White Paper

Protecting Sensitive Data and Achieving Compliance in a Multi-cloud World

ENTRUST

SECURING A WORLD IN MOTION

Keeping up with security and compliance requirements in a post-single-cloud world

On May 25, 2018, the new General Data Protection Regulation (GDPR) went into effect in the European Union (EU) with sharper teeth than any other compliance regulation to date. With tighter controls and higher penalties, the new compliance law has changed how organizations enforce data protection and handle private data. While other compliance regulations, like Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Standard (PCI), have ratcheted up their rules and enforcement in recent years, it's highly likely the GDPR will remain the standard that other regulatory bodies will be inspired or compelled to mimic.

This compliance sea of change will make today's accelerating move to multi-cloud environments that much more challenging for organizations – especially since many clouds aren't even ready for the GDPR. According to the June 2016 Netskope Cloud Report on readiness in the cloud, as much as 75% of all cloud apps used in enterprises are out of compliance with the new rules. To keep data safe and remain compliant, every organization must ask themselves: How will we comply with our industry and legal regulations across our multiple cloud platforms? This document provides insight and data security best practice recommendations.

How will you protect your sensitive data in a multi-cloud future?

Our business world demands high speed and agility – and the cloud delivers on these demands and more. In fact, the advantages of cloud platforms, services, and applications are too enticing for most organizations to ignore. So much so that one cloud platform isn't agile enough for their ever-expanding business needs. They need multiple clouds to gain the functionality and availability their business objectives demand. As a result, the percent of organizations working in multi-cloud environments today is on a rapid incline.

Multi-cloud means that an enterprise is using two or more public and private cloud services, platforms, or applications in a single heterogeneous architecture. Public clouds are owned and operated by third-party service providers like Amazon Web Services (AWS), Microsoft (Azure), IBM (SoftLayer), and others. Customers of these cloud providers gain the capabilities they need along with economies of scale because infrastructure costs are spread across all users. The benefits are undeniable, including agility, speed, cost savings, scalability, and specialty capabilities, to name a few.

As more business needs are met with cloud offerings, it's clear that multi-cloud is rapidly becoming the dominant IT model of the future. But, along with delivering significant business advantages, this model comes with challenges, including data security, which has emerged as the topmost concern. As a result, organizations expanding into multi-cloud must find reliable solutions for securing the sensitive data they own, such as personally identifiable information (PII), consumer financial data, patient health information (PHI), product-related data, confidential government data, and much more.

MULTI-CLOUD USE ON THE RISE

Adoption of multi-cloud environments is on the rise. A study conducted by Entrust of more than 400 attendees at VMworld 2016 found that 64% expect to use multiple cloud service vendors.

Complicating multi-cloud deployments is the fact that most organizations are required to comply with an ever-expanding regime of increasingly stricter industry- and government-mandated regulations across all cloud environments. Unfortunately, many organizations have not adequately addressed these regulations yet, which is placing their data at risk of breaches and their organizations at risk for severe penalties.

The reality is clear. Our multi-cloud world is creating enticing opportunities, but also serious questions with few easy answers, including:

- What does it mean to have your data spread across multiple cloud platforms?
- Do you know where all of your sensitive data resides today? Tomorrow?
- Can you retain control of your sensitive data across multiple clouds?
- Who owns data security and compliance in the cloud?
- Who is liable if a data breach occurs in the cloud?
- Are you prepared to meet and prove compliance to your auditors?

The following sections of this document address critical multi-cloud challenges – and share insights that provide clear guidance for every organization working in or moving to a multi-cloud environment.

The multiple risks of noncompliance

Noncompliance of industry and government data security regulations can result in several significant problems, including:

- Vulnerability to hacker attacks and security breaches
- Inability to protect organizations and meet compliance requirements
- Noncompliance fines, fees, legal costs, and sometimes jail time
- Loss of end-user or public confidence, resulting in negative publicity
- Organization devaluation by business rating organizations
- Inability to recover records or funds, rendering it impossible to conduct business
- Loss of customers to competitors
- Closure of departments or entire business

How are regulatory bodies responding to multi-cloud security risks?

When an organization makes the decision to outsource its infrastructure to a cloud service provider (CSP), it also makes the decision to hand over some level of control of its data to a third party. In fact, many organizations are moving data to multiple clouds without a clear understanding of how their data will be safeguarded and governed outside of their business walls. This introduces multiple data security and compliance uncertainties and can potentially put organizations in a dangerous position. The danger spikes several degrees higher for heavily regulated organizations and those handling EU citizens' data, where privacy is governed with a heavier hand than in the U.S.

In response to escalating external and internal threats and uncertainty, lawmakers and regulators around the world are strengthening their data security compliance requirements, implementing new legal frameworks, and exacting higher noncompliance penalties. This places organizations at tremendous risk for compliance violations, along with the resulting fines and remediation costs.

Compliance challenges are particularly relevant when working in the EU. Its 28 countries have some of the strongest data residency and privacy regulations in the world to protect citizens' data. The more than 100 national data privacy laws on the books impact any organization that deals with EU citizens' PII, including U.S. organizations. Consequently, meeting data residency and privacy regulations can become a great challenge for global enterprises working in several countries and with several cloud providers.

Among the EU regulations is the rule that all customer and employee data must not be accessible to anyone outside of their home legal jurisdiction, except when given explicit consent on a per usage basis. European countries are especially troubled by the fact that U.S.-based cloud vendors can be subpoenaed by U.S. governments to provide access to specific information, even if it resides outside of the U.S.

With the GDPR, the EU is working to unify and strengthen the data protection of its citizens' data even more. Every organization is forced to comply or face penalties, including incurring damaging fines and even losing the opportunity to work within the EU.

While security and data compliance on multiple clouds may be murky, it's crystal clear that if organizations want to leverage the benefits of multi-cloud environments, they need to understand how to securely manage the distribution of their sensitive data across multiple cloud vendors. This means understanding their share of the cloud's "shared responsibility model."

Two categories of data compliance regulations

Data compliance regulations fall into two broad categories:

1. Data privacy and residency legislation
Laws in specific states, countries, and government associations, such as the EU, dictate that sensitive or private information may not leave the physical boundaries of the country or region (residency), and that the information should not be exposed to unauthorized parties (privacy). The primary example is the newly ratified GDPR in Europe.

- GDPR. This compliance regulation was created to solve the confusion and inefficiency created by the patchwork of data protection laws that currently exist across Europe. It replaced the 20-year-old Data Protection Directive when it went into full effect in May of 2018.

2. Industry-specific compliance requirements
These are laws or mandates covering a specific industry, type of business, or government agency, which prescribe the appropriate treatment and security of private or sensitive information. Examples include:

- Payment Card Industry Data Security Standard (PCI DSS). The PCI regulation requires privacy protection of cardholder information. To comply, organizations need to secure cardholder data.
- HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH). These regulations require Electronic Patient Health Information (ePHI) to be secured and access to be controlled.
- National Institute of Standards and Technology (NIST) Special Publication 800-53. This requires organizations to maintain specific security controls on Federal information systems.
- Federal Risk and Authorization Management Program (FedRAMP). This government-wide program provides standards for cloud security.
- Federal Information Processing Standard (FIPS) Publication 140-2. This specifies the security requirements that must be satisfied in cryptographic-based security systems.

What's your share of multi-cloud's "shared responsibility model"?

While some organizations have decelerated their move to multi-cloud because of security and compliance challenges, others have enthusiastically entered this new environment with unrealistic expectations. They assume their cloud providers are 100% responsible for the security and compliance of their data. But the reality is that organizations cannot outsource their data security and compliance responsibility to third-party cloud providers. Depending on the type of cloud service procured, organizations may be able to outsource some security controls, but overall responsibility and accountability clearly rests with the organizations themselves.

Because the unique nature of cloud computing places different obligations on CSPs and their customers, Amazon Web Services pioneered a model to bring structure to public cloud computing, also known as the **shared responsibility model.** Simply stated, this model breaks down data security and compliance responsibilities as follows: CSPs are responsible for security and compliance of the cloud. Organizations are responsible for compliance and security in the cloud. Specifically, this means:

- CSPs are responsible for the security and compliance of their cloud-based infrastructures, including computing, storage, databases, and networking.
- Organizations are responsible for the security and compliance of their own data, networks, applications, and operating systems that live in the cloud.

What does the shared responsibility model mean for organizations that currently use or plan to adopt a multi-cloud infrastructure? It means they must understand how the model is structured with each of their cloud vendors, because no two cloud providers operate in exactly the same way. Further, organizations must understand that this model is not static and will most likely shift as new cloud paradigms are introduced, such as containers. The bottom line is that if organizations don't have their share of the shared responsibility model nailed down, it's the equivalent of sitting in a well-built, fortified castle with the gates wide open.

Three non-negotiable security best practices for your multi-cloud world

The challenge for organizations is to find effective ways to protect their data and meet the ever-expanding list of regulatory mandates without forfeiting the countless benefits offered by multi-cloud deployments. This section examines three data security best practices that can ensure data is protected and compliance standards are upheld across multi-cloud environments – encryption, key management, and key ownership.

Best practice 1 – Block prying eyes by encrypting data at rest

The HIPAA/HITECH Act categorizes encryption as an "addressable" regulation, meaning that each organization can determine if encryption is a reasonable and appropriate safeguard for managing risks to the confidentiality, integrity, and availability of electronic patient health information (ePHI). However, any organization that decides encryption is not necessary must document its rationale. That rationale must be deemed acceptable by HIPAA if the organization ever experiences a data breach. The catch is that it's difficult, even impossible, to imagine a scenario in which it would be "reasonable and appropriate" to elect not to use encryption to protect ePHI.

Encryption at a glance

Encryption is a mechanism used to protect data by transforming information into an unreadable format so it remains private from anyone or anything not approved to read it. An individual or application that needs access to encrypted information must possess the correct secret code – called a "key" – to convert the data back to its original readable format. In this way, encryption provides a fail-safe mechanism where, if all other security measures fail and data is stolen, the information is still protected.

There are three methods of encryption: data at rest, data in transit, and data in use. While all are important, we'll focus on data at rest. For a hacker, data at rest – such as data in databases, file systems, and storage infrastructures – is much more attractive than data in transit, which is individual data packets crossing the network. Data at rest tends to have logical structures, meaningful file names, or other clues that let hackers know this data is valuable – for example, credit card data, intellectual property, personal information, healthcare information, or financial information.

When it comes to data at rest in the cloud, there are several categories of threats that organizations must consider – and encryption is the first step in addressing these threats:

- Cyber-attacks – hackers compromise a cloud service and gain access to organizations' data that is being processed by or stored in the cloud
- Insider threats – malicious or rogue administrators steal physical disk drives or servers containing data in the cloud
- Government threats – agencies use subpoenas or patents to get access to a customer's data in the cloud without their knowledge

Many headline-generating data breaches shed a glaring light on these risks because either the stolen data was not encrypted or the encrypted data was compromised through unauthorized key access. For example:

- Marriott in 2020 lost 383 million records due to hackers obtaining login credentials
- BlueKai, owned by Oracle lost over a billion records due to data not being password protected or encrypted
- Microsoft, lost 280 million customer records after a database was left unprotected on the internet.

Even though encryption is one of the most effective ways to maintain the integrity and security of data in the cloud, many organizations fail to adequately encrypt data at rest. A study conducted by Entrust found that 28% of the respondents don't encrypt their data in the cloud at all. This will undoubtedly change with the mounting regulatory pressures to encrypt data at rest – from NIST to PCI to HIPAA to the upcoming GDPR. While not all regulations require encryption, many regulations provide an organization with a "safe harbor" if their compromised data was encrypted.

CSPs are also falling short when it comes to protecting data through encryption. According to a study by Skyhigh Networks that assessed over 12,000 CSPs – only 9% had encrypted data stored at rest in their environments. In fact, some of the biggest names in cloud computing don't encrypt stored data. That's unnerving when you consider that the cloud is now home to a significant amount of sensitive personal, corporate, and military data. This reality reinforces the imperative that organizations must find solutions for securing their own data at rest rather than assume they can leave it in their cloud providers' hands.

Still, encryption alone is not enough. And the days of auditors simply accepting the use of encryption "as good enough" are numbered. As compliance mandates and privacy obligations evolve, the spotlight is beginning to turn from basic encryption to the specifics of key management in the cloud.

Best practice 2 – Micro-manage your encryption keys – from creation to destruction

When the updated PCI security standards took effect in January 2014, the guidelines represented a sweeping attempt to "move organizations from mere compliance to more comprehensive security approaches built on Shared Responsibility." Because of this, the requirement to have a clearer and stronger focus on effective encryption key management is now a critical part of PCI. Moreover, PCI is not alone as more and more regulatory bodies also add language that explicitly addresses specific phases of the key management lifecycle, such as the storing and rotation of encryption keys.

The rationale behind this compliance trend is based on the recognition that even the best encryption practices are only as good as an organization's ability to protect the encryption keys. In encrypted environments, keys effectively act as proxies for the data they protect. So if the keys are compromised, so is the data. Put more simply, keys are the equivalent to the series of numbers that open the combination lock of a safe. If a thief knows a safe's combination, even the strongest safe in the world provides no real security. Similarly, poor or no key management can easily compromise the strongest encryption, because with the right keys, any attacker can access the underlying data.

In view of the critical role encryption keys play in securing data, organizations must be able to efficiently manage keys throughout the key lifecycle, including the ability to generate, distribute, store, rotate, and revoke/destroy keys as needed. PCI, for example, requires organizations to rotate encryption keys once per year, because if the same key is used over a long period, the risk of that key being compromised increases. Correspondingly, the longer a key is in use, the amount of data it protects increases and, therefore, so does its value to an attacker. Key rotation is just one example of the type of tasks that require continuous and vigilant administration. But the same rigor applies to all of the other phases of the key management lifecycle, such as storing and revoking keys, etc.

FIPS 140-2 – The highest encryption standard

In the U.S., one of the most rigorous encryption standards is the Federal government's FIPS 140-2. If a product has been FIPS 140-2 validated, it has been tested and formally validated by the U.S. and Canadian governments and meets the following three criteria:

- Uses an approved algorithm
- Manages encryption keys appropriately
- Handles data to be encrypted in a specific way – with a precise block size, amount of padding, and some degree of randomness – so the cipher text cannot be searched

The big challenge that organizations face is that key management is typically considered so operationally complex that it's often referred to as the "Achilles' heel of encryption." The complexity is, of course, magnified in a multi-cloud environment, where organizations are now expected to manage keys across multiple clouds. The more cloud platforms an organization is managing, the more keys they have in use, and the more complex key management will become – not a simple task for even the most sophisticated IT and security teams. If organizations are going to successfully move forward with a multi-cloud strategy, they should consider key management solutions that will enable them to automate the administration of all critical tasks associated with the key management lifecycle – without disrupting or impacting the daily IT operations that support the business.

While the function of encryption and key management in a multi-cloud environment is straightforward, the more important question of who owns and controls the encryption keys in these environments is not.

Best practice 3 – Control your encryption keys and you control your kingdom

NIST states specifically that to "maintain best practices and pass audits, organizations should manage their keys in the custody of their own enterprise or that of a credible service from a cryptographic service provider." What this means is that organizations must maintain complete control of their encryption keys and not give any cloud provider access. NIST is not alone in this requirement. Many regulations restrict key access to only privileged users who are supposed to have access to the encrypted data. This security measure breaks down in multi-cloud environments when organizations relinquish control and give cloud providers ownership of their keys.

The question of who has control of the encryption keys is paramount to any organization's data security and compliance strategy. In fact, the location of an organization's keys – who has access to them and who has control of them – is almost as important as encrypting the data in the first place.

Regulatory bodies recommend data encryption

Officers, auditors, and regulators within compliance entities share a strong consensus that properly applied encryption is a critical component of maintaining compliance, including these three examples:

- PCI regulations require organizations to fully encrypt sensitive cardholder information with strong encryption methods.
- HIPAA sets out numerous examples of encryption methods that can be employed, along with factors to consider when implementing and ensuring the success of a HIPAA encryption strategy.
- Data breach disclosure and notification laws, such as the UK Data Protection Act, vary by jurisdiction. But most include a "safe harbor" clause if the lost data was encrypted.

When all data was kept within an organization's data center, the question of encryption key ownership was clear cut. But, in the cloud, the question becomes murky. Even when data at rest is strongly encrypted, organizations need to ensure that the cloud provider never holds or controls the keys that encrypted the data and, therefore, the CSP cannot be responsible for decrypting it. This means that only the organization's authorized users will be able to access the data because only they have access to the key. If an attacker or malicious insider steals a user's credentials and accesses the cloud service, they will see nothing but indecipherable data.

Misguidedly, some organizations using Infrastructure-as-a-Service (IaaS), for example, place their own keys on top of the infrastructure provided by the CSP, not realizing that they are still relying on the provider to protect the underlying service and that the key might not be as secure in the cloud as it is in a dedicated physical infrastructure.

