Google Cloud

The role of BCDR tools

So far, you've learned that business continuity and disaster recovery (BCDR) tools can range from BCDR plan builders and backup and restore utilities, to sophisticated software that handles data center failovers. BCDR tools aren't just pieces of software, they're what you, as a cloud security professional, can use to ensure your business continues to run smoothly and efficiently during disaster recovery.

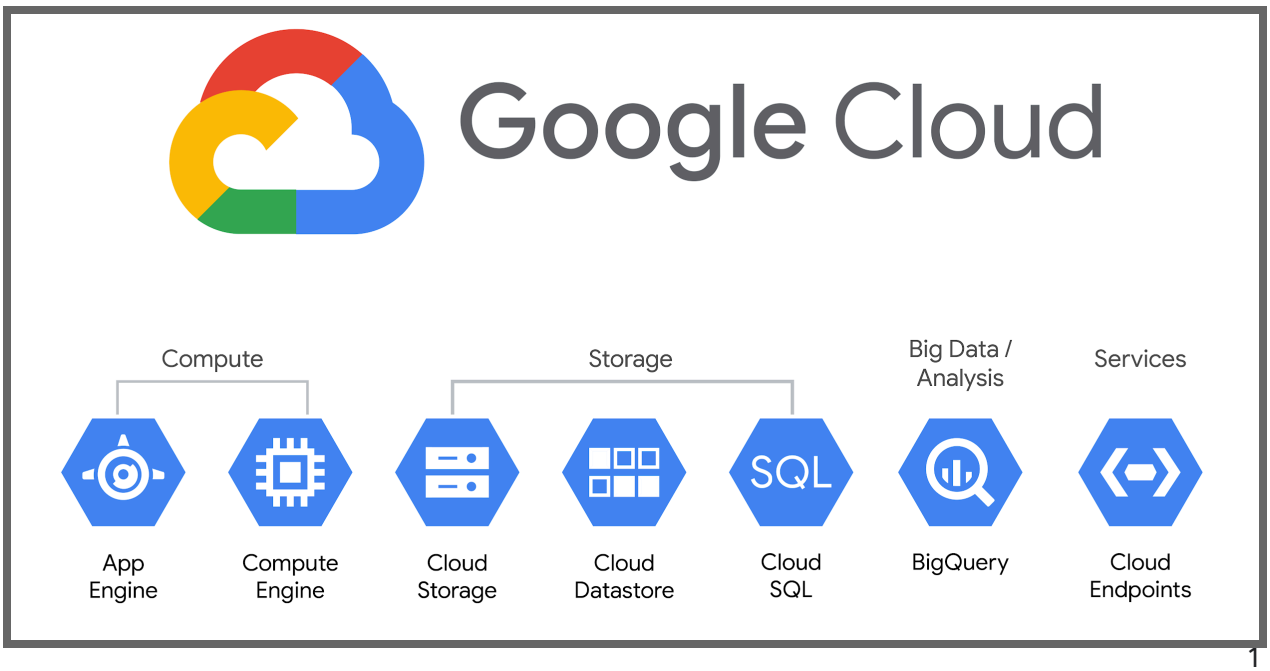
In this reading, you'll learn about BCDR categories and some common BCDR tools and their key features. Then, you'll learn the general steps to using the all-important BCDR recovery toolset for any cloud-based operation. Next, you'll inspect Google Cloud services that aid in disaster recovery.

You'll also explore some of the many ways you can automate the tasks involved in recovery, including a scenario using Google Cloud Backup and Disaster Recovery (DR) to help a business minimize downtime and get back to business as quickly as possible.

BCDR categories

BCDR tools can be categorized into two main types:

- **On-premises BCDR tools:** These tools are installed and run on the organization's own hardware and software.
- **Cloud-based BCDR tools:** These tools are hosted and managed by a cloud services provider.



BCDR common tools and key features

BCDR tools can help you and your cloud security team make and execute a plan to restore your systems and get data back online. The tools ensure you can continue normal operations and continue serving your users without any interruption. There are a variety of different BCDR tools available, each with its own specific purpose.

Some common BCDR tools and their key features include:

- **Backup and recovery tools:** Use these tools in the event of a data loss to back up and restore data on a variety of different storage media, including on-premises storage, cloud storage, and tape.
- **Disaster recovery automation tools:** Use these tools to automate the process to restore systems and data to a working state after a disaster, or other disruptive event. You can also use these tools to support a variety of different disaster recovery strategies, including:
    - **Failover:** Helps protect systems from failure
    - **Failback:** Restores the latest data from the backup image to the production application, restores the application from the latest data, and then performs a clean up
    - **Replication:** The process of continuously creating copies of data to multiple locations to support availability
- **Business continuity (BC) tools:** Use these tools to develop BC management plans to help maintain your business operations during and after a disaster. You can also use these tools to generate BCDR reports on activities and track performance in order to identify BCDR plan progress and areas for improvement.

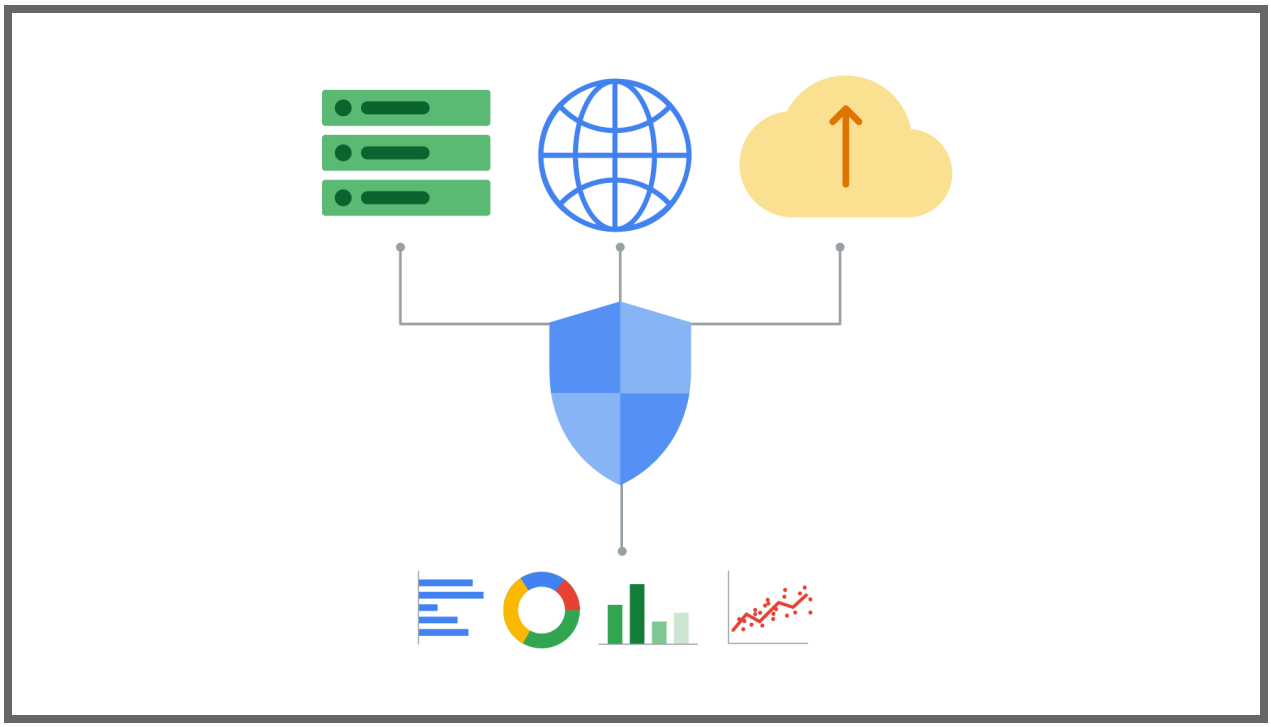
How to run a BCDR recovery tool:

To run a BCDR recovery tool, you'll typically need to:

1. **Identify the affected systems and data:** The first step is to identify the systems and data that have been affected by the disruptive event. This may involve running reports or manually checking systems.
2. **Select the appropriate recovery option:** Once you've identified the affected systems and data, you need to select the appropriate recovery option. This will depend on the type of disruptive event and the severity of the damage.
3. **Run the recovery tool:** Once you've selected the appropriate recovery option, you can run the BCDR recovery tool. The tool will automate the recovery process, restoring the affected systems and data to their previous state.
4. **Test the recovered systems and data:** Once the recovery process is complete, you

need to test the recovered systems and data to ensure that they're functioning properly.

Pro tip: It's important to test your BCDR recovery plan regularly with logging and monitoring to ensure that it's working as expected. This will help you identify any potential problems before they occur in a real-world disaster.



Google Cloud services

Google Cloud offers a variety of services that can help businesses implement BCDR plans. Google Cloud categories include Compute, Storage, Big Data / Analysis, and additional Services. Some of the popular Google Cloud services for BCDR include:

- **Cloud Storage:** Cloud Storage is a highly durable and scalable object storage service that can be used to store backups of data.
- **Cloud SQL:** Cloud SQL is a fully managed database service that offers high availability and disaster recovery features.
- **Cloud DNS:** Cloud DNS is a fully managed DNS service that can be used to implement DNS failover.
- **Cloud Load Balancing:** Cloud Load Balancing is a fully managed load balancing service that can be used to implement load balancing failover.
- **Compute Engine:** A Computer Engine is a secure and customizable compute service that lets you create and run virtual machines on Google's infrastructure.
- **Kubernetes Engine:** A Kubernetes Engine cluster has a control plane and machines

called nodes for managing multi-cluster infrastructure and securely running optimized AI workloads.

Note: It's important to understand that Google Cloud services are not a substitute for a comprehensive BCDR plan. Businesses should develop and implement a BCDR plan that's tailored to their specific needs.

Google Cloud Backup and Disaster Recovery (DR)

Google Cloud Backup and DR is a BCDR tool that you can use to back up, recover, and test data on Google Cloud. Google Cloud Backup and DR offers a variety of features that can help your security team implement BCDR plans, including the ability to:

- Centralize backup management for various Google Cloud and hybrid workloads.
- Create application-aware backups, which capture the state of an application and its data at a specific point in time.
- Restore using point-in-time recovery, which allows security teams to restore applications and data to any point in time.
- Automate data replication to multiple regions, which can help protect data using regional disaster recovery strategies, like failover and failback, and be used to improve application performance and availability.
- Create immutable backups, which are protected from deletion. This can help prevent data from being accidentally deleted or corrupted.
- Create testing and development (test / dev) clones of backups, which can be used to test new software or applications without affecting production data.
- Provide reporting and analytics, which can help security teams identify and troubleshoot backup and recovery issues.

Here's one common scenario of how BCDR tools can be used in Google Cloud: A company's security team uses a cloud services provider to host its customer database. To ensure BC, the company uses a BCDR tool—like Google Cloud Backup and DR—to implement a high availability solution for a database.

First, the security team initiates a plan to create database backups on a regular basis on cloud storage. Unfortunately, a disruptive event occurs, and the primary database server fails. Fortunately, the data team is able to use the backup and recovery tool to restore the database to a secondary server. And, the business is able to continue operating with the secondary database until the primary database server is restored and tested to function properly.

Key takeaways

BCDR tools are an essential part of any risk and recovery management strategy. By using the right tools and having a plan in place, organizations can minimize the impact of outages and disasters on their business operations and customer service. Google Cloud offers a variety of

services that can be used to support business continuity and disaster recovery, making it a good choice for organizations of all sizes.