Cloud Advisor

Vulnerability search in software and OS’s in public clouds

Author: Cloud Advisor

Document: Whitepaper

Contents

Introduction

In recent years, the cloud has evolved from a promising new technology that many were at first wary of trusting their data completely into a critical business strategy tool. More and more companies are entrusting their critical workloads to cloud providers, moving important processes and resources to cloud. This simplifies business processes, speeds up new product releases, and ultimately improves the competitiveness of the solutions and the company as a whole. However, not everyone realizes that the use of new technologies requires new approaches to information security.

Security was the number one challenge facing respondents in ten of the eleven State of the Cloud reports.

Flexera 2022 State of the Cloud Report

One of the main practices for ensuring security has always been to prevent exploitation of vulnerabilities. Software vulnerability infiltration is considered one of the most popular attack vectors. Let's see what vulnerability management techniques currently exist and how well they work in the cloud.

Scanning

Classic approaches to vulnerability scanning

The following vulnerability scanning technologies are the most common today.

1. Unauthenticated scan

With this approach, a virtual machine is scanned as a "black box" about which the only thing known is its IP address.
The scanner does not know what is happening directly on the VM, but only tries to speculate based on the VM's responses to incoming network requests sent by the scanner. The disadvantages of this approach are obvious:

a. The risk of missing something important, since data can only be obtained from a limited number of ports open at the time of the scan and available services.

b. Large number of false positives.

c. Low granularity of the responses.

d. The need for network access from the scanner module to the host to be scanned.

2. Agent-based scan

In this case, scanning is performed with the help of agents that are installed directly on the VMs, they collect information and send on to the control module. Main disadvantages:

a. In practice, it is impossible to achieve 100% coverage of the entire infrastructure with agents, which results in the so-called "blind spots".

b. The need to install and update agents on each VM increases the total cost of ownership.

c. Agents affect the performance of the system.

d. Agents can be deleted, disabled, or bypassed by intruders or malicious code.

e. Agents themselves may contain vulnerabilities and thus increase the attack surface (for example, CVE-2022-0015 or CVE-2021-1647).

3. Authenticated scan

With this approach, the scanner gains network access to the VM using authentication over SSH or RDP and performs the scan in the context of the target system. There are the following disadvantages:

a. Having an additional account with broad privileges necessary to perform a scan on each VM increases the attack surface.

b. Lack of coverage, similar to agent-based scanning, due to the inability to "reach" every system in a distributed infrastructure or the lack of an additional account required for scanning.

c. The requirement of password rotation for this account makes it difficult to maintain the solution.

d. This type of scan affects the performance of the system.

Cloud Advisor scan

The method implemented by the Cloud Advisor solution takes advantage of the benefits available in the cloud and therefore avoids the disadvantages described above. On the contrary, this approach:

- Provides 100% coverage of all virtual machines immediately after deployment.
- Allows you to deploy Cloud Advisor in minutes and get full information about all vulnerabilities in your infrastructure within an hour.
- Doesn't require any effort to install and update agents, reducing the total cost of ownership.
- Has no effect on virtual machine performance.
- Requires no network communication between the machine and the scanning module.

