WHITE PAPER

Strategies for Archiving in Hybrid Environments

An Osterman Research White Paper

Published October 2017

proofpoint®

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

There are five primary drivers for the growing use of hybrid archiving solutions, in which organizations store some of their content on-premises and some in the cloud:

1. An increasing proportion of electronic content is being generated and stored in the cloud, including new content types – such as social media, online and text messages – that previously were archived only rarely.

2. A growing number of cloud archiving vendors offer robust solutions that offer performance that is often better than legacy on-premises solutions when accounting for security procedures, hardware/software/infrastructure currency, disaster recovery, provisioning and performance.

3. Decision makers are becoming more comfortable with the notion of storing essential business content in cloud archives.

4. Despite the rapid shift toward cloud-based archiving solutions, existing on-premises archiving solutions, including legacy solutions, still offer significant value and will continue to play a role in corporate archiving strategies for many years to come. Aging off content often makes more sense than migrating it to a new software/delivery provider.

5. The development of a unified archiving solution that will permit the search and production of information from both on-premises and cloud-based archiving platforms offers a number of important advantages compared to just one or the other solution.

Decision makers are becoming more comfortable with the notion of storing essential business content in cloud archives.

KEY TAKEAWAYS

- Organizations archive electronic content for a variety of reasons, but most often because of their regulatory, legal or contractual requirements to retain data for specified periods, their need to comply with various industry regulations, for purposes of disaster recovery or business continuity, and to retain data for eDiscovery.

- Decision makers are adopting cloud-based archiving solutions at a much faster pace than their on-premises counterparts, although the latter will continue to be an essential component of most organizations' archiving strategies for at least the next several years.

- A plurality of decision makers view a hybrid archiving approach – as opposed to using only an on-premises archiving system or a cloud-based solution – as preferable for some of their most important content management requirements, such as satisfying their regulatory obligations, maintaining 24x7 access to their archives, and minimizing the cost of maintaining an archiving system.

- Decision makers are of two minds with regard to archiving: while 40 percent of decision makers believe that on-premises archiving solutions are more secure than those in the cloud, the majority believe that cloud-based archiving is at least as secure as on-premises systems, if not more so. This tells us that both archiving delivery models will continue to thrive, but with an increasing focus on cloud archiving.

ABOUT THIS WHITE PAPER

This white paper discusses the key issues facing corporate decision makers surrounding archiving requirements and the location of their data. The paper also discusses some of the results of an in-depth survey of content archiving decision makers and influencers in mid-sized and large organizations that was conducted during August 2017.

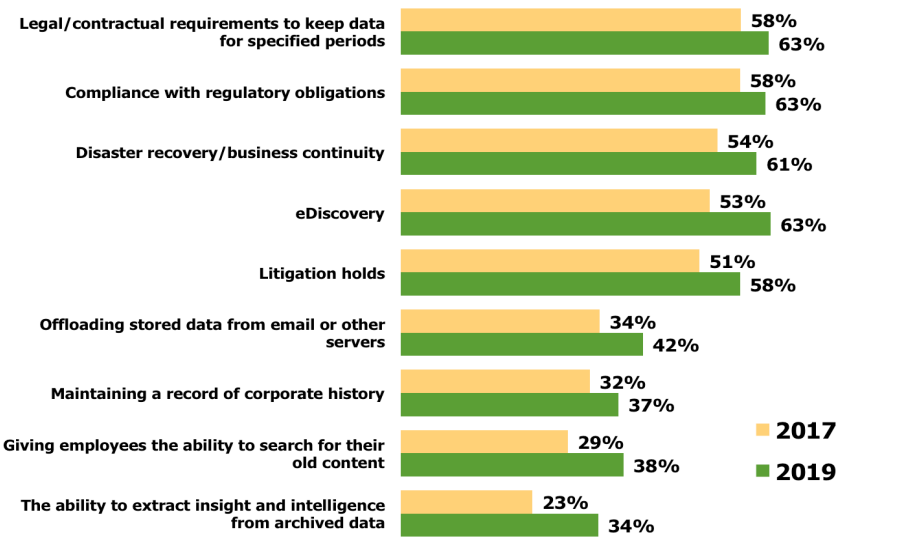
This paper was sponsored by Proofpoint – information about the company is provided at the end of the paper.

LEADING DRIVERS FOR ARCHIVING

The drivers for archiving electronic content in a particular organization depend on a number of factors, including its corporate culture, senior management's appetite for risk, the regulatory obligations it faces, the geographies in which it operates, and a variety of others.

The survey conducted for this white paper asked decision makers and influencers to rate the various drivers for electronic content archiving on a scale of 1 (not a driver) to 7 (a major driver), and also how these were changing over time. As shown in Figure 1, the most important drivers in 2017 are legal and contractual requirements to retain data for specified periods, regulatory compliance obligations, disaster recovery/business continuity, and eDiscovery.

Figure 1
Drivers for Maintaining an Archiving Solution, 2017 and 2019
Percentage Indicating an Important or Major Driver



Source: Osterman Research, Inc.

While all of the drivers for archiving electronic content will become more important over the next two years, two findings from the research are noteworthy:

1. While eDiscovery is today a fourth-place driver (albeit a close fourth place) for archiving, it will become tied for the most important driver in just two years' time.

2. The drivers for archiving that will grow in importance most quickly over the next two years are extracting insight and intelligence from archived data (growing in importance as a key driver by 50 percent) and giving employees the ability to search for their old content (33 percent). Admittedly, these are the least important motivators today for organizations to archive their electronic content, but a growing number of decision makers understand the importance of using their archived content for new and imaginative applications to business problems.

Osterman Research is a supporter of the view that archiving should be used as a tool to gather intelligence about an organization and gain competitive or other advantages based on the insight gleaned from this information. For example, a huge amount of information is stored in data archives, such as emails, spreadsheets, social media posts, memos, graphics files, presentations, voicemails, contacts, databases, CRM data and other data types. This content is generated by and stored in a wide variety of venues. The traditional view of archiving will preserve this content in the event it is needed in the future – a proactive view of archiving will perform analytics on this content to search for meaningful insights that can be extracted from it.

LEGAL AND CONTRACTUAL REQUIREMENTS

Organizations are subject to a host of legal and contractual requirements, and must manage their eDiscovery process and control the costs associated with eDiscovery. Every organization – regardless of its size, the industry it serves or how much data it possesses – must retain important records for various lengths of time. The requirement to retain data is imposed from a variety of sources, including legal precedent (courts establish standards for the length of time that data must be retained), statutory obligations (specifically defining the retention and production obligations for certain types of data), and internal best practices. Retention obligations apply to all forms of data, both physical and electronic. Organizations that reasonably anticipate pending litigation may also need to subject certain electronic content to a legal hold period that is different from their standard policies. A centralized archive can facilitate that process.

If eDiscovery is managed using a centralized and properly maintained archive, organizations are generally much more capable of addressing their litigation requirements and controlling the costs associated with those activities. In addition, for organizations that have frequent or extensive litigation or investigations, proactively addressing eDiscovery in a systematic way can significantly reduce overall eDiscovery expenses and other costs of litigation.

Easy search and access to electronic records, particularly across the multiple siloes in which an organization's data is stored, can permit legal counsel to evaluate the merits of a case before investing substantial time, money and effort in electronic records retrieval. In short, legal counsel and senior management can make better decisions about whether to fight or settle a lawsuit by having easy access to all archived content.