Beyond the security considerations around letting CSPs control their keys, organizations must also address the legal considerations of key ownership. When examining any product or service where the encryption key is controlled by the vendor, courts can request access to the keys to decrypt the data in the U.S. and UK – with more countries potentially following suit. For example, if the courts or government agencies request access to encryption keys and a CSP controls the keys, the cloud provider can hand them over. But if an organization retains control of the encryption keys to their data, they can refuse the request.

To illustrate this point, in 2015, Microsoft was ordered to hand over a customer's emails to U.S. authorities, even though the data was in a data center in Ireland. If Microsoft had also held the data's encryption key, it would have been compelled to give authorities the key. The company that owned the data would have been held responsible for the compliance breach and faced the repercussions. Organizations with multiple cloud vendors face this threat with each provider.

"WHEN CRYPTOGRAPHY IS USED TO PROTECT VALUED DATA, THE RISK IS TRANSFERRED FROM THE CONTENT TO THE KEYS. ONCE ENCRYPTION HAS OCCURRED, PROTECTION OF CRYPTOGRAPHIC KEYING MATERIAL BECOMES PARAMOUNT."

– Cloud Security Alliance (CSA)

Entrust simplifies the path to a multi-cloud world

It's simple: When moving to a multi-cloud environment, the security and compliance of sensitive data is ultimately the organization's responsibility, not the cloud provider. So how do organizations achieve all of the great benefits that come from outsourcing their infrastructures to multiple cloud providers without putting their sensitive data at risk and their auditors on alert?

Organizations need to implement an enterprise-level encryption and key management system that is powerful, yet flexible and simple to deploy – whether the data is in the organization's own data center or at any of the multiple cloud providers' facilities. It's crucial to find a solution that removes the complexity of encryption and key management, while still allowing the organization to have 100% ownership and control over the encryption keys.

"IT'S IMPORTANT FOR ENTERPRISES TO RETAIN CONTROL OF ENCRYPTION KEYS AND MAINTAIN SEPARATION OF DUTIES BETWEEN THE ENTERPRISE AND THE CLOUD PROVIDERS WHO HOST THE DATA. THIS PROVIDES THE GREATEST PROTECTION, BOTH AGAINST EXTERNAL BREACHES OF THE CSP, AS WELL AS ATTACKS ORIGINATING FROM PRIVILEGED USERS."

– Cloud Security Alliance (CSA)

The Entrust Cloud Workload Security Platform

The Entrust Cloud Workload Security Platform features a broad range of solutions for data-at-rest encryption, integrated key management, privilege user access controls, automated compliance and remediation, and data sovereignty. Through this robust platform, both enterprises and government agencies can automate the enforcement of security policies and compliance mandates across any cloud environment.

By leveraging Entrust's enterprise-level data at rest encryption and integrated key management solutions, Entrust DataControl and Entrust KeyControl, organizations can secure cloud workloads and their sensitive data throughout the entire lifecycle – from deployment and migration to decommission. The Entrust solution is easy to deploy and manage and can run in any type of cloud environment. It also supports the highest levels of availability by offering the capability to perform initial encryption and key rotation tasks with zero downtime – in other words, zero disruption to the business.

Entrust has changed the game for organizations operating in multi-cloud environments. They can now leverage a powerful enterprise encryption and key management solution to enable – rather than obstruct – their multi-cloud adoption strategy.

Conclusion

As today's organizations deploy multiple cloud platforms, applications, and services, they stand to gain multiple new business advantages and opportunities. However, just as these new opportunities are opening, some doors are closing due to the challenges of keeping data secure and compliant in multi-cloud environments. At the same time, key regulatory bodies are raising the stakes for the level of security that organizations must deliver. The rules are getting stricter and the penalties more damaging. Finally, organizations are learning the reality of shared responsibility in the cloud, realizing they cannot rely 100% on cloud providers for security and compliance of their data.

The challenges can seem insurmountable. But they don't have to be. If organizations change their "accountability mindset" by taking full responsibility for encrypting their sensitive data at rest and implementing a holistic key management program with 100% control (or ownership) of their keys, they can mitigate most if not all of the risks to their data, no matter how many clouds they add to their environment – now or in the future.

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust is dedicated to securing a world in motion by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact