Google Cloud

On-the-job asset management applications

So far, you've learned that **asset management** is the process of tracking assets and the risks that affect them. You've also learned about the importance of following the best practices and steps of asset management. In this reading, you'll learn why you should implement an effective asset management approach and review a few on-the-job examples that successfully apply asset management.

Reasons to implement asset management

The number and seriousness of cyber threats continues to rise. So as a cloud security professional, it's imperative to practice effective asset management to maintain your organization's security resilience. In today's enterprise environment, most assets are created in the cloud. An effective asset management approach can:

- Show full visibility of all your cloud service assets, in addition to your on-premises assets.
- Help you to discover new assets or changes to existing assets as they're added, if you use automation with asset management.

Why prioritize asset management?

Effective asset management is crucial because you can't secure what you can't see. When you don't make effective asset management in your organization a top priority, the potential of cyberattacks increases. Suppose a development team within a company provided a jumpbox server with SSH access to third party contractors, and the company 's cloud security team is unaware of the jumpbox server. This is an example of not prioritizing asset and inventory management. Remember, you can't secure what you can't see. When the company's security team is not aware of the jumpbox server, they can't secure it proactively. Threat actors now have a way to exploit vulnerabilities, using enumeration techniques and research vulnerabilities on unpatched assets. Misconfigured and publicly accessible resources are other ways a threat actor can gain access into your environment.

When organizations place emphasis on effective asset management, they can better avoid problems. Having effective asset management also contributes to maintaining resilience and security maturity, which is crucial in the face of ever-evolving cyber threats.

Pro tip: Be sure to always have an accurate and up-to-date asset inventory, including a way to analyze your historical data.

Note: If you build an asset register, which is a subset of the asset inventory that focuses on security-critical information, it's only as good as its data. So, keep your asset register up-to-date at all times.

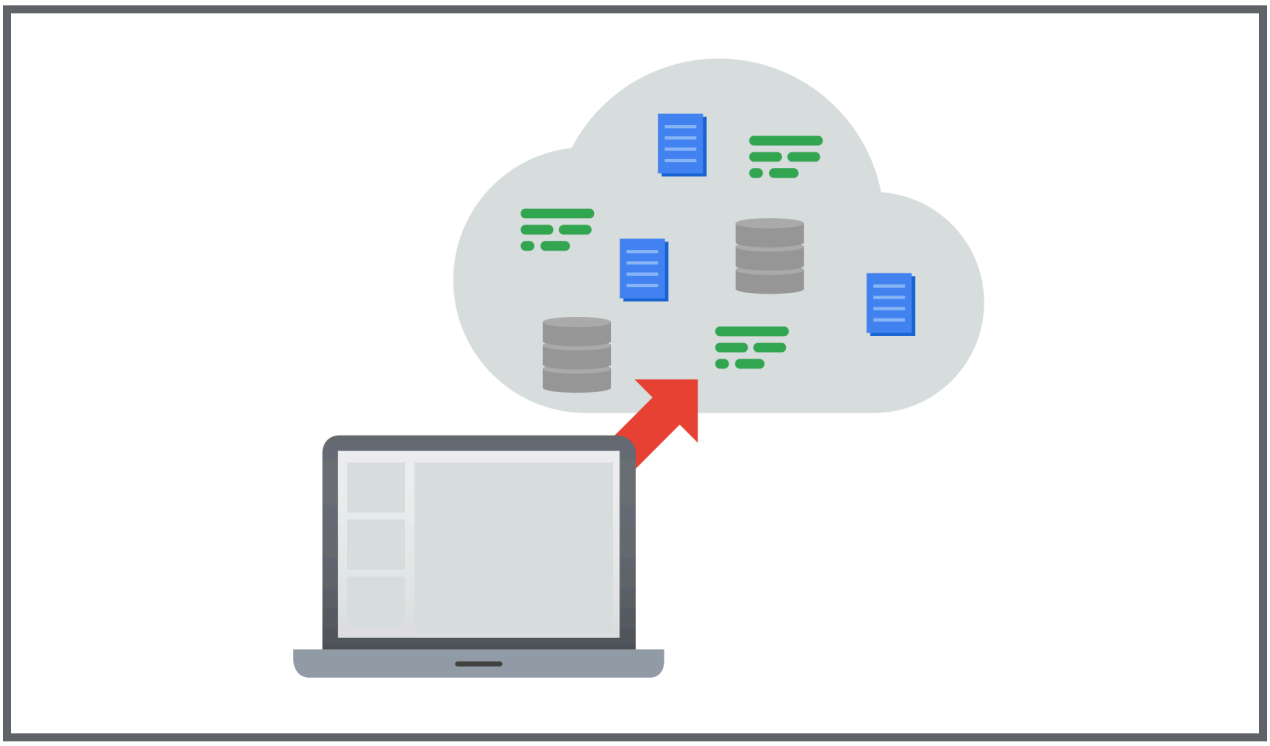
On-the-job examples applying asset management

Next, you'll review some scenarios covering organizations that successfully implemented asset management.

Part 1: Security governance and operations

A company improves its cloud operations using asset management by following these steps:

1. Include tracking resources in the asset management system to address privacy and data security across their assets. By tracking resources, they can assess and address privacy and security requirements for the assets and the data managed by them.
2. Build policies to ensure security controls are applied consistently across its cloud. This will minimize the threat of a breach.
3. Set policies to ensure consistent configurations that manage risks from drift, recovery, and discoverability.
4. Implement the vulnerability remediation process of identifying, assessing, and resolving security vulnerabilities in their cloud environment using both cloud security posture management (CSPM) and data security posture management (DSPM). CSPM focuses its protection on software and infrastructure, while DSPM focuses its protection on data.
5. Set policies for standardization, centralization, and consistency in its deployment approach.



Part 2: Security operations focus

The company now wants to focus on security, and they realize asset management is vital. The security team decides to automate the company's asset management. The team knows there can be policy deviations, so they monitor the assets for any deviations. For example, privileges may be escalated, or assets may be created without proper security controls. Here are some tools and how a company can use them to automate asset management and monitor policy deviations:

- **Security Command Center (SCC)**
  - Monitor cloud resource policies for compliance deviations.
  - Generate reports on cloud resource usage and configuration, surface these findings, and provide recommendations for changes to cloud resources or their configurations.
- **Cloud Asset Inventory:**
  - Search asset metadata by using a custom query language.
  - Export all asset metadata at a certain timestamp or export event change history during a specific timeframe.
  - Monitor asset changes by subscribing to real-time notifications.
  - Analyze IAM policies to find out who has access to what.
- **Cloud Identity and Access Management (IAM):**
  - Enforce defined policies on who can access cloud resources and what they can do with them.

- Audit access to cloud resources and generates reports on compliance.
- Work with the policy intelligence service to provide role recommendations.
- Help you enforce the principle of least privilege by ensuring that principals have only the permissions that they actually need.

The company's cloud security team uses their security information and event management (SIEM) system to monitor, detect, and analyze security events within their environment. The security team can integrate SCC with their SIEM, and have SCC data sent to the SIEM platform for more analysis. The security team can then respond to and manage response to security findings there.

Key takeaways

Since cloud computing assets are online instead of on-premises, you can't physically see those assets. So, you need to practice effective asset management, like proactively checking the assets to ensure they're secured.

It's also important to set policies for your assets. These policies should ensure consistency in identity management and configuration. While automation can take on some of the management duties, you need to constantly monitor assets for any deviations.