PKWARE

pkware.com

Is Sensitive Data Safe in the Cloud?

Best Practices for Security and Compliance in AWS

2021

Cloud providers such as Amazon Web Services (AWS) take responsibility for securing their cloud infrastructure. They also give you tools and support to help you secure the data you put into the cloud. But is that enough to safeguard your organization's most sensitive data?

Whether you are pondering a move to the cloud, already in the cloud, or expanding to multiple cloud platforms, it's time to get a true assessment of your risk and learn how to manage sensitive data in the cloud with confidence.

Contents

Pros and Cons of the Cloud

There Are So Many Reasons to Use the Cloud

Organizations everywhere are tapping the power and efficiencies of cloud computing to reduce IT costs, eliminate data silos, and fuel data-driven business initiatives. Cloud computing providers such as Amazon Web Services (AWS) enable rapid access to a host of flexible, reliable IT resources over the internet, with pay-as-you-go pricing. It's a compelling proposition.

AWS owns and maintains all the network-connected hardware and software, including enterprise-grade servers, storage, databases, and application services. You simply access the computing resources you need, when you need them. You only pay for what you use, typically at a low cost, thanks to the efficiencies of AWS' scale and expertise. Data analysts, for example, can get their big data projects off the ground with the virtual swipe of a credit card—without IT involvement—processing more data faster than ever before.

> The biggest challenges that IT decision makers face when it comes to the ability to take full advantage of their public cloud resources are controlling cloud costs and data privacy and security challenges.
>
> – IDG Cloud Computing Survey 2020

The appeal of the AWS cloud is clear: It allows you to focus on projects that drive value for your business and your customers, not on wrangling the IT infrastructure needed to support those projects. Speed, agility, flexibility, and cost efficiencies are just some of the many business benefits of cloud computing.

Cloud Use is Growing, But Concerns Linger

Still, many organizations are hesitant to use cloud services broadly. Their number one concern is data security, particularly as it relates to compliance with regionally specific and continually evolving privacy laws. For global organizations in highly regulated or brand-driven industries, a data breach or compliance violation could seriously damage consumer confidence and cost millions of dollars in fines, legal fees, and lost business.

Managing data security and compliance is difficult enough in on-premises environments. Even with a plethora of security tools in place, data breaches still happen, and companies still fail audits, all too often. Moving to the cloud is perceived to compound the challenge and, potentially, the risk. In this case, perception is reality.

The Cloud is Being Used, Whether You Know It or Not

That fast, easy access to on-demand computing resources that makes the cloud so appealing can also wreak havoc on an enterprise's data security and compliance efforts. IT teams across the globe are scrambling to understand, rein in, and manage cloud usage by business teams who see the cloud as a way to circumvent slow, onerous IT processes.

Often, the workloads being moved to the cloud contain sensitive data that should be protected, whether the business users know it or not. With enterprise-wide data governance programs slow to take hold, it's doubtful that these users know how to protect sensitive data (in the cloud or otherwise) or even that they are required by law or corporate policy to make the effort.

How can you ensure that your organization's sensitive data—all of it, on a global scale—will be safe in cloud-based environments you don't own? This paper addresses that fundamental question.

> Some organisations have attempted to weed out the use of shadow IT by tightening up governance, but this strategy isn't usually effective. There's a reason shadow IT inevitably crops up in enterprises: it helps people do their jobs.
>
> –Chris Rechtsteiner, Vice President, ServerCentral Turing Group
> *Cloud Tech*, February 4, 2021

Shared Security Responsibility in the Cloud

You Are Responsible for Data Security and Compliance in the Cloud

AWS operates under a "shared security responsibility" model in which AWS is responsible for securing the underlying cloud infrastructure, and you are responsible for securing data workloads you deploy in that cloud infrastructure. Per AWS, it's designed to give you "the flexibility and agility you need to implement the most applicable security controls for your business functions in the AWS environment. You can tightly restrict access to environments that process sensitive data, or deploy less stringent controls for information you want to make public."

Unquestionably, the AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. But it's up to you to control the security of your data inside that AWS environment, as well as ensure compliance with any data privacy regulations that apply to your business operations across the globe.

AWS Gives You Powerful Tools to Define Your Controls in the Cloud

To be sure, AWS has a wide range of offerings to help you with those controls. In fact, practically everything you need to manage data security in the cloud is available to you in AWS, including tools and features for:

- Network security, such as firewalls and encryption of data in transit
- Inventory and configuration management to manage the creation, identification, and decommissioning of AWS resources
- Data encryption for data at rest in AWS storage and database services, with flexible key management and storage options
- Access control, such as identity management and multifactor authentication
- Monitoring and logging, such as API call log aggregation and alert notifications
- API integrations with your own security applications and tools

AWS is responsible for security **of** the cloud.

You are responsible for security **in** the cloud.

AWS even offers guidance and expertise on security and compliance through online tools, resources, support, and professional services provided by AWS and its partners.

As with security, AWS goes a long way to help you be compliant with regard to the physical infrastructure of your AWS environment. AWS publishes and maintains an extensive list of certifications, programs, reports, and third-party attestations to help you assess your risk and compliance in the cloud. Those same "governance-enabling" security features provided by AWS can also help you with compliance in your data workloads. But, ultimately, compliance is your responsibility.

The bottom line is this: AWS is responsible for the data infrastructure; you are responsible for the data. Rephrased from a risk perspective: AWS may be responsible for security *of* the cloud, but you are still responsible for security *in* the cloud.

The Challenge: Protecting the Unknown

To Manage Risk, You Need to Know What You Don't Know

The majority of companies we work with—data-driven enterprises in highly regulated industries that are getting ahead of the problem—have had some unsecured sensitive data on premises or in the cloud that they didn't know was there. It's this sensitive data inadvertently left in the clear that puts you at risk during an audit or breach.

In the age of big data and the Internet of Things, data is being generated constantly in unfathomable volumes. What if there are people in your enterprise putting sensitive data into the cloud without your—or their—knowledge? How do you keep up with security and compliance? What if you're breached between audits?

Some organizations know, or at least suspect, that there is unsecured sensitive data within a larger data repository, such as a Hadoop cluster or an Amazon S3 bucket. Instead of going through a very manual and analytical (i.e., costly and time-consuming) process to find the sensitive data and secure it, they lock down the entire dataset, much to the frustration of users. Risk may be minimized, but so is the value of all that data.

Protecting Sensitive Data in the Cloud Requires More Than Security

The biggest challenge, then, is not that of securing the sensitive data that is known to you. There are many ways to protect your sensitive data assets in the cloud, and there are many security tools that can be applied appropriately based on the sensitivity and use case. For example, you can use data masking to protect privacy while still preserving broad usability, or you can encrypt data to tightly control access.

The biggest challenge is finding sensitive data when its existence or location are unknown to you so that you can make fully informed, risk-based decisions about data security and compliance in light of your business goals. It is identifying the gaps in your security and compliance efforts. Masking and encryption can only be effective if you know exactly what to mask and encrypt. Access monitoring is only effective if you can monitor precisely what needs to be monitored. It is governing, not just securing, sensitive data that will give you the freedom to take on new cloud-based initiatives that will fuel innovation and growth for your business.

Sensitive Data Discovery and Protection

Visibility and Automation Are Key to Cloud Governance

Protecting sensitive data in the cloud involves managing both the known and the unknown. You need the ability to discover sensitive data that exists in your cloud environments as well as detect sensitive data as it enters (and leaves) your cloud environments. If you're migrating data from an on-premises environment to the cloud, you can secure it beforehand or upon ingest, but you still need to know it's there. This visibility is critical to successful data protection, and it isn't possible without automation.

The days of manually searching for, locating, and securing sensitive data are over. Today, the sheer volume, variety, and velocity of data make for an elusive target. Now, your IT arsenal must include a solution for automatic discovery of sensitive data, including common types (e.g., names, emails, credit card numbers, Social Security numbers, birth dates) and uncommon types that may be specific to your business (e.g., fingerprints, health IDs, military records). Accuracy is important, lest you waste cycles on non-important data and neglect truly sensitive data, missing the point of governance entirely.

Take Responsibility of Sensitive Data in the Cloud

To operate safely in the cloud, you must be able to take total responsibility of your enterprise's sensitive data—on premises, in the cloud, and everywhere in between. What's needed is a solution for sensitive data discovery and protection that provides control and visibility of all entities involved in managing sensitive data security and compliance.

The solution must be:

- **Comprehensive**, covering all data types and platforms, and all user profiles and roles, across the entire data lifecycle—from on premises to cloud to multi-cloud environments
- **Automated**, to keep up with data explosion on a global scale

The solution must deliver automated capabilities that make it easy to:

- Define policies for data security and compliance purposes
- Discover, detect, and inventory sensitive data continuously in real time
- Mask or encrypt sensitive data at rest
- Dynamically encrypt and decrypt sensitive data
- Enforce access policies for sensitive data
- Monitor access patterns around sensitive data to identify potential breaches and adjust protection and access policies in response

The solution must provide dashboards that enable CIOs, CISOs, and CDOs to:

- Understand sensitive data protection status and exposure, including an inventory of people who currently have access to sensitive assets
- Identify gaps in sensitive data protection coverage, including masking, encryption, monitoring, and access policies
- Visualize the overall coverage and progression of sensitive data-related processing, to identify trends, anticipate needs, and assess risk

You probably already have technologies in place that will play a role in your overall data governance framework. Whether you are pondering a move to the cloud, on the verge of moving to the cloud, or already in the cloud, it's time to take responsibility of sensitive data, fill in the gaps, and get a true assessment of your risks.

The Cloud is Safe. Are You?

Is Sensitive Data Safe in the Cloud?

The answer is: It's as safe as you make it. Treated equally, it's no less safe than data on your own premises, and perhaps safer, provided you've taken the right steps. How confident are you that the sensitive data—all the personal, health, financial, and other confidential information subject to legal scrutiny—in your cloud workloads is appropriately protected?

Yes, cloud providers give you tools and support to help you secure the data you put into the cloud, but it's still your responsibility to know (1) what sensitive data exists in the cloud and where, and (2) how to safeguard it and comply with regulations—while still extracting maximum business value from it. To live up to that responsibility, you need a solid strategy and solution for sensitive data discovery and protection.

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance.
To learn more, visit PKWARE.com.

PKWARE

PKWARE.com

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI