Cloud Advisor

Next generation CSPM with context analysis

Author: Cloud Advisor

Document type: Whitepaper

Content

Cloud security and CSPM solutions

The cloud model of service consumption continues to gain momentum. Some companies are growing their presence in the cloud by increasing the number of resources there, while others are just discovering new opportunities. The cloud is a dynamic structure where objects are constantly being created, changed, and deleted. A large number of objects with complex interrelationships are deployed on cloud provider sites. Often, employees who have a shortfall of security expertise hold access rights to the cloud. This can result in public cloud configuration mistakes, the consequences could lead to loss of data or a leak.

More than 123 million records of clients and employees of Decathlon, a French sporting goods retailer, were leaked to the public because of the wrong configuration of cloud resources. They included unencrypted emails and passwords, API call logs, employee personal data (employment contracts, dates of birth, social security numbers, etc.).

In response to such threats, a class of Cloud Security Posture Management (CSPM) software products have emerged. These solutions retrieve configuration data of objects located in your cloud infrastructure, checks them for compliance against security policies, and alerts on possible violations and potential threats.

CSPM issues

Given the number of objects and the dynamic nature of the cloud, the CSPM product generates a large number of security policy violation alerts. In some environments, the number can reach several hundred per day. This leads to a number of serious negative consequences:

- Increased response time to a critical incident. An engineer may deal with lower-priority alerts, while critical events are left unattended.

- Missing an important alert due to alert fatigue. Responding to one alert is simple; responding to dozens or hundreds of alerts is an order of magnitude more difficult. The more there are, the greater the risk of missing something important and critical.

- Higher costs associated with parsing alerts, which are false positives. Many of the alerts require a lengthy investigation involving specialists from other departments.

- Emotional burnout of engineers. The constant flow of alerts and the monotonous work of sorting them out leads to employee burnout, increased staff turnover, decreased job satisfaction and productivity.

Solution – alert prioritization

The only way to fight the enormous number of alerts is to prioritize them properly. Let's take a look at prioritizing with a single example: imagine that we have a misconfigured Security Group which allows all inbound connections from all IP addresses.

A traditional CSPM will read the data about the Security Group object and alert about wrong configuration, suggesting appropriate remediation. What is the priority of this problem? And if there is more than one Security Group, which one should you pay attention to first?

Let's analyze the possibilities, based on the context:

- The Security Group may not be associated with a virtual machine or it may be associated with a VM that has no public access. In this case, the priority of this problem is Low. This problem can be dealt with when all high-priority alerts are handled.

- The Security Group is associated with a public VM. An attacker can connect to this VM if there are software vulnerabilities or using previously stolen access credentials. This problem needs to be solved quickly and its priority is High.

- A Security Group is associated with a public VM that has administrator rights to the entire cloud account. In this case, an attacker can not only infiltrate the machine, but also gain control over the cloud account. This problem is a Critical priority and needs to be addressed immediately.

However, traditional CSPMs do not analyze this kind of context and see no difference in the importance and danger of the options described. Moreover, traditional CSPMs see all three situations - a Security Group configuration error, a VM with a public IP address, and a VM having high privileges - as three separate, unrelated alerts with the same danger level - Medium.

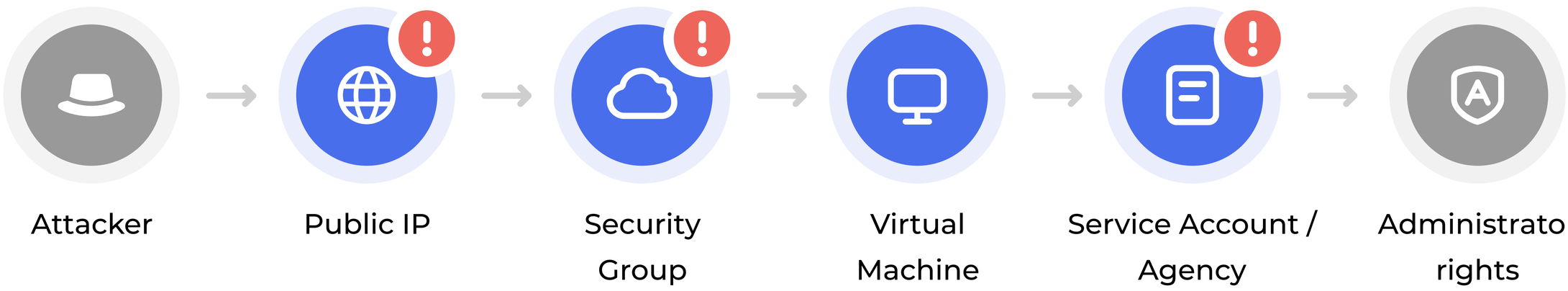
Next generation CSPM with context analysis

The next generation CSPM not only analyzes each cloud resource as an individual object, but also looks at its network connections to other cloud objects and the permissions the resource has in the cloud.

Thus, the next generation CSPM sees not individual alerts, but their toxic combinations that form the actual attack vector.

> Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.
>
> John Lambert, Microsoft Threat Intelligence Center

In this case, we have the following attack vector:



The case with a Security Group above is just an example, all other cloud security checks should also take the context into account.

Conclusion

Public cloud security teams need to use cloud security posture management (CSPM) tools. We recommend use of next generation tools, with prioritization of alerts based on network connectivity and permissions analysis in the cloud. Such solutions increase the speed and quality of security incident handling and reduce the cost and labor intensity of the process.

Cloud Advisor is one of these solutions that provides protection for cloud infrastructures deployed in Huawei Cloud, Yandex.Cloud, or SberCloud.Advanced. More information about the product is available at www.cloudadvisor.app