REGULATORY COMPLIANCE

A large proportion of the electronic records that pertain to an organization's business activities are subject to regulatory compliance obligations, which vary by industry and jurisdiction. It is important to note that virtually every organization and industry faces some level of regulatory compliance obligation to retain its records, and that retention obligations are not limited to "regulated" organizations or industries, since there is no such thing as an "unregulated" one. A few examples of data retention requirements outside of industries that are normally considered to be "heavily regulated":

- US and foreign air transport carriers must retain for three years the complaints they receive from individuals with disabilities who use these carriers.[1]
- Employers of homeworkers in the clothing, jewelry and related industries must retain for three years any documents related to stop watch time studies or other work measurement methods used to demonstrate piece rates so that these employers can prove that employees are making at least minimum wage.[2]

Every organization – regardless of its size, the industry it serves or how much data it possesses – must retain important records for various lengths of time.

[1] 14 CFR 382.157
[2] 29 CFR 530.202

- Bottlers involved in the labeling and advertising of distilled spirits must retain for five years certificates of age and/or origin for spirits imported to the US in bulk where those spirits are bottled and removed from the plant.[3]

These regulations require the retention of content such as financial documents, email correspondence between organizations, employee records, invoices, shipping information and a variety of other data. In fact, even metadata must be preserved – the Supreme Courts of both Arizona and Washington State have ruled that metadata must be retained along with other records.

Among the more heavily regulated verticals worldwide is the financial services industry. In the United States, for example, rules of the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) require members of national securities exchanges, brokers and dealers to preserve securities transaction records for a minimum of six years, the first two years in an easily accessible place. In Canada, records of purchase and sell orders of securities must be retained for seven years, the first two years in an easily accessible location. And in the United Kingdom, investment service and transaction records must be retained for at least five years.

The consequences to financial services firms of not complying with these retention regulations can be severe and typically involve the imposition of significant financial penalties.

Another heavily regulated industry is healthcare. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), requires organizations to protect patients' electronic health information from unauthorized users and to retain such information for six years. Non-compliance with HIPAA requirements could result in fines of up to $50,000 per violation, or criminal penalties of $250,000 and up to 10 years in prison for violations based on intent or malice.

Virtually every organization, even in industries which are not considered heavily regulated, are subject to electronic content retention requirements and the consequences of non-compliance with requirements, as discussed above.

THE GDPR

Aside from the enormous fines associated with violation of the European Union's General Data Protection Regulation (GDPR) – up to €20 million or four percent of an organization's annual turnover – there are some important implications to consider for organizations that possess data on residents of the EU. For example:

- Article 15 of the GDPR gives data subjects the right to ask any entity that possesses or processes his or her personal data (a data controller) to produce that data on demand. These individuals also have the right to know if and when their data is transferred to a third country or to an international organization, along with whatever safeguards are in place to ensure on-going protection of the data after it has been transferred. A data controller must provide a copy of any personal data that is being processed at no charge the first time it is requested.

- Article 17 states that, subject to certain conditions, a data subject has the "right to be forgotten" by any data controller that possesses or controls his or her information.

- Article 30 requires that data controllers keep records of their data processing activities, with a list of specific information to be retained for each record.

[3] 27 CFR 5.56

Moreover, implementing the right organizational and technological safeguards on all production systems that contain personal and sensitive personal data is essential, but it isn't enough. Sufficient controls are required for:

- Copies of production databases that contain personal data taken for testing, development, or analytics purposes.
- Spreadsheets and other data sources populated by exporting customer contact and profiling details for a mail merge.
- Email archives, whether stored on-premises, in cold storage or in the cloud are likely to contain personal data that must be protected under the GDPR.

The GDPR imposes a major burden on any organization that has data on residents of the European Union, requiring a level of data retention and management that is on par with the level of effort required for eDiscovery activities. Plus, these activities must often be performed without charging those who request information, and so archiving and related activities must be efficient and easy to use. In short, compliance with many of the key provisions of the GDPR will not be possible without a robust archiving capability.

STORAGE MANAGEMENT AND PERFORMANCE

An archiving system can help enable storage management by indexing content and making it more accessible and discoverable. This is particularly important for organizations that must respond to frequent retrieval requests for email and files because it can dramatically reduce the time employees spend looking for, filtering and producing data. Sunshine-law and Freedom of Information Act (FOIA) requests are two common types of requests, but there are numerous others.

