ManageEngine
Cloud Security Plus

The National Security Agency's recommendations for cloud security

www.cloudsecurityplus.com

Index

Introduction

Cloud adoption comes with numerous advantages and benefits to an organization, but it also comes with a certain amount of risk. As the cloud industry becomes more mainstream, the underlying concept of cloud technology still isn't fully understood by everyone who uses it, making security decisions a hassle. To ease the confusion, the National Securty Agency (NSA) has published a document explaining the cloud infrastructure and its security vulnerabilities.

Cloud vulnerability classes according to the NSA

The NSA categorizes cloud vulnerabilities into four classes:

- Misconfiguration
- Poor access control
- Shared tendency vulnerabilities
- Supply chain vulnerabilities

1. Misconfiguration

Users are given certain privileges within the cloud infrastructure based on their responsibilities in the organization. When these privileges are not configured correctly, some user accounts may have access to information they're not supposed to have access to, while others may not have access to the information they need. Such misconfiguration of privileges, especially access privileges, pose the risk of sensitive information being leaked.

To prevent users from sharing sensitive information publicly, organizations can implement cloud service policies. Apart from leveraging cloud service policies, organizations should also continuously monitor all cloud resources, security events, and configuration changes to detect any misconfigured access or misuse of access.

One way to do this is auditing access logs using automated third-party solutions as these solutions provide detailed information about what happens in your cloud environment. Cloud Security Plus is a log management and monitoring tool for public cloud platforms that enables admins to monitor user activity and configuration changes, and receive real-time alerts through email to detect unusual behavior.

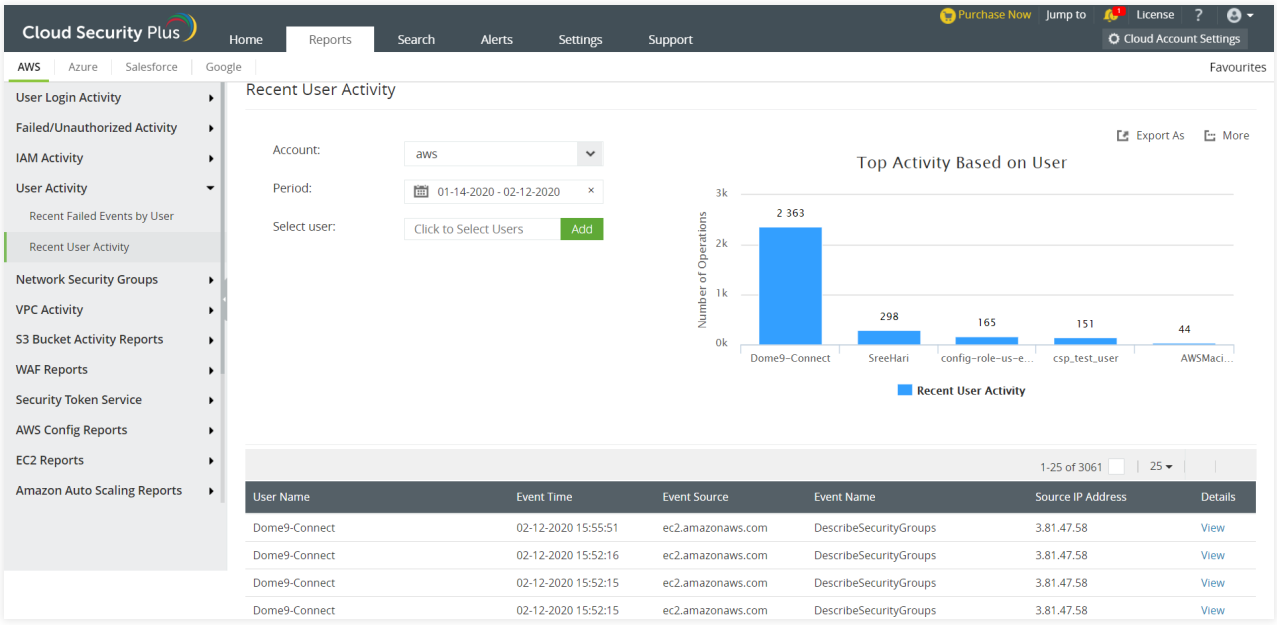

Figure 1: Recent user activity report in Cloud Security Plus

2. Poor access control

Authentication is the definitive security layer that prevents intruders from getting inside an environment. When this access control mechanism is compromised, the consequences can be disastrous. A poor access control mechanism will give intruders easy access to sensitive information, and allows them to change privileges and wreak havoc from within an organization.

