Google Cloud

Posture management tools and techniques

Previously, you learned that vulnerability remediation is the process of identifying, assessing, and resolving security vulnerabilities in your cloud environment. You also learned that posture management is the continuous process of monitoring, assessing, and maintaining the security stance of an organization's cloud resources. And, you learned the steps to address vulnerabilities in an application.

In this reading, you'll learn more about posture and vulnerability management and the advantages and disadvantages of different posture management strategies. You'll also find out how these techniques can enhance a business's cybersecurity posture and help prevent problems with an on-the-job example.

Cloud security posture management (CSPM)

Cloud security posture management (CSPM) is an automated software tool that finds security risks in your cloud infrastructure. Based on predefined or customly defined security policies, it inspects your cloud-hosted resources and finds potential vulnerabilities and security risks.

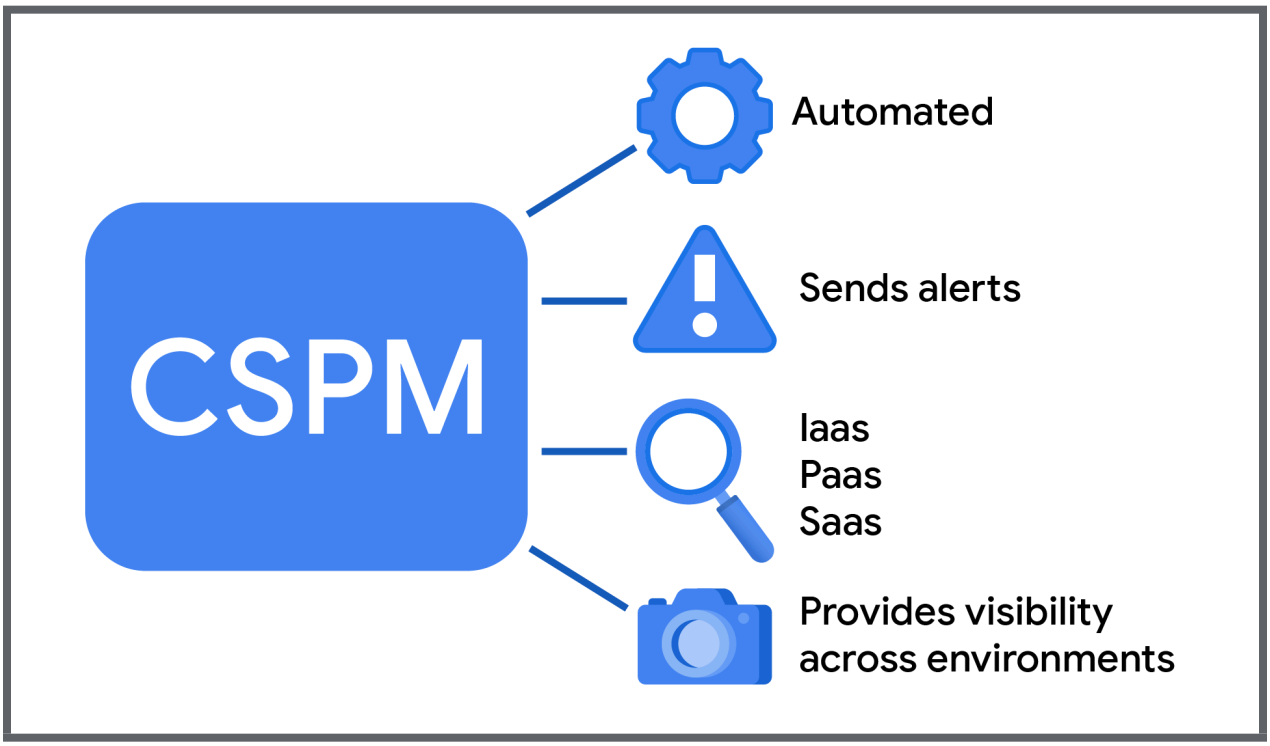
Here are some of its benefits:

- CSPM is automated, so it runs in the background and analyzes your cloud for vulnerabilities and risks.
- CSPM sends alerts to security teams when it finds potential risks.
- CSPM can search resources and services used across your infrastructure and platform.
- CSPM helps with monitoring by providing visibility across environments and across multiple clouds.

While CSPM has many benefits, it also has some challenges:

- CSPM is designed for infrastructure / environment level assessment, so it shouldn't be used to replace web application vulnerability scanning and other measures to identify security weaknesses.
- CSPM does not detect lateral movement. Even though it may not directly detect an attacker moving laterally through the cloud environment, CSPM results can serve as indicators for a compromise or an ongoing lateral movement.

Pro tip: When using CSPM, be sure to use it together with other strategies and mechanisms to provide a holistic coverage and mitigate the challenges identified.



Data security posture management (DSPM)

Data security posture management (DSPM) is a group of technologies and practices. It focuses on the content and context of your protected data, with an emphasis on protection for all sensitive data.

Here are some of its benefits:

- DSPM helps provide data discovery and scans for sensitive data, mapping how sensitive data is being stored and processed.
- DSPM classifies data in the cloud and helps teams prioritize incident response procedure and policy development.
- DSPM helps enforce security practices dealing with data access. These include encrypted storage, user management, and access control.

Like CSPM, DSPM has some challenges:

- DSPM requires specialized expertise because it's a combination of technical implementation and administrative process improvements.
- Like other security practices, DSPM is most effective when integrated into your overall security methodology and tools, like Data Loss Prevention (DLP) or Security information and event management (SIEM). So, it shouldn't be seen as a practice that should be implemented stand-alone.
- DSPM is not specific to data in the cloud, but should be applied across a company's

environments, including on-premises. This requires an approach that can be applied consistently across all environments.

CSPM and DSPM techniques

Now CSPM and DSPM are not mutually exclusive. They can be used together to enhance a business's cybersecurity posture and help prevent problems. To explore this topic, consider these two questions:

1. How can CSPM and DSPM be used together?
2. How can using CSPM and DSPM help prevent problems?

How can CSPM and DPSM be used to prevent problems?

Example 1

An on-the job example of how an organization that stores a lot of sensitive data on the cloud can use CSPM and DSPM together is to implement CSPM for infrastructure-level controls, and implement DSPM for data-level security controls. This combination can help prevent problems.

Consider an organization with a security policy that doesn't allow the creation of VMs with external IP addresses. When this kind of attempt is made in the organization's environment, CSPM will detect unauthorized creation of resources with external IP addresses and block this action.

Note: Industry regulations prevent saving financial data in plaintext format. If a developer makes a mistake attempting to save the log data containing credit card numbers, DSPM will kick in and apply data level controls before the data gets written to storage.

Example 2

Now consider another on-the job example of how an organization can use CSPM and DPSM to prevent problems that result from unintentional actions. Any organization can face risks from intentional or unintentional actions. Intentional actions happen when an attacker from outside, or a malicious agent inside, finds a way to cause damage. Unintentional actions happen when a mistake leaves sensitive data exposed to the public.

In this unintentional action, millions of files belonging to a major service corporation, including private data for its users, are exposed because a storage bucket was configured improperly.

Posture management—in this case CSPM—will prevent misconfigurations like this bucket configuration by detecting the files in a storage bucket or account that are exposed to the public. DSPM will detect the labeling and security policy applied to the files or data and apply data protection control.

Key takeaways

Posture management is vital to you as a cloud security professional, and different types of posture management have different benefits and challenges. Both CSPM and DSPM can be used together to enhance a business's cybersecurity posture and help prevent problems. CSPM focuses its protection on infrastructure and resources, while DSPM focuses its protection on data.