Google Cloud

# Cloud tools for risk management

You've already learned about how to use cloud tools, like Risk Manager and Policy Analyzer, to help manage risk. In this reading, you'll learn more about cloud tools for risk management that fall under the five pillars of the NIST CSF framework. Please note, the following reading should not be considered legal advice.

## Cloud tools for risk management

There are key cloud tools that your cloud security team can utilize that fall within each of the five pillars of the NIST CSF:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

### Identify

Tools that relate to *Identify* help your security team to identify access controls, cloud assets and data, and the current security posture of cloud assets.

**IAM**: IAM manages access control by defining who has access to resources. In IAM, permissions are grouped into roles. It's best practice to bind roles to groups and then place users into groups, rather than to bind a role directly to a user. This is because it is easier to move a user into or out of a group to allow them necessary permissions. Once a user is a member of a group they'll be able to access the desired resource.

**Cloud Asset Inventory:** Cloud Asset Inventory provides inventory services based on a time series database. This database keeps a 35-day history of Google Cloud asset metadata. This helps you to identify which assets need to be secured.

**Cloud Identity:** Cloud Identity is an Identity as a Service (IDaaS) solution that centrally manages users and groups.

**Google Cloud Security Command Center (SCC):** SCC fits into the Identify pillar by providing your organization with a centralized view of your security posture across your cloud resources. SCC includes a number of features that help organizations identify security risks and vulnerabilities, including:

- Asset discovery and inventory: SCC continuously scans GCP resources to identify and

inventory all assets.
- Vulnerability management: SCC scans GCP resources for known security vulnerabilities.

## Protect

The *Protect* pillar includes tools and security measures that protect cloud data and assets.

**Cloud Intrusion Detection (IDS)**: Cloud IDS is an intrusion detection service that provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network. Cloud IDS works by creating a Google-managed peered network with mirrored virtual machine (VM) instances.

**reCAPTCHA Enterprise**: reCAPTCHA Enterprise uses an advanced risk analysis engine and adaptive challenges to keep malicious software from engaging in abusive activities on your website. Meanwhile, legitimate users will be able to login, make purchases, view pages, or create accounts, and fake users will be blocked.

**Cloud Armor:** Cloud Armor is a network security service that helps protect your applications and website against distributed denial of service (DDoS) and web application attacks. It also offers a rich set of Web Application Firewall (WAF) rules.

**Beyond Corp Enterprise:** BeyondCorp Enterprise ties together a user's information with device and location context to help your organization enforce its security policy.

**Identity Aware Proxy (IAP):** IAP lets you establish a central authorization layer for applications accessed by HTTPS, so you can use an application-level access control model instead of relying on network-level firewalls.

**Two factor authentication(2FA)**: 2FA is an identity and access management security method that requires two forms of identification to access resources and data. It includes security tokens like Titan keys and passkeys.

**Security Command Center (SCC):** SCC can help you protect resources by detecting threats. More about detecting threats is covered in the next pillar, *Detect*.

**Service controls:** Service controls help protect against accidental or targeted action by external entities or insider entities, which helps to minimize risks from Google Cloud services, like Cloud Storage and BigQuery.

**Zero trust:** Zero trust is a security model used to secure an organization based on the idea that no person or device should be trusted by default, even if they are already inside an organization's network.

## Detect

The *Detect* pillar includes tools that log, monitor, detect, and manage vulnerabilities.

**Cloud Logging**: Cloud Logging is a real-time log-management system with storage, search, analysis, and monitoring support. Cloud Logging automatically collects logs from Google Cloud resources. You can also collect logs from your applications, on-premises resources, and resources from other cloud providers. You can configure alerts to notify you if certain kinds of events are reported in your logs, and for regulatory or security reasons, you can determine where your log data is stored.

**Cloud Monitoring**: Monitoring is the process of continuously examining IT infrastructure to help detect cyber threats and data breaches. It can help detect changes in performance, in availability, and in behavior or other changes. Monitoring gives you immediate insights into unauthorized updates or suspicious activity on your network. Google's Cloud Monitoring tool provides automatic data collection dashboards for Google Cloud services. It also supports monitoring of hybrid and multicloud environments.

**Security Command Center (SCC):** SCC helps your security team detect and manage vulnerabilities and strengthen your security posture. SCC uses a variety of signals to detect and analyze threats to GCP resources. These signals include security alerts from Google Cloud services, threat intelligence feeds, and custom rules that your organization can create. SCC provides you with a centralized view of security alerts and incidents, and it helps you to prioritize and respond to threats.

**Chronicle Security Information and Event Management (SIEM):** Chronicle SIEM is a collection of services and tools that help a security team collect and analyze security data as well as create policies and design notifications. It combines the management of security information and security events using real-time monitoring and the notification of system administrators.

## Respond

Tools that relate to the *Respond* pillar help to ensure that your cloud security team responds quickly and effectively to threats and breaches.

**Chronicle Security Orchestration, Automation and Response (SOAR)**: Chronicle SOAR is a Google software solution that enables your security team to integrate and coordinate separate tools into streamlined threat response workflows.

**Mandiant:** Mandiant helps you to identify what was compromised, assess the pathway to attack and remediate the breach, so you can resume regular business activities.

### Recover

Tools related to the *Recover* pillar help your security team to recover from a breach safely and quickly, so that business can continue.

**Backup and restore**: Backup and restore tools for Google Cloud restore data in its original format, so that many workloads are available directly from long-term backup storage with no need for data movement or translation. After an initial full backup is performed, data is backed up incrementally, updating and storing any data that changed since the last backup. All backups, including those for general applications, VMs, databases, and file systems, are managed using the Google Cloud console.

**Actifio Go:** Recovery tools like Actifio Go, can help to recover data, including:

- Granular recovery: recovery of individual files, folders, or database records
- Application-aware recovery: recovery of applications and their associated data together, ensuring that applications are recovered in a consistent state
- Bare metal recovery: recovery of entire systems, including the operating system and all applications and data

**Cyber insurance:** A cyber insurance policy helps your organization pay for any financial losses incurred in the event of a cyberattack or data breach. It also helps your organization cover any costs related to the remediation and recovery process. Related costs might include investigations, crisis communication, legal services, and refunds to customers.

## Key takeaways

You can associate the five pillars of the NIST CSF: Identify, Protect, Detect, Respond, and Recover with cloud tools that your cloud security team can utilize. Knowing more about the key purposes and best practices for cloud tools will enable you to more effectively prepare for risk management.

## Resources for more information

Review these resources to learn more:

- To learn more about making analysis queries check out this link Policy Analyzer for IAM
- Click the link to learn more about IAM