A strong authentication model is imperative to prevent breaches in security. Multi-factor authentication can also be implemented to ensure that only authorized users gain access to an organization's network. Apart from stringent authentication measures, auditing access logs and login attempts can show if there are signs of a breach or unusual activity.

Third-party solutions provide more comprehensive information than native solutions of cloud service providers (CSPs) on reports such as user login activities. With solutions like Cloud Security Plus, admins can also track failed login attempts, which come in handy for detecting threats such as brute-force attacks.

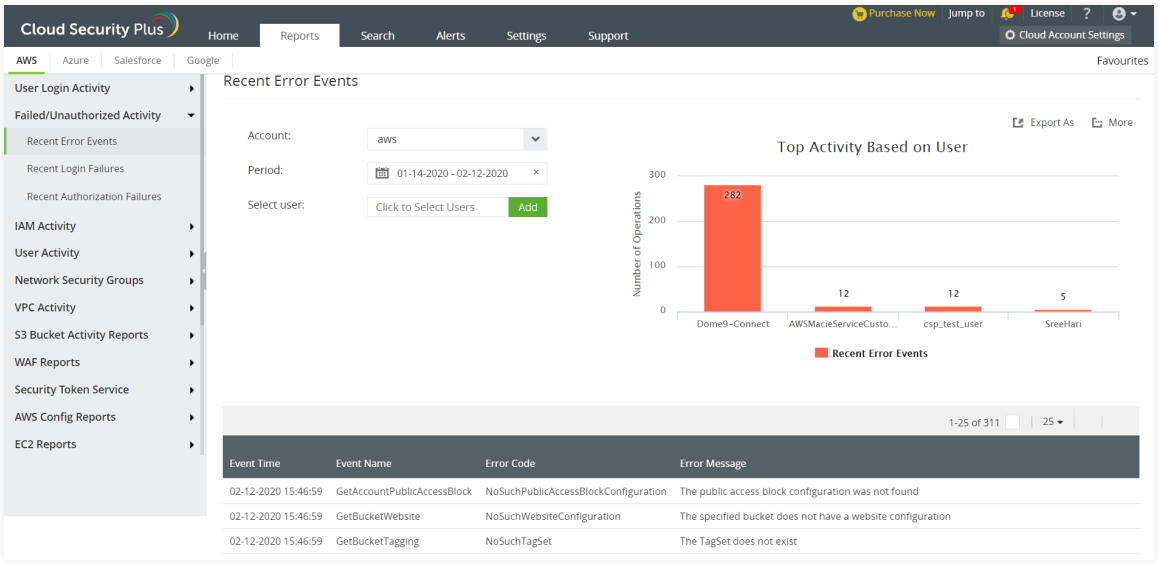

Figure 2: Recent error events report in Cloud Security Plus

3. Shared tenancy vulnerabilities

Cloud environments involve the use of multiple hardware and software components which are often sourced from various vendors. With such a complex infrastructure, there is a risk of one or more of these components will contain a vulnerability. Any attacker who is well-informed about the components used in a particular cloud environment can easily exploit the vulnerabilities of those components.

Two vulnerabilities that fall under this category are:

- Hypervisor vulnerability
- Containerization vulnerability

Hypervisor is software responsible for creating and running virtual machines. Cloud environments rely heavily on virtualization, which makes any hypervisor vulnerability critical. Containeriztion is technology that involves encapsulating all the necessary components to run an application independently on suitable hardware. Containerization vulnerabilities may give impostors access to sensitive data, which can be misused.

