# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>03</td>
</tr>
<tr>
<td>Report Background and Introduction</td>
<td>04</td>
</tr>
<tr>
<td>Cloud Adoption and Security Challenges</td>
<td>05</td>
</tr>
<tr>
<td>Cloud Adoption Compelling Events</td>
<td>05</td>
</tr>
<tr>
<td>Cloud Security Challenges</td>
<td>06</td>
</tr>
<tr>
<td>Cloud Data Protection Usage</td>
<td>09</td>
</tr>
<tr>
<td>Collaboration &amp; Management Tools</td>
<td>09</td>
</tr>
<tr>
<td>Enterprise Requirements</td>
<td>09</td>
</tr>
<tr>
<td>Adoption by Industry Users</td>
<td>11</td>
</tr>
<tr>
<td>Data Protection Insights</td>
<td>13</td>
</tr>
<tr>
<td>Data Classification Requirements</td>
<td>13</td>
</tr>
<tr>
<td>Data Protection Approaches by Industry</td>
<td>14</td>
</tr>
<tr>
<td>Data Protection by Region</td>
<td>14</td>
</tr>
<tr>
<td>Healthcare &amp; Pharmaceuticals</td>
<td>15</td>
</tr>
<tr>
<td>Banking &amp; Finance</td>
<td>17</td>
</tr>
<tr>
<td>Government</td>
<td>18</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>20</td>
</tr>
<tr>
<td>Conclusions</td>
<td>21</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Cloud computing is fundamentally transforming the way organizations deliver IT functions. Faster time to market, reduced capital expenditure costs, and on-demand flexible scaling are just a few of the benefits of adopting cloud.

CipherCloud enables organizations to embrace cloud applications by protecting critical data going into the cloud. This approach has been adopted by millions of users in multiple industries, such as healthcare, banking and finance, telecommunications and government, across the globe. This report gathers insight from CipherCloud’s installed base and provides analysis on how enterprises approach cloud security and data protection.

The study found the following:

- **Cloud adoption drives more than technology innovation for enterprise:** The leading driver for companies adopting cloud is the opportunity to introduce new tools and capabilities into the organization, unlocking value across functions and throughout the enterprise.

- **Compliance and data protection concerns remain top barriers for cloud adoption:** Regulatory compliance requirements such as data residency and information security standards continue to be the top challenges for enterprises moving to the cloud.

- **Encryption is the number-one data protection mechanism for enterprise:** Companies concerned about data protection are turning to encryption technologies first and foremost to meet their needs.

- **Financial services and healthcare sectors lead in cloud data protection maturity:** Across the numerous global deployments, financial services and healthcare companies have the most complex data protection requirements and boast the most mature strategies.

“Regulatory compliance requirements and information security standards remain top challenges for enterprises moving to the cloud.”
This CipherCloud research paper provides insight on how organizations are mitigating the cloud security data protection risks by utilizing the CipherCloud platform. CipherCloud’s installed base spans organizations across the globe, ranging from mid-market to Fortune 50 companies. Most are mature cloud users, with a small percentage that are just starting their cloud journey. They are often geographically distributed with departments situated in different regions. Figure 1 provides a geographic representation of organizations that are included in this study.

**Figure 1. Cloud Security Data Protection: Customer Adoption by Region**

North American organizations are most heavily represented in the study, roughly 65%, as they are the most mature in their cloud journey and also the most advanced in their approach to cloud data protection.

European, Middle Eastern and African (EMEA) organizations represent approximately 23% of the study and have similar cloud data security requirements when compared to their North American counterparts, but more stringent privacy constraints.

Asia Pacific (APAC) and Latin American (LATAM) organizations make up the remaining 12%. These organizations must contend with their respective regional privacy regulations along with their audit and compliance requirements. Organizations in the APAC region often face stringent data residency requirements while LATAM companies typically prefer to balance security with cloud functionality requirements.
Cloud Adoption Compelling Events

Global organizations are adopting cloud solutions for a variety of compelling reasons ranging from new business opportunities to reduction in costs, to overall improvements in operational efficiency. CipherCloud conducted a global assessment of its installed base to ascertain the prioritization of the compelling events that drove cloud adoption decisions.

Figure 2 provides insights from the research. The assessment is comprised of organizations from across global geographies, multiple industries and in different deployment phases for each independent cloud application. Most organizations have two or more of the following compelling events apply to them.