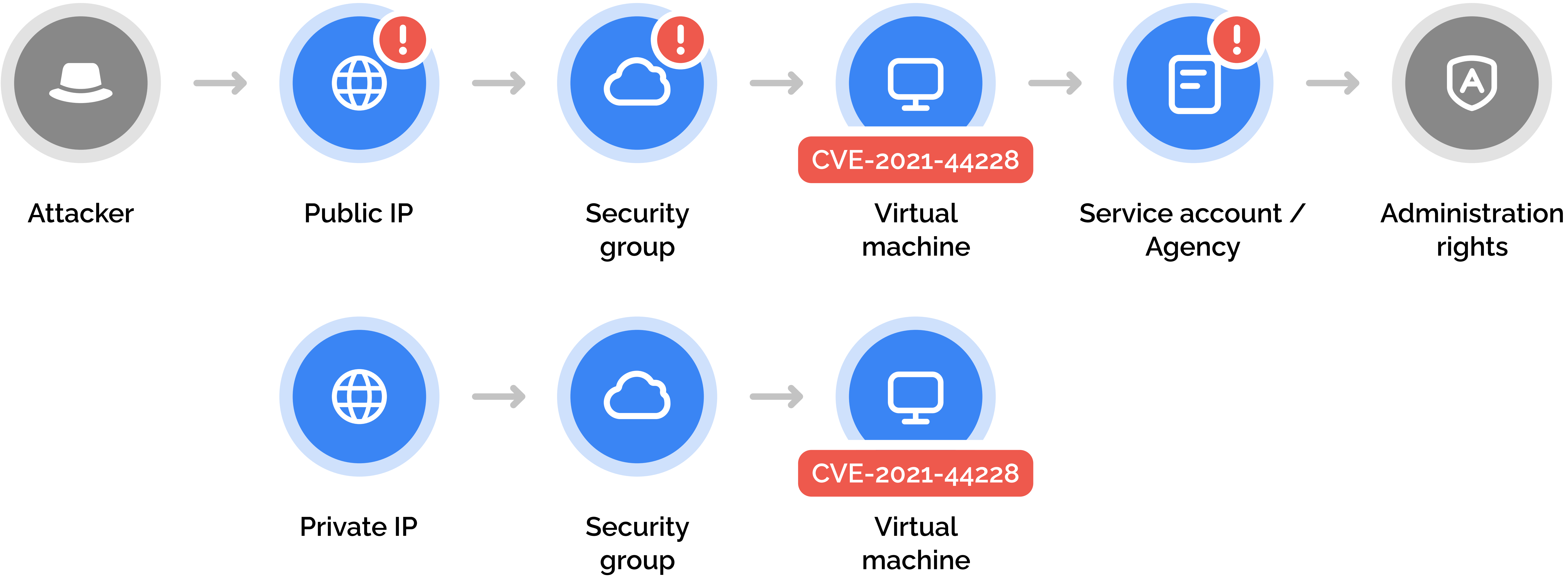
One of the drawbacks is that this approach solely functions in the cloud, as it relies on the VM disk management capabilities offered by the cloud provider. Additionally, there is a small rise in cloud costs since the scanning capabilities are implemented within the user's account.

Prioritization

One of the most important tasks in the vulnerability management process is their prioritization.

Traditional approach

Traditional vulnerability scanning tools do not possess data about network connectivity and rights of virtual machines in the cloud. For solutions designed for on-prem, the priority of a Log4Shell vulnerability on a public web server with access to an important database and Log4Shell on a forgotten private machine without any rights would be the same.



Some products provide VM prioritization capabilities, but only in manual mode, because the vulnerability search tool does not have access to cloud configuration information, and therefore does not have data about network connectivity and VM rights in the cloud. Manual prioritization does not work in a dynamically changing cloud environment.

As a result, the user receives hundreds, sometimes thousands of alerts about vulnerabilities found on VMs. This leads to a number of serious negative consequences:

- Increased response time to a critical incident. The engineer can deal with lower-priority alerts while critical events go unattended.
- Missing an important alert due to alert fatigue. Responding to one alert is not difficult, but responding to dozens or hundreds of alerts is much harder. And the more there are, the greater the risk that the employee will miss something important.
- Increased costs associated with parsing alerts that 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.

Cloud Advisor approach

The only way to deal with a large number of alerts is to properly prioritize them. Similar to traditional vulnerability management tools, Cloud Advisor performs prioritization using information about the presence of public exploits, vulnerability type, CVSS score, etc.

However, having full information about the network connectivity of cloud resources, Cloud Advisor additionally analyzes public IP addresses, load balancers, NAT, while analysis of security group rules imposed on the resource allows to calculate effective public exposure, i.e. to separate public exposure from all IP addresses and public exposure from a limited number of IP addresses. This analysis helps to understand which vulnerabilities are found on resources with unrestricted public access and should therefore be addressed first.

In addition, based on the data about rights of resources in the cloud, Cloud Advisor is able to assess the possible consequences from their compromise and raise the priority of vulnerabilities found on VMs with broad rights in the cloud (for example, access to the object storage or rights to start other VMs).

Conclusion

Modern vulnerability scanning tools are not designed for the cloud. The presence of blind spots, high total cost of ownership, and impact on cloud resource performance are caused by the use of legacy on-prem approaches. Increased incident response times and missed important alerts are the result of a lack of proper prioritization based on cloud configuration data.

Cloud Advisor provides an easy to install and easy to use tool that provides instant deployment and 100% coverage of your infrastructure. Complete information about cloud configuration allows Cloud Advisor to report only a small percentage of really important incidents that are critical to your organization.