To mitigate these vulnerabilities, it is advised to run sensitive workloads on bare-metal or dedicated instances so that there are no other tenants in that instance that can access your information through an exploit. Additionally, data can be encrypted with strong encryption methods, which can then be continuously monitored. Closely monitoring the network can also help in detecting and mitigating a breach at the earliest stage.

4. Supply chain vulnerabilities

Supply chain vulnerabilities occur due to the design of cloud technology itself: i.e, multiple sources of hardware and software. It is a daunting task for CSPs to monitor a wide network of resources where they might miss some vulnerabilities, so it is wise to implement a security measure to ensure that your environment is not exploited through those loopholes.

Monitoring plays an important role here as well. Monitoring sensitive resources helps with detecting unusual activity in file servers. With every cloud activity logged, admins can detect unusual behavior by monitoring specific logs, but finding patterns that indicate suspicious behavior manually can be a time-consuming challenge.

Third-party solutions offer canned reports that collect logs and display them in an easy-to-read format. Cloud Security Plus can go a step further by allowing admins to configure alerts via email for activities that indicate malicious intent.

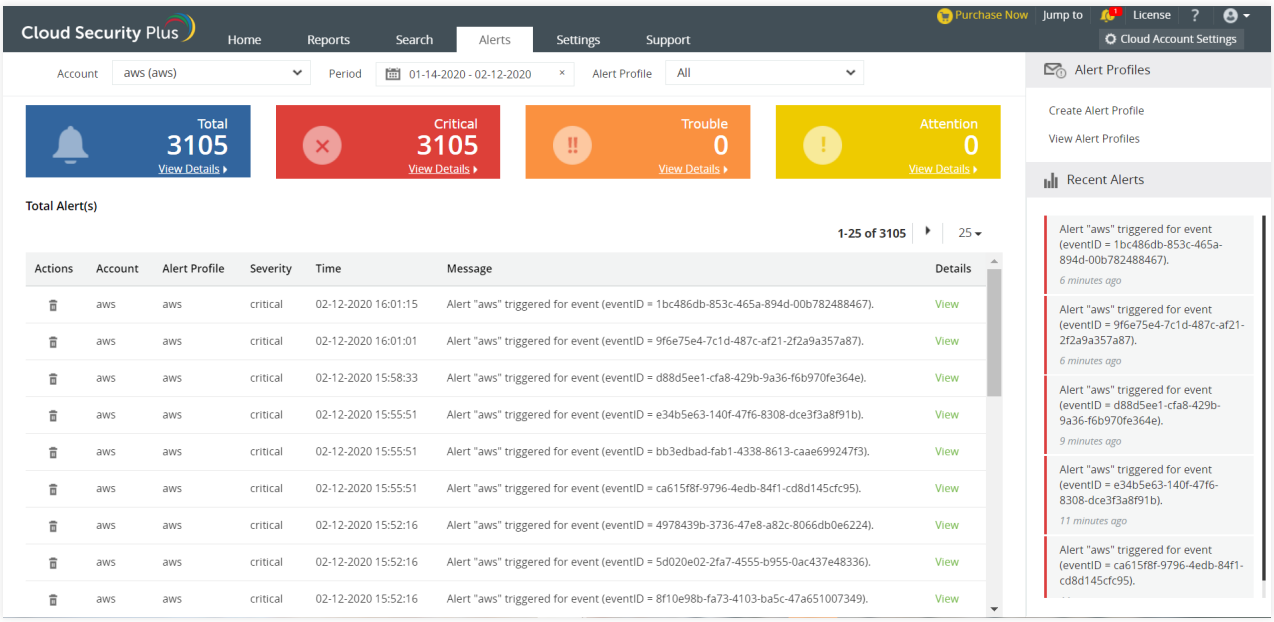

Figure 3: Alerts tab in Cloud Security Plus

Summary

The benefits cloud environments offer attract many organizations to migrate to the cloud. Careful implementation of the cloud environment will ensure effective security against vulnerabilities and the risks associated with cloud technology. Third-party security solutions can go a long way in mitigating those risks and vulnerabilities. To simplify cloud security and management, organizations should look to implement a comprehensive solution that can provide the necessary insights for monitoring and securing cloud environments.