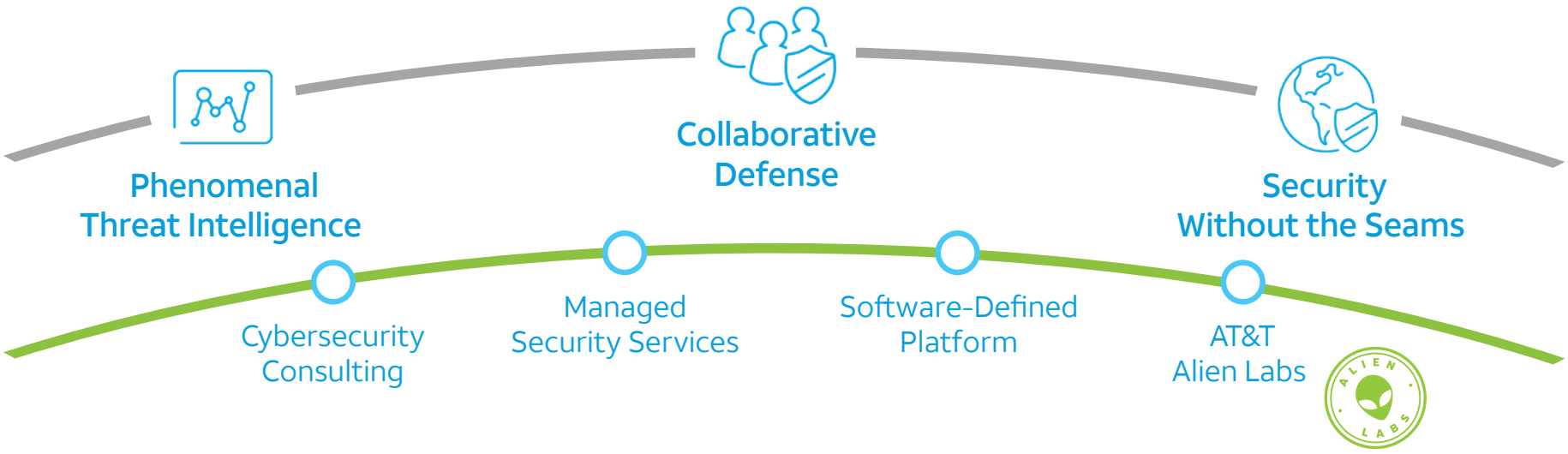
USM Anywhere provides an integrated security monitoring platform, saving you time and money so you can fully benefit from the speed and agility advantages of AWS. You can deploy USM Anywhere within minutes and start detecting threats the same day.

Click here to learn more about AWS security monitoring with AlienVault USM Anywhere.

About AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning – helping to enable our customers around the globe to anticipate and act on threats to protect their business.

Unified Security Management



This document is intended to include general information for beginners learning about security information and event management (SIEM). Use of names of third party companies in the document are for informational purposes only and do not constitute any endorsement by AT&T Cybersecurity (formerly AlienVault).

AT&T Business