![Figure 2. Cloud Adoption Compelling Events](image)

Although the majority of the organizations cited multiple compelling events that drove them to invest in the cloud, the primary cloud adoption driver is the opportunity to introduce new tools and services. These upgrades provide a uniform interface that maintains a consistent customer experience. As a result, new services are introduced more efficiently and scale with customer demand. The following are a few examples of new cloud-based services:

- New home mortgage application portals
- Ability to streamline automobile research and financial service options
- Portals to simplify the upload of sensitive medical files
- Medical services that provide reviews and recommendations
- Self-service portals that provide government services
The following three compelling cloud adoption events outlined in Figure 2 focus on improving the traditional methods of information collaboration and taking advantage of cloud technologies.

- Replace legacy Enterprise applications
- Enhance information collaboration
- Aggregate and centralize data

Traditional on-premises Enterprise applications are typically developed by separate internal groups and lack the application uniformity required for a consistent user experience. Due to this lack of uniformity, information collaboration with external partners as well as other internal groups introduce workflow inefficiencies and data integrity issues. Stemming from the lack of data centralization, the omission of the other departmental or group data minimizes the effectiveness of data analysis activities and any subsequent business decisions.

Additional key drivers for the adoption of cloud-based solutions include the rising infrastructure costs of:

- On-premise hardware
- Software development
- Facility improvements
- In-house support teams

An organization’s ability to either activate or deactivate business services and avoid incurring the continuous costs for deactivated services is a key investment decision. Several organizations are also consolidating their legacy data centers into new energy efficient, in-country facilities that operate seamlessly with cloud-enabled technologies.

Cloud Security Challenges

Although the benefits of a cloud-enabled business strategy may seem straightforward, organizations noted that several challenges persist. These challenges are not limited to technology but also extend to legal, financial and political influences. These influences are comprised of government and regional regulations which contain language that requires compliance. The combination of Audit, Compliance and Privacy account for almost two-thirds of the identified challenges associated with adopting a cloud solution. Figure 3 highlights the top four cloud security challenges.
A closer inspection of the Audit, Compliance and Privacy challenges identify three primary concerns that are inhibiting organizations from adopting a cloud solution. These concerns address data protection policy violations that pertain to a country, an organization or a defined data residency boundary.

The number one concern identified is a regulation that a country imposes upon an industry or organization. The regulation often references the collection of data on their citizens and utilizes cloud applications to process and store the information. Organizations responsible for adhering to these data protection regulations have teams that include the Chief Legal, Security and Information Officers. It is their responsibility to ensure that their cloud solutions are compliant and prepared for third-party audits. Figure 4 provides further insight with regards to the three primary concerns that caused the most challenges.

**Figure 4. Audit, Compliance and Privacy Concerns**

- Violation of Country Data Protection Policy: 58%
- Internal Security Policy Adherence: 31%
- Data Residency Not Adhered: 11%
Several organizations are proactively instituting self-imposed data security regulations for any cloud-based application. These internal regulations are extensions of existing Enterprise data security policies and best practices. The primary concern associated with self regulation is the lack of data classification standards. This paper addresses this topic further in the Cloud Data Protection Insights section.

The final Audit, Compliance and Privacy concern is data residency requirements, which introduces strict security guidelines stipulating how user data can be interpreted. These policies are a combination of both government and regional regulations that pertain to personal information. The following are a few examples of personal information typically associated with data residency policies:

- Name
- Race or ethnic origin
- Political, religious or philosophical opinions
- Medical history

The additional cloud security challenges that organizations identified and prioritized are:

- Unprotected or clear text data within the cloud application
- Inability to detect malware
- Scanning files for policy violations

These challenges are not mutually exclusive from the Audit, Compliance and Privacy challenges. As a result, a cloud business strategy has to ensure that the cloud application functionality is preserved while still adhering to security policies.
Collaboration & Management Tools

The rapid adoption of cloud-based products, tools and services across global enterprises has led to a sharp increase in the need to protect these assets from security threats. Tools and systems that were made available to organizations during the early onset of cloud computing have garnered the largest market share for their associated cloud applications; accordingly these tools are also at most risk of external cyber attack.

These applications fall into the following categories:

- Customer Relationship Management
- Enterprise Content Collaboration
- Enterprise Service Management
- Human Capital Management
- Private Cloud Protection

Customer Relationship Management (CRM) cloud applications comprise the majority of the cloud data protection requirements. The remaining aforementioned tools must also be supported in varying degrees for data protection, data loss prevention, and scanning for malicious programs.

Enterprise Requirements

Cloud adoption strategies along with the identified cloud security challenges compelled organizations to investigate new solutions that could mitigate cloud security and data risks. New solutions that provide cloud data protection methods while maintaining operational functionality are key components for adopting a cloud strategy. Surveyed customers prioritized their use cases and protection requirements as represented in Figure 5.

*Figure 5. Cloud Data Protection: Enterprise Requirements*
While data encryption is considered the primary method for protecting data in the cloud, additional requirements include the organization’s ability to control access to the encryption keys and preserve search, sort and filtering functions.

Successful cloud security deployments also require workflows and interoperability with both enterprise on-premises applications as well as external cloud-based applications. Organizations categorized the workflow requirements as Enterprise Infrastructure Integrations and Cloud Eco-System Integrations.

Enterprise Infrastructure Integrations are classified as:

- **Access** (authentication, authorization, accounting)
- **Communication Collaboration** (email, instant messaging)
- **Source Data** (databases, spreadsheets etc.)
- **Infrastructure Devices** (firewalls, load balancers, proxies, web gateways, hardware security modules, etc.)

Cloud Eco-System Integrations are classified as cloud-based applications. They continue to be an integral part of the core cloud application value proposition. They typically have a trusted relationship and have undergone some level of acceptance testing for interoperability with the core cloud application. These eco-system applications are dependent upon the data within the core cloud application. Maintaining these workflows while introducing cloud data protection functionality account for 34% of the requirements.

Data residency policies are typically addressed by data masking methods. These methods are selected primarily due to the non-association of the represented data residing within the cloud application and the source data. Country and regional regulations that contain data residency language are mostly addressed utilizing the data tokenization protection method.

Additional requirements to protect an organization’s cloud assets are based upon data threat protection. An example of a specific use case is where files require a scan before uploading them to the cloud. These files may contain malware and a preliminary scan is required before the file is accepted. In addition, several organizations require detection of policy violations as files are uploaded to a cloud application. In these scenarios, organizations provide content rules that are incorporated into a data loss prevention policy. These policies flag sensitive information i.e., social security number, credit card number etc., and a protection method workflow is initiated per the organization’s governance model.
Adoption by Industry Users

Cloud adoption is becoming pervasive across industries globally. The combination of government and self-imposed regulations is causing the predominantly regulated industries, such as banking and finance, healthcare and telecommunications, to adopt cloud security data protection strategies. Representative of industry as a whole, Figure 6 highlights the top four industries that comprise 88% of all CipherCloud users that access protected data using a cloud security platform.

The highest percentage of users implementing cloud security measures are in the healthcare and pharmaceutical industries, as these organizations are required to adhere to the Protected Health Information (PHI) policies and other privacy regulations. While these regulations vary by region and local governments, the common theme is to ensure both the data at rest within the cloud application and associated data workflows are protected, which enables these organizations to launch new service portals and provide improved methods for sharing information.

The banking and finance, telecommunications, and government sectors also recognize that traditional security measures, such as perimeter defenses, are not sufficient in meeting the increasing number of cloud security threats and regulations. As a result, these organizations are looking to ensure that they can scale their data protection solution to meet both business and regulatory demands.
The remaining 12% of users is made up of industries that have emerged with new cloud security data protection requirements. Due to their recent emergence, these industry segments have a higher propensity to implement highly customized data protection solutions. As a result, the data protection requirements vary significantly between industries and the selected cloud application. The industry data reflected in Figure 7 is a percentage of the emerging industry installed base total of 12%.

*Figure 7. Cloud Security Data Protection: Adoption for Emerging Industries*

The manufacturing industry has a greater degree of data protection requirements for customized objects and fields. The protected data ranges from consultant comments to pricing to technical details. The media and entertainment industry also has a higher degree of customized data protection requirements. Information that pertains to payment benefits, terms, and agreements is classified for protection while preserving application functionality.

The additional industries outlined in Figure 7 have a combination of standard and custom field data protection requirements. These requirements are applicable for text and numeric field types that are associated with credit card and street address fields.
Data Classification Requirements

Data protection requirements and use case priorities require organizations to assess the viability of data encryption or a data tokenization method. Both methods have their unique value proposition, however, application functionality and associated workflows are the deciding factor in selecting a method. In order to assist organizations with the data protection method selection, it can be useful to measure an organization’s needs against a cloud data classification framework. The below sample framework in Tables 1 & 2 enables organizations to determine which method meets their data protection requirements. Additional data classification examples are provided in the industry-specific section of this report.

**Table 1. Cloud Security Data Classification Framework: Security Classification Sample**

<table>
<thead>
<tr>
<th>Security Classification</th>
<th>Security Requirement</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personally Identifiable Information</td>
<td>Highly Sensitive</td>
<td>Social Security Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bank Account Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Credit Card Number</td>
</tr>
<tr>
<td></td>
<td>Sensitive</td>
<td>Email Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mailing Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phone Number</td>
</tr>
<tr>
<td>Protected Health Information (PHI &amp; ePHI)</td>
<td>Sensitive</td>
<td>Patient Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Date of Birth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Case Procedures</td>
</tr>
<tr>
<td>Business Sensitive</td>
<td>Sensitive</td>
<td>Shipping Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LinkURL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Campaign Name</td>
</tr>
</tbody>
</table>

**Table 2. Cloud Security Data Classification Framework: Operational Classification Sample**

<table>
<thead>
<tr>
<th>Operational Classification</th>
<th>Operational Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Full word, wildcard</td>
</tr>
<tr>
<td>Sort</td>
<td>Selection</td>
</tr>
<tr>
<td>Filter</td>
<td>Alphabetical, report views, lookup</td>
</tr>
<tr>
<td>Server Side Workflows</td>
<td>Triggers, formulas</td>
</tr>
<tr>
<td>Audit</td>
<td>History Tracking</td>
</tr>
</tbody>
</table>
Data Protection by Region

The predominant cloud data protection method implemented worldwide at 81% is data encryption. Tokenization accounts for the remaining 19% of cloud security deployments. Figure 8 provides a comparison of how each region implements a data protection encryption method versus a tokenization option.

Figure 8. Cloud Data Protected Fields by Region

North American organizations predominantly utilize encryption methods due to function preservation and the ability to search, sort and filter their data.

EMEA organizations have similar criteria as their North American counterparts; however, the regional privacy directives are subject to each individual country’s interpretation. As a result, tokenization methods account for 22% of the protected fields.

APAC organizations have a 50/50 split of both encryption and tokenization implementations. Data Residency requirements account for the increased utilization of tokenization methods.

LATAM customers prefer to utilize data encryption methods for cloud data protection due to their search, sort and filtering requirements.
Cloud Data Protection: Healthcare & Pharmaceuticals

Practically every healthcare provider, pharmaceutical company, and health insurance provider is responsible for some form of sensitive personal health data and are therefore subject to the stringent data protection requirements imposed by HIPAA, HITECH, and other regional regulations. CipherCloud protects numerous organizations in the healthcare industry, and for this report, we extracted some of the common practices from these customers.

There are 18 types of electronic Protected Health Information (ePHI), and we have seen all of them in our customer deployments. Figure 9 depicts the distribution of protected data across ePHI and other sensitive data categories. As shown, 100% of health industry organizations protect ePHI, 65% protect business sensitive information such as business documents, opportunities, and non-health and treatment activity history. An additional 30% protect user-generated content, which typically includes web comments, user community discussions, and social media engagement records. As healthcare companies expand digital customer engagement channels, we see more user-generated and user-engagement content begin to appear on the data protection radar of different companies.

When we look closer into ePHI data, we see that of the 18 ePHI types, an average company would have approximately 7.5 different data types that fall into various ePHI categories. These categories include names, addresses, phone numbers, healthcare policy IDs, email addresses, account numbers, and other identifying information. Figure 10 provides a distribution of the number of ePHI categories seen across the industry. As shown, approximately 50% of the healthcare companies have 6 to 9 different ePHI data types they must protect, 21% have over 10 different ePHI types, while roughly 29% have 5 or fewer ePHI data types.
Figure 10. Healthcare & Pharmaceuticals Data Protection: ePHI Category Classification

- 21% 10 and above
- 29% 5 and below
- 50% 6 to 9

Figure 11 shows the distribution of encryption versus tokenization techniques used to protect different types of data in the healthcare industry. Encryption is the predominant technology healthcare companies use to protect sensitive data with 67% of the companies in our study using encryption versus 33% using tokenization. To protect business sensitive data, 17% use tokenization while 83% utilize encryption.
Cloud Data Protection: Banking & Finance

Banking and Finance is another industry that has stringent data protection requirements due to PCI, GLBA, FFIEC, and other related regulations or standards. CipherCloud is actively supporting numerous banking and finance organizations by protecting their critical and confidential data. We see that companies in this industry sector are typically concerned about four categories of data while working with clouds:

- **Personal Identifiable Information (PII)**
  Names, addresses, phone numbers, email addresses, IP addresses, and any other information that identifies a living person

- **Highly Sensitive Personal Identifiable Information**
  This category includes information such as SSN, date of birth, and other highly sensitive personal data

- **Personal Financial Data**
  This includes credit card numbers, investment information, account balance, stock ticker symbols, loan numbers, and the like

- **Business Sensitive Information**
  This category includes anything that is business confidential such as internal documents, intellectual property, business communication and the like

Figure 12 presents the percentage of sampled companies that use CipherCloud to protect these four categories of data. 100% of the sampled companies use CipherCloud to protect PII sensitive data, 53% protect business sensitive data, 47% protect personal finance data, and 33% focus on highly sensitive PII.

*Figure 12. Cloud Data Protection: Banking & Finance Importance*
In addition, we reviewed the methods utilized to protect each category of data and documented our findings in Figure 13. As illustrated, 13% of the sampled companies are using tokenization to protect PII sensitive data. In contrast, 60% are using encryption to protect highly sensitive PII. Encryption is the predominant method used to protect personal finance data and business sensitive data.

**Figure 13. Banking & Finance Cloud Security Data Protection Methods**

![Bar chart showing data protection methods for personal finance data, PII-sensitive data, PII-highly sensitive data, and business sensitive data.]

It is not surprising that more companies use tokenization (40%) to protect highly sensitive PII than any other category of data going into the cloud. Information such as birth dates and Social Security numbers, if leaked, can cause severe financial and public relations consequences for the company. We also see tokenization used to protect PII and personal finance data, but not as a predominant practice.

**Cloud Data Protection: Government**

Government agencies across the globe are also adopting cloud solutions to provide information portals and other service applications. The information collected and analyzed typically contains PII which requires data protection. Figure 14 provides a summary of how the data protection security fields are classified for CipherCloud Government clients.
A combination of data residency regulations and security data protection method interpretation resulted in customers implementing the tokenization method.

Tokenization accounts for 64% of all data protected fields for the Government market segment. The cloud security data protection methods selected by CipherCloud Government clients is illustrated in Figure 15.

**Cloud Security Data Protection Methods:**
- Tokenization: 64%
- Encryption: 36%

**Figure 15: Government Cloud Data Protection Methods**
A majority of the fields that are tokenized for the Government deployments are classified as PII – highly sensitive. The selected tokenization method is dependent upon additional characteristics such as field type, field length, and unique label conventions.

Data encryption methods are utilized for those fields that are typically classified as business sensitive. These fields have field types that vary from text, dates, strings etc.. The majority of the fields require some combination of function preservation and protection for email fields.

Cloud Data Security: Telecommunications

Cloud security data protection requirements for the telecommunication industry are dependent upon the various countries in which they operate. The advantages of centralizing their information within cloud applications provides these organizations unique insights into trends and overall usage of their products and services. The primary cloud security data requirement is overwhelmingly associated with business sensitive fields as illustrated in Figure 16. These fields have a higher degree of third-party application integration requirements. As a result, encryption methods are utilized 100% of the time to ensure function preservation.

Cloud Security Data Protection Method: Encryption 100%

Figure 16. Telecommunications: Cloud Data Protection Classification Priorities
CONCLUSIONS

The benefits of cloud computing are being realized by organizations across the globe. The ability to introduce new business tools and services, transform IT operations, and scale for future growth are all examples of how cloud computing is impacting every industry. The impact is not without consequences. Though there are several compelling events that drive cloud adoption, the risks associated with cloud security and data protection are significant inhibitors.

The conclusions based on this research paper are summarized as follows:

**Cloud security data protection challenges are resolvable**
An organization's primary inhibitor for adopting the cloud is data protection. These protection requirements are clearly defined by regulations that encompass audit, compliance, and privacy laws. Research has shown that whether your organization is in a mature or emerging industry with respect to its cloud journey, data protection, malware detection and workflow integration challenges have been successfully resolved.

**Customers have successfully secured their cloud data**
Data protection methods have been utilized to protect data in cloud collaboration and management tools that range from CRM, Enterprise Content Collaboration, Enterprise Service Management and others. Organizations have selected encryption for their primary data protection method due to the preservation of search, sort, and filter requirements. 81% of CipherCloud's global customer install base utilizes the encryption method. Data residency requirements have also been addressed by implementing the tokenization method. The financial services and healthcare sectors are leading the charge in securing their data within the cloud.

**Customers have access to industry best practices**
Each organization has its own standard and unique data protection requirements. These requirements are based on industry-specific or government regulations. Interpreting these regulations and crafting a cloud strategy with the associated data protection policies is a complex, sophisticated process. As a result, new data classification tools are utilized to simplify the decision-making process.

As organizations continue to evolve their cloud adoption strategy, they are leveraging industry best practices and mapping them to the applicable use case. These mappings are ensuring the appropriate level of data protection is in place and that cloud adoption is accomplished successfully.