PKWARE

pkware.com

Securely and Selectively Migrating Enterprise Data To the Cloud

2021

Contents

- Security Lacking in Advancing Technologies
- The Inherent Difference of Security in the Cloud
- Shared Security Responsibility Model
- Selectively Migrating Data To the Cloud Using PK Protect
- Moving Sensitive Data To the Cloud

Security Lacking in Advancing Technologies

Enterprises today are amassing more data than ever before. Although the value and impact of this data can be seen through powerful analytics, there were many challenges getting to where we are today. Specifically, when we talk about storage, costs and scalability were major hurdles that motivated the creation of big data technologies. But when you factor in reliability and high availability, the developers combating these challenges became oblivious to the security issues at hand. Thus, came about highly cost-effective technologies for storing data but with meager security guarantees.

The advent and adoption of big data technologies was then contingent on how well the security industry could catch up. Industry leaders like PKWARE played a huge role in accomplishing this. However, even though the Hadoop ecosystem and its landscape of security matured, the spotlight was soon stolen by the Cloud, as it offered compute power and even cheaper storage.

The Inherent Difference of Security in the Cloud

One of the biggest barriers for enterprises to migrate to the cloud has been the lack of a comprehensive and reliable security solution. Even early on, experts raised serious questions on the security of data in the cloud, and there is a great reason to back up this apprehension. Before the cloud, all enterprise data was typically stored on data centers owned and maintained by the enterprise itself. It is widely accepted that enterprises can collect sensitive data as long as it resides in an environment that they can protect and ensure complete compliance with PII, PCI, HIPAA, and other standards.

This meant that enterprises prioritized their resources on strengthening the network perimeter and tightening access control. However, to move data to the cloud, enterprises faced a new dimension in their security challenge—to ensure that no PII, PCI, HIPAA, or data complying with a similar policy could leave their on-premises environment. And this is the inherent security challenge for a cloud environment—before data can be migrated over to it, all sensitive data must be secured.

Shared Security Responsibility Model

When designing security solutions, it is imperative to understand the scope of what each party will be responsible for. The cloud vendors who have built this massive infrastructure and invested immense resources in it obviously want to create a secure environment, so, from an infrastructure perspective, they took upon the responsibility of providing the customers with a secure environment. However, when enterprises move their data into the cloud, the ownership of the data is still with the enterprise itself. The cloud vendors therefore do not take responsibility of securing the customer data inside the cloud.

This is the shared responsibility model, whereby the cloud vendor manages security of the Cloud, but the customer manages security in the cloud. What this implies is that before an enterprise can move its data to the cloud, it must ensure that all sensitive data is obfuscated or left on premises.

Selectively Migrating Data To the Cloud Using PK Protect

Enterprises today have so much data and so many different requirements to use their data that there is a high variability in how data is collected, where it is stored, and how it is used. Within an enterprise itself, there can be a large scale verticalization of data. Different departments can choose to handle their data differently, and even within that scope, different datasets within that department can be subjected to varied processes and procedures. The ramifications of such variability are that enterprises cannot just forklift their entire data repository to the cloud. They require much finer control on how and when they can do so.

PK Protect offers the ability for enterprises to detect, audit, protect, and monitor data across Hadoop, databases, and file shares at the element level. It uses a single dashboard to run tasks and display reports. The dashboard can identify the exact location and counts of sensitive data content, how much of it is secured (through

masking and/or encryption), and whether any unauthorized users are accessing it. This allows the users to segregate their data and run detection and protection processes over time, as it may not be possible to plough through the entire data repository all at once. Sometimes it may not be possible for an enterprise to have their entire database comply with the required policy like PCI, PII, and HIPAA, so when PK Protect empowers these enterprises to selectively protect their data, they can choose to securely migrate

Moving Sensitive Data To the Cloud

On-premises datacenter			Cloud	
Production	Copy of Production			
PK Protect Server	Staging	Staging		
STEP 1 PK Protect connects to on-premises database	STEP 2 PK Protect detects and masks sensitive data	STEP 3 “Masked” data is ready to be moved	STEP 4 Users are given access to database in the Cloud	STEP 5 Developer can access masked data

About PKWARE

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.

Enterprise-Wide Policy Management

The PKWARE Enterprise Manager provides a single point of control for data protection activity across the entire organization

Simple Workflow

With PKWARE, data protection is automated for end users and easy for administrators to manage

Easy Implementation

PKWARE supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure and workflows

Protection Without Gaps

PKWARE works on every enterprise operations system and provides persistent protection that remains with data even if it's copied or shared outside organizations

Integrated Discovery, Classification, and Protection

No other solution has the capability to find, classify, and protect data in a single automated workflow

Multiple Protection and Remediation Options

Organizations can take a policy-based approach to data protection and choose from action including persistent encryption, quarantine, masking, and deletion.

BOOK A DEMO

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 53204

NASSCOM ISO 27001 ISO 9001 Silver Microsoft Partner