

the  
**GORILLA**  
**GUIDE**<sup>®</sup> to...



# Data Security Across the Clouds

The Critical Importance of  
Understanding Data Retention  
Policies

**JAMES PANETTI**

# Data Security Across the Clouds

---

By James Panetti

## TABLE OF CONTENTS

---

Introduction.....	3
Policies Drive Behavior.....	4
Data Retention.....	6
Plays Well with Friends .....	8
Password Hygiene.....	10
The Principle of Least Privilege.....	12
Logs and Audits.....	13
When Your Data Is Source Code.....	15
Strong Vendor Relationships.....	17
Powerful Principles.....	18

Copyright © 2022 by ActualTech Media

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

### ACTUALTECH MEDIA

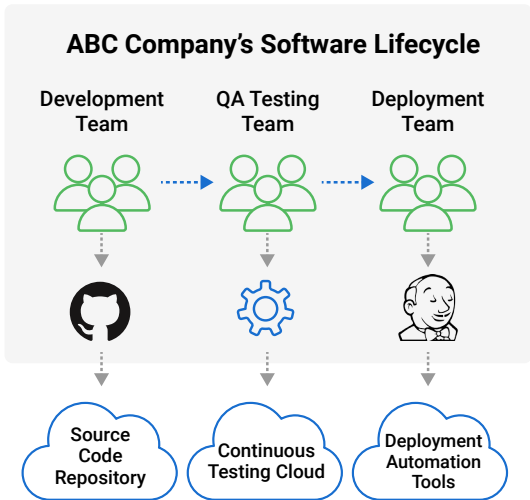
6650 Rivers Ave Ste 105 #22489 | North Charleston, SC 29406-4829

[www.actualtechmedia.com](http://www.actualtechmedia.com)

# Introduction

Over the course of the last decade, more and more enterprises have moved their data into the cloud. Today, as this model has advanced, an organization may often process data through multiple cloud platforms. For example, source code may be stored in an online repository by the development team, continuous testing performed in a Software-as-a-Service (SaaS) environment by the quality assurance team, and deployed to yet another cloud by a continuous deployment team. See **Figure 1**.

Unfortunately, this trend has resulted in a plague of software leaks over the past decade. How can a modern organization utilize multiple cloud solutions across multiple teams, yet still ensure their data is secure across the board?



**Figure 1:** Security has gotten more challenging as data gets more distributed

This Gorilla Guide explores the various ins and outs every enterprise should consider when uploading their data to any type of cloud platform. In addition, it provides information on vendors who have offerings in these areas, to help you when you're looking for a solution.

## Policies Drive Behavior

---

Before discussing any practice, tool, or framework for protecting data, a baseline of agreed-upon behaviors should be in place—otherwise the means for protection hold little value if everyone isn't committed to protection to begin with.

---

**When an organization opts to host or process any of its data in the cloud, airtight policy documentation should lay down the rules of engagement.**

---

Data security—on the cloud or otherwise—relies first and foremost on sound internal policies. Not only must policies exist, but they must be clearly understandable and enforceable, reviewed, audited, and updated on a regular basis to ensure relevance. Organizations such as Gartner Inc. and ISACA, for example, offer services to help policies achieve this goal.

When an organization opts to host or process any of its data in the cloud, airtight policy documentation should lay down the rules of engagement. A data retention policy will ensure no sensitive data is allowed to linger on a cloud platform past its usefulness while a data privacy policy will outline what boundaries will be in place to ensure sensitive data is properly handled.

Some organizations create cloud-specific policies to further define what is and is not acceptable on the cloud, and any such policy should account for the reality of multiple and often interfacing cloud solutions.

When evaluating a cloud solution vendor, you should also carefully review the vendor's own relevant policies and ensure they align with your own policies. Only engage with vendors who have compatible policies, and never expect a vendor to modify their existing policies to align with your own.



## SECURITY POLICY VENDORS

(Note: this is not an exhaustive list, but rather a starting point for vendor research)

### ISACA

- ISACA is an international professional association focused on IT governance

### Gartner

- Gartner is one of the leading analysis firms in the IT industry, and offers a huge range of information around this topic

# Data Retention

---

When reviewing a prospective vendor's policies, their rules governing data retention should be a top priority. Once your data has been uploaded to a cloud platform, it's too late; you are at the mercy of whatever policies the vendor already has in place. It is absolutely critical to have a clear understanding of what circumstances and how long the platform will keep your data once uploaded.

Be careful not to gloss over any aspect of this, for the devil is in the details. Consider that some cloud solutions *store* your data while others may merely *process* your data (only storing it temporarily, until processing completes).

---

**Special attention should be given to how requests for data deletion are handled. How fast and how fully will each cloud vendor delete your data upon request?**

---

For example, data uploaded to an online repository typically remains stored there until you remove it, whereas a software performance testing platform may only pass your data through its systems until the test completes. In the latter case, your data may only exist on a virtual image strictly for the duration of the process's execution.

This is exponentially more important if your organization utilizes multiple cloud solutions, in which case each individual vendor's policy must be reviewed and treated with equal concern. As outlined earlier, your own internal policies should drive what rule you measure these by.

Special attention should be given to how requests for data *deletion* are handled. How fast and how fully will each cloud vendor delete your data upon request? For organizations within the European Union, assurance is granted via the General Data Protection Regulation (GDPR), but for many other organizations, an extra measure of diligence should be taken. How will a vendor verify that your data has been fully deleted once requested? Can they verify that deletion includes any backups that may include your data, as well?



## DATA RETENTION VENDORS

There are many vendors in this space. Here's a sampler.

- **SAP.** Its [Data Warehouse Cloud](#) has a lot of powerful abilities
- **Druva.** Offers full automation capabilities
- **Iron Mountain.** The company's Policy Center manages retention and privacy policies
- **HubStor.** Offers a SaaS-based backup and archival service

Be likewise cautious when closing out an account for a cloud service. Closing, removing, or otherwise deactivating an account doesn't automatically ensure your data is fully deleted, so request verification if assurance isn't already provided in their documented policies.

## Plays Well with Friends

---

It's more common than ever that, within a single organization, many different teams need to move different data through different cloud solutions for different purposes. Needless to say, this can present a data security nightmare if not handled with extreme care. It need not be an insurmountable challenge, however.

---

**Be absolutely certain that you're aware of all parties involved in each cloud service you sign a contract for. Understand how the vendor's policies account for these integrations and what policies each additional party has in place.**

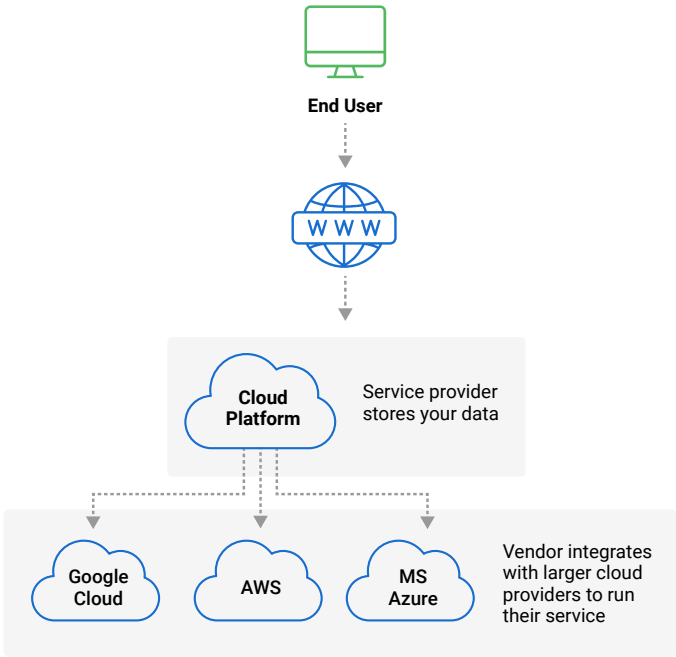
---

Even if you have purchased a subscription to only one cloud service, you may nonetheless be using two or more. For example, a cloud provider's own machines may be virtual machines, pods, or containers themselves hosted by another

third party, such as Amazon Web Services (AWS), Google Cloud, or Microsoft Azure. A provider whose cloud solution you upload data to may in turn store their own data in the cloud. See **Figure 2**.

Be absolutely certain that you're aware of all parties involved in each cloud service you sign a contract for. Understand how the vendor's policies account for these integrations and what policies each additional party has in place.

You never want to learn of these finer details only after a security incident has taken place.



**Figure 2:** Your data may be widely scattered, as in this example, which makes it crucial to understand where your data resides, and on which clouds and platforms

# Password Hygiene

Once your policies and your vendors' policies are sorted, the next item that should be of foremost concern is how your users log in to each service.

All providers have some degree of password requirements that must be met any time a password is created or reset, but keep in mind that you may have stricter internal requirements, in which case your users should be made aware and encouraged to adhere to your stricter requirements.



## PASSWORD MANAGEMENT SOFTWARE

Password management can be done on both a small, local scale and enterprise scale. Some of the leading vendors include:

- **1Password**. A favorite among the Apple crowd, among others
- **RoboForm**. Offers a password manager specifically for business
- **Thycotic**. Has an interesting Office 365 password reset tool
- **Keeper**. Well-regarded in the space

First, each user should create a strong password for each account they use. There are many guides online, but generally speaking, passwords should use some combination of uppercase letters, lowercase letters, numbers, and symbols. Passphrases (in which the password consists of multiple words) are superior to passwords and are typically much harder to crack.

It is imperative—doubly so when multiple cloud services are in use—that each user creates a unique password for every account; in other words, never reuse a password. A common attack is to compromise a third-party site, steal user account details, then test the logins from those stolen accounts on multiple other platforms, relying on reused passwords to expand the scope of what the attackers can access.

Two-factor or multifactor authentication should be required for every cloud service account. This approach, in which the user is provided a rotating, temporary login token each time they log in, adds an extra layer of security by ensuring that even if a password is stolen, it alone will not grant the attacker the keys to your data.

---

**It is imperative—doubly so when multiple cloud services are in use—that each user creates a unique password for every account; in other words, never reuse a password.**

---

Finally, you may want to consider changing the password for each account on each platform on a regular basis, even if the platform itself doesn't require it.

## The Principle of Least Privilege



Another method for protecting data when hosted across multiple clouds with varying policies and security measures is to employ the least privilege principle to all platforms and services that touch your data.

The principle of least privilege, aka the principle of minimal privilege or principle of least authority, is a strict requirement that each user or service that touches data only touches the absolute minimum amount of data needed to perform their designated task. In other words, data is accessed and used on a strict, as-needed basis.

This principle, when fully leveraged, is especially helpful when data is shared, used, or manipulated across multiple entities and platforms.

What each individual, service, or process needs will vary widely from one to another, thus access levels must match these needs accordingly without offering anything more than the minimum required.



## PRIVILEGE-LIMITING SOFTWARE

There's a ton of security software out there, and many offer "Least Privilege" restrictions. Here are a few to help you get started.

- **SecureLink**. There are various versions available, including one specifically for healthcare
- **CyberArk**. The company notes that it was listed in Gartner's "Magic Quadrant" for "Privileged Access Management" in early 2020
- **BeyondTrust**. Another entry in the same Gartner Magic Quadrant, BeyondTrust offers what it calls "Universal Privilege Management"
- **Digital Guardian**. Least Privilege is part of data loss prevention, or DLP, which is a Digital Guardian specialty
- **Ermetic**. A newer security company, focusing heavily on machine and human least-privilege access

## Logs and Audits

Regardless of where your data goes and who or what interacts with it, there should be a digital "paper trail" documenting the journey at all times.

We often take logging for granted until there's a crisis. Every person and service who touches another's data must take responsibility for archiving all interaction. To be clear: Every time data is uploaded, accessed, or processed in any way, that activity must be logged.

Ensure every cloud service you engage with has sufficient logging mechanisms and that relevant logs are available for your own review (what qualifies as "sufficient" is left to your discretion). Always make sure that both you and each provider retain logs for a sufficiently long period of time. Not only must these logs be available to you, but you must be able to access them quickly in the event of an audit or crisis.



## LOGGING AND AUDITING SOLUTIONS

IT security logging and auditing is crucial to your defense posture. These vendors are among those that you should check out.

- **Splunk**. One of the industry's best-known security information event management (SIEM) vendors; logging and auditing is a key part of SIEM
- **ManageEngine**. Its [EventLog Analyzer](#) is a core part of its SIEM strategy
- **Exabeam**. Has what it calls a "security data lake" for collecting huge amounts of log data
- **Netsurion**. Uses real-time analysis of event logs to get out ahead of security issues

This brings us to the topic of audits themselves. Your data and the logs about them should be audited on a regular basis. The frequency is up to you, but audits should be periodic and frequent enough that you're reasonably prepared to respond to a security crisis.

In other words, don't wait until a crisis to review your logs—be familiar with them and the narrative they provide long before any problem occurs. To that end, audits should be performed with an eye for crisis prevention.

Time lost digging through unfamiliar logs is extra time that a security crisis has the opportunity to grow in scope and severity.

## When Your Data Is Source Code



A special word should be said for companies whose sensitive data in question is source code. Most companies today, even if they're not software companies, handle some degree of software development in-house, even if it's only the occasional internal application.

Source code is commonly uploaded to at least one or more cloud platforms to ease the development team's workload. For example, GitHub is a very popular online source code repository. Unfortunately, GitHub, as with many services like it, is a tempting target for attackers looking to steal your source code or any of the secrets that may be stored within it.



## GITHUB INTERNAL SECURITY MEASURES

From the GitHub website:

*Because GitHub encrypts all data in transit, all login information and credentials are always protected. GitHub stores a one-way hash of all user passwords using bcrypt. Your account login is protected from brute force attack with rate limiting.*

Any source code—even the simplest internal app—uploaded to a cloud must be free of confidential information. For example, it is by no means uncommon for a developer to hardcode an Application Program Interface (API) token used to log in to a third-party application in order to communicate with it. The bad news is that if said source code is ever leaked, the attacker will not only have your proprietary code, but any login information stored within it.

Instead of storing authentication tokens, logins, or similar sensitive information within the source code itself, your developers should employ a mechanism to store that information in another secure location, then pass it *through* the code during build or runtime, such as through a variable of some kind.

There are a number of creative methods to achieve this, but the greater point is to ensure that if the worst comes to pass

and your code is ever somehow stolen, then that will be all the attackers achieve, with no further threat posed to the systems that it may integrate with.

## Strong Vendor Relationships



As mentioned earlier, you must know each of your vendor's policies and practices pertaining to proprietary, sensitive, or otherwise confidential data. This relies on having a strong, continuous line of communication open.

Clients often assume that a swift means of communication is in place until an emergency incident proves otherwise. Educate yourself in your provider's policies regarding severity definitions. Understand that what qualifies as a "severity 1" or emergency incident in your organization may not qualify as such in their organization.

A failure to communicate and understand any such differences beforehand often results in panic and unnecessary conflict during an actual crisis. What constitutes an emergency should be agreed upon between all parties long before any such event occurs.

To this end, it's wise to establish a reliable individual contact within the vendor's organization. Most technical support teams have a very strict and rigid process that they must adhere to, even in the event of emergency issues. Expecting a support team to shortcut such a process during a crisis is typically futile.

The better solution is to have a reliable, single point of contact within the vendor organization (typically a dedicated account manager) who you can reach at any time and who can help facilitate work with the support team to ensure you get the kind of response you need. Get well acquainted with your designated contact and have their direct phone number on hand.

## Powerful Principles

---

The ease and frequency with which many parties within a single organization upload data to cloud services makes data security more complicated than ever, but having a multi-faceted plan in place before engaging a single service is key to simplifying threat mitigation.

---

**If you practice each of these principles, you will have laid a very strong foundation to build your online data security upon going forward.**

---

Your own carefully crafted internal policies set your rules. Data retention practices must always be foremost on your mind. Practicing sound password hygiene and implementing the principle of least privilege place multiple layers of protection into place. A service that records and shares logs

pertaining to your data opens the door to your ability to perform audits and prepare for crises before they happen.

All of these factors are made all the easier when you have a strong relationship with each vendor in which expectations are clear and communication is always ongoing.

If you practice each of these principles, you will have laid a very strong foundation to build your online data security upon going forward.

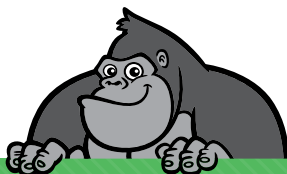
# About ActualTech Media



ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit <https://www.gorilla.guide/custom-solutions/>