MSP360
MANAGE. SUPPORT. PROTECT.

WHITEPAPER

Protecting Your Org's Google Workspace Data: Why Google Isn't Doing It for You

1-866-4-MSP360
1-415-301-7773
sales@msp360.com
6425 Living Place Suite 200
Pittsburgh, PA 15206
msp360.com

In today's digital landscape, cloud services like Google Workspace have become integral to organizational operations, offering scalable solutions for communication, collaboration, and data management. However, leveraging these services necessitates a clear understanding of the Shared Responsibility Model, which delineates the security and operational duties between the service provider—Google—and its customers.

A critical component of this model is *data backup*, where responsibilities are distinctly divided to ensure data protection, compliance, and business continuity. But where exactly is the line drawn between Google's role in maintaining the platform's functionality and your organization's responsibility to protect the data within it?

This whitepaper explores the Shared Responsibility Model as it applies to Google Workspace, outlines Google's stance on data protection, and provides guidance on best practices to keep your organization's data secure, available, and reliable.

Google's Shared Responsibility Model

When Software as a Service (SaaS) applications emerged, questions arose about the division of responsibilities between service providers and customers. Traditionally, internal IT teams managed on-premises applications entirely. With cloud-based services like Google Workspace, responsibilities are shared.

Google's Shared Responsibility Model clarifies this division:

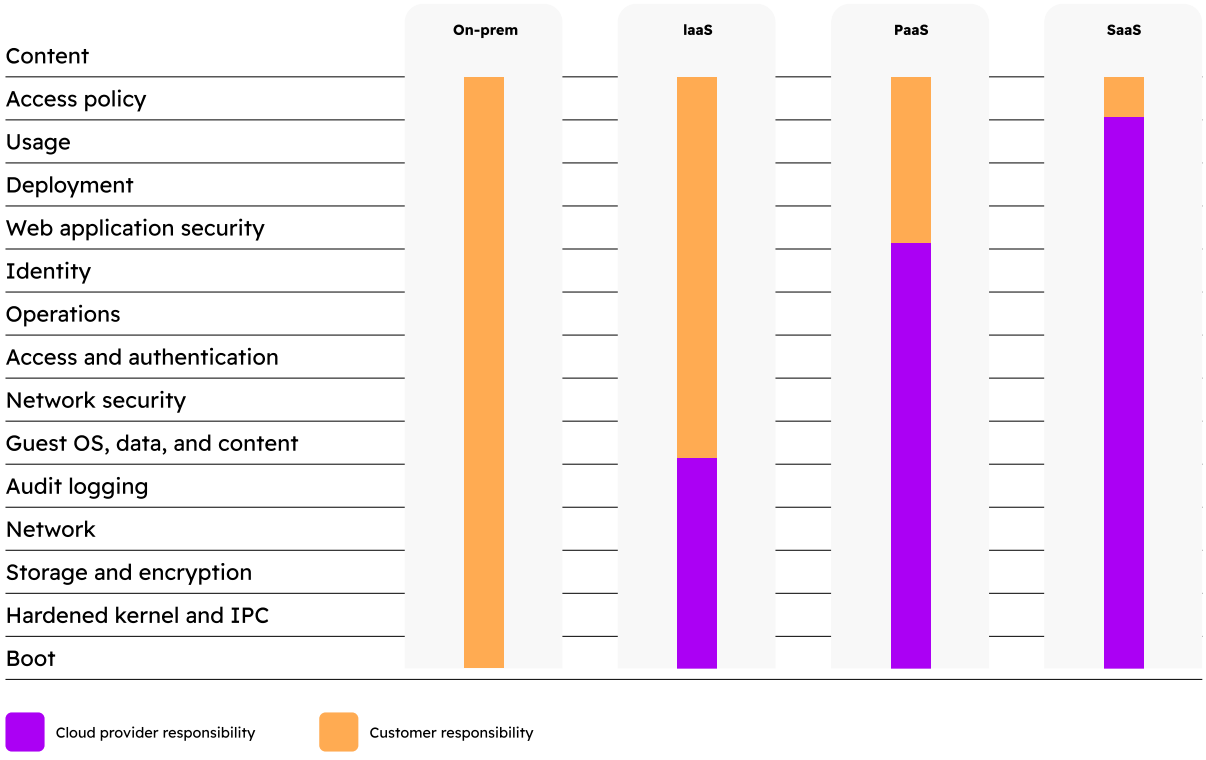

Diagram 1. Source: Google, "Shared responsibilities and shared fate on Google Cloud"

Google's Responsibilities:

As the provider, Google's responsibilities primarily revolve around maintaining the infrastructure and ensuring the availability and security of the Google Cloud services. Key aspects of Google's obligations include:

- **Infrastructure:** Google manages the physical and virtual infrastructure, including data centers, servers, and networking components, ensuring they are secure, available, and reliable.
- **Application Availability:** Google ensures that Workspace applications like Gmail, Drive, and Docs are available and functioning correctly.
- **Platform Security:** Google implements security measures to protect against threats to the platform, including malware detection and prevention systems.

Customer's Responsibilities:

In general, your organization as the Customer is responsible for anything you connect to or store on Google's platform. This includes:

Data Management: Customers are responsible for the data they create, upload, and manage within Google Workspace.

Access Controls: Customers must manage user access, permissions, and authentication methods to ensure only authorized individuals can access data.

Compliance and Backup: Customers are responsible for complying with relevant regulations and implementing appropriate data backup solutions.

What about Backups?

While Google maintains the infrastructure and ensures application availability, it does not provide comprehensive backup solutions for customer data. The do perform backups of your Google Workspace data for their own purposes (like disaster recovery), but these backups have limited retention periods and are not available for customers to use to restore data due to user error or other issues.

According to their Shared Responsibility Model, they differentiate their services from what Customer Data—that is, the content you create (think emails, docs, chats, files, videos, and anything else you create and use anywhere in the Google Cloud) and make the following statement (emphasis added):

> As the diagram shows, the cloud provider always remains responsible for the underlying network and infrastructure, and **customers always remain responsible for their access policies and data**.

It's evident that Google is putting the following responsibilities fully on the shoulders of its' Customers:

- **Data Management:** Customers are responsible for the classification, integrity, and protection of their data within Google Workspace. This involves implementing appropriate data loss prevention policies, ensuring data accuracy, and managing data lifecycle requirements.
- **Data Backup:** Despite Google's data replication efforts, customers are responsible for implementing comprehensive backup solutions to protect against data loss scenarios such as accidental deletions, malicious actions, or corruption. Utilizing third-party backup solutions is often recommended to ensure data recoverability and compliance with organizational or regulatory requirements.

But, wait… doesn't Google native data protection?

Google's Native "Data Protection" Features

Google does offer several native data protection features within their platform, but – as you'll see in a moment – they are far more about simply retaining data than actually protecting it:

- **Data Replication:** Google replicates data across multiple data centers to ensure high availability and resilience against hardware failures. However, this replication is primarily designed for high availability and disaster recovery, not for data restoration in cases of data loss caused by Customer actions.
- **Retention Policies:** Google offers retention policies and recovery features that allow users to recover deleted items within retention timeframes. However, these features have limitations in terms of retention duration and may not fully align with an organization's data retention requirements.

It's important to note that while these features provide a basic level of data protection, they do not replace the need for comprehensive backup solutions managed by the customer.

Additionally, Google does offer two solutions that provide some data protection capabilities:

- **Google Vault:** An archiving and eDiscovery tool that allows organizations to retain, search, and export data for compliance purposes.
- **Google Takeout:** This tool allows individuals to export a copy of the content in their Google Account to back it up or use it with a service outside of Google.

However, none of these features are substitutes for comprehensive backup solutions. They may not protect against all data loss scenarios, such as accidental deletions or ransomware attacks and this is not a comprehensive list of the gaps in Google Workspace backup.

Protecting Your Data: Best Practices for Customers

To effectively uphold your responsibilities within the Google Cloud Shared Responsibility Model, customers should consider the following best practices:

- **Implement Comprehensive Third-Party Backup Solutions:** Deploy third-party backup solutions that offer centralized, automated backup with granular recovery options and alignment with organizational recovery time objectives (RTOs) and recovery point objectives (RPOs). A good example is MSP360 Backup For Google Workspace which ensures cloud-to-cloud data protection, with simple setup and maintenance that supports all core M365/GW components.
- **Enforce Strong Access Controls:** Utilize role-based access controls (RBAC) and enforce multi-factor authentication (MFA) to minimize the risk of unauthorized access that could result in a data breach. Regularly review and adjust permissions as necessary.
- **Educate Users:** Train employees on best practices for data handling, phishing awareness, and security protocols to minimize the risk of data loss as well as potential threats to the organization's data within Google Workspace.
- **Regularly Review Security Strategies:** Periodically assess and update security tools, configurations, and response actions to adapt to evolving threats.

Conclusion

The Google Cloud Shared Responsibility Model delineates the security and operational obligations between Google and its customers. While Google ensures the security and availability of the infrastructure and services, customers must actively manage the protection of their data, standing ready to recover should the unthinkable happen. By fully understanding and embracing their responsibilities, organizations can enhance their security posture and effectively mitigate risks associated with data loss from within Google Workspace.

Here you can learn more about why you need to back up Google Workspace and how MSP360 helps