Use Case

Simplify Cloud Compliance

For Banking & Financial Services

> “Minimize reliance on third-party CSPs for protecting payment card data”
>
> PCI DSS Cloud Computing Guidelines – PCI SSC

SecureDoc™ by WinMagic

WINMAGIC®

Cloud adoption in the banking sector is expected to ramp up substantially, from zero use of infrastructure as a service to as much as

30%

Of workloads to public cloud within three years according to Deutsche Bank Researchers in 2016[1]

> “The growth in cloud platforms raises security challenges as data moves among multiple cloud platforms[2]

Sources

1 Big Banks Starting to Embrace Pub-lic Cloud, Deutsche Bank Says – Wall Street Journal 2016

2 The Cloud Security Market Grows From $1.5 Billion in 2017 to $3.5 Billion in 2021 – Andras Cser and Jennifer Adam (Forrester 2017)

3 FINRA Case Study – AWS 2016

Financial Services are Embracing Cloud

Across the financial sector, there is unprecedented demand to optimize, accelerate and automate every aspect of business. Merchants, banks, and payment service providers are running hundreds of applications from transactional processing to low-latency trading – hard pressed to accommodate the sheer volume and constant flux in demand for data processing and storage.

Despite hesitation by large banks and financial services to move to the public cloud, adoption is expected to grow following FINRA (Financial Industry Regulatory Authority) which moved about 90% of its data stores to AWS.[3] Innovative organizations, from fintech startups to international banks, have realized the need for a shift from existing on-prem infrastructure to a hybrid model involving one or more infrastructure as a service (IaaS) solutions. Embracing cloud as part of their overall datacenter strategy enables them to meet heavy demands while improving cost efficiencies.

But Compliance is Complex

But as innovators in the financial sector expand their cloud footprint, they must pay close attention to the jurisdictions where their data is stored. For instance, a U.S. bank can be subject to multiple regulations, including federal laws, like the Sarbanes-Oxley Act (SOX) and the Gramm-Leach-Blilely Act (GLBA) – in addition to the Payment Card Industry Data Security Standard (PCI-DSS) set by the credit card companies, and state-level laws like the New York Cybersecurity Requirements for Financial Services Companies.

Beyond that, businesses operating globally must consider the European Union’s General Data Protection Regulation (GDPR), which introduces data residency and privacy concerns, with exponentially higher penalties for non-compliance. That said, banking and financial regulation is a labyrinth. Navigating compliance in virtual and cloud environments, spanning multiple jurisdictions, where regulations are continuously evolving, is no easy task.

95%

Of financial organizations are primarily concerned with security and privacy of data in the cloud[1]

> “If a security failure does occur, questions about the use of encryption are virtually inevitable. It most certainly helps avoid negative attention in the case of data breaches – leaked encrypted data is not a meaningful exposure, while leaked clear-text sensitive or confidential data can result in severe loss[2]

Sources

1 Netwrix 2016 Cloud Security Survey – Netwrix (2016)

2 CISO Playbook: How to Retain the Right Kinds of Control in the Cloud – Gartner (Mar 2017)

Business Need: **Security, Privacy & Control**

Merchants, banks, payment service providers and others that play a role in processing payments must protect the privacy of cardholder and account data. But when that data resides on diverse sets of virtual machines, containers or databases across integrated private and public datacenters, with high degrees of automation – knowing how that data is protected, where it resides and who has access is critical – both to meet business goals and to comply with PCI-DSS, EU GDPR and other regulatory obligations.

The Problem: **Cloud Risks & Compliance Gaps**

With GDPR compliance looming, PCI DSS evolving, daily breaches and cyberattacks, and increasing customer privacy concerns, protecting data in the cloud has never been more critical. That said, IT decision makers in the financial sector are faced with varying security capabilities across different virtualization, cloud and hardware vendors, with little to no cross-platform visibility. Without a unified approach to cloud security, organizations face serious risk and gaps in compliance, including:

Data Breach
Sensitive cardholder and account data stored in plain-text are vulnerable to loss, theft or exposure in the cloud.

PCI Recommendation: “Strong data-level encryption should be enforced on all sensitive or potentially sensitive data stored in a public cloud”
PCI Cloud Computing Guidelines

Loss of Control
Strong cryptography is recommended to protect sensitive cardholder and account data, but without control of keys, data is still at risk.

PCI Recommendation: “Because compromise of a CSP could result in unauthorized access to multiple data stores, it is recommended that cryptographic keys used to encrypt/decrypt sensitive data be stored and managed independently from the cloud service where the data is located”
PCI Cloud Computing Guidelines

Data Sprawl
Even sensitive workloads restricted to the private datacenter can easily leak to unprotected environments, leading to unmanageable risk scenarios and conflicts with data residency under EU GDPR.

PCI Recommendation: “As well as being present in known locations, cardholder data could exist in archived, off-line or dormant VM images, or be unknowingly moved between virtual systems via dynamic mechanisms such as live migration or storage migration tools”
PCI Virtualization Guidelines

Siloes & Security Gaps
Security solutions – including encryption – tied to a specific cloud service provider, hypervisor or dedicated hardware appliance create siloes in risk management and gaps in security between different environments.

PCI Recommendation: “The use of disk encryption may be subject to specific virtualization-related implementation issues which could render encryption ineffective. For example, moving or migrating encrypted VM images, containing cardholder data, to another host, VM image, or removable media could disrupt the effectiveness of the encryption mechanism”
PCI Virtualization Guidelines

The Solution: **Simplify Cloud Compliance with SecureDoc CloudVM**

As banking and financial regulations and data residency concerns drive the need for cloud compliance, CIOs and IT decision makers need a solution that provides visibility and control over all virtual servers and desktops running on-prem or in the cloud. They need a security approach that enables their organization to take full advantage of the cloud – capable of making cloud workloads just as secure as those residing within their own datacenter.

SecureDoc CloudVM provides FIPS 140-2 validated encryption and strong cryptographic key management to support requirements for protecting personally identifiable information (PII), account data and cardholder data under multiple regulatory standards, particularly PCI-DSS and EU GDPR.

Protect Cardholder Data

Meet PCI DSS Requirement 3 to protect all stored cardholder data, whether it resides in a public, private or hybrid cloud environment. SecureDoc is designed to encrypt and travel with the VM from spin up to spin down, including migration, replication, backup and disaster recovery – even snapshots.

Lock Down Systems

Support PCI-DSS requirements to secure and authenticate access to systems (Requirements 6 & 8). With SecureDoc, virtual server and desktop instances will not boot without keys provided from enterprise-controlled key management server.

Control Workloads

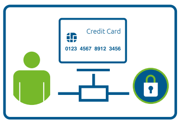
Strengthen access controls to cardholder data (Requirement 7) and prevent data residency conflicts under EU GDPR. CloudVM enforces geo-fencing and IP-blocking controls, as well as clone restrictions right at boot time to prevent data sprawl.

Protect stored cardholder data

Develop and maintain secure systems and applications

Restrict access to card-holder data by business need to know

Identify and authenticate access to system components



Track and monitor all access to network resources and cardholder data

Track & Monitor Access

Discover and track VMs across all cloud providers, subscriptions and regions to simplify audits and support PCI-DSS Requirement 10 to track and monitor access to all cardholder data and network resources.

Protect & Control Keys

Align with PCI Virtualization and Cloud Computing Guideline recommendations to manage and store keys independent of your CSP. CloudVM also ensures that keys are only delivered when policy allows, supporting PCI DSS mandates to protect, limit and restrict access to keys.

Eliminate Security Gaps

Deploy encryption that remains effective from the moment a VM is created to the time it's securely disposed of. CloudVM assures protection of VMs as they're moved to another host, image or even copied onto removable media.