An archiving system can also improve email and other system performance by minimizing the amount of "live" data that must be stored on active servers. Because electronic data like old email messages and files older than 30 days are accessed relatively infrequently, it often makes sense to move this content to an archiving system for better system performance. This can reduce the amount of time required to backup email and data servers, it can speed the time to restore a server from backups, and it can reduce the amount of overall downtime experienced in key systems.

KNOWLEDGE MANAGEMENT AND END-USER SELF-SERVICE ACCESS TO CONTENT

An organization's email and other electronic content constitute one of its most important business knowledge repositories. Some analysts have estimated that the majority of an organization's intellectual property is contained in its messaging systems. Even if that is overstated, an organization's electronic content does contain important (structured and unstructured), employee-generated information critical to its growth, ongoing operations and profitability, competitive advantage, and its ability to innovate.

To satisfy employees' constant need for business information, email, collaboration tools and other electronic content repositories are often relied upon as the primary tools used for work. For example, an employee may need to locate stored emails quickly so he or she can review their own email correspondence or other content, such as attachments, in email. Alternatively, a new employee may have to trace back email and other electronic content between his or her predecessor and a customer.

Employees are also extracting business intelligence and data from electronic content servers. This makes the preservation and availability of the content extremely important. An organization that does not store its important content adequately risks the loss of information that it has paid employees to create.

The drivers and needs for archiving are changing over time and organizations, including those operating hybrid environments, must be able to adapt.

THE DRIVERS ARE CHANGING OVER TIME

The drivers and needs for archiving are changing over time and organizations, including those operating hybrid environments, must be able to adapt. For example, cyber security has emerged as a driver for archiving and for preserving content from bad actors or those seeking to deploy malicious cyber attacks.

Regulations are evolving and archiving requirements are typically getting more stringent. Newer regulations like the European Union's General Data Protection Regulation (GDPR) and the New York Department of Financial Services (NYDFS) implementation of Cyber security Requirements for Financial Services Companies (CRFSC) are two examples of the changing nature of the archiving challenge.

HOW ARCHIVING IS EVOLVING

The survey of decision makers and influencers looked at the types of electronic content that organizations archive today and where that content resides. Notably, as shown in Figure 2, a high percentage of corporate email on-premises (61 percent), users' files (61 percent), invoices (58 percent), security audit logs (52 percent), and project data (48 percent) are all archived on-premises. Not surprisingly, corporate email in the cloud tends also to be archived in the cloud (56 percent). In addition, slightly more than 20 percent of both user files and on-premises email are stored in the cloud.

Figure 2
Types and Methods of Electronic Content Archiving, 2017 and 2019
Based on Percentage of Organizations

	2017		2019		2017-2019	
Content Type	Archive On-Prem	Archive in the Cloud	Archive On-Prem	Archive in the Cloud	On-Prem Change	Cloud Change
Corporate email on-premises	61%	21%	41%	46%	**-20%**	**25%**
Users' files	61%	24%	50%	54%	**-11%**	**30%**
Invoices	58%	25%	49%	45%	**-9%**	**20%**
Security audit logs	52%	17%	45%	40%	**-7%**	**23%**
Project data	48%	25%	39%	49%	**-9%**	**24%**
Content from SharePoint or similar collaboration tools	33%	31%	29%	56%	**-4%**	**25%**
Web pages	32%	25%	25%	43%	**-7%**	**18%**
Voicemails from the company phone system	30%	17%	28%	33%	**-2%**	**16%**
Machine-generated data	30%	17%	30%	33%	**0%**	**16%**
Content from company-owned mobile devices	22%	18%	21%	40%	**-1%**	**22%**
Company-managed file sync and share content	22%	32%	20%	56%	**-2%**	**24%**
Corporate IM content	20%	15%	24%	41%	**4%**	**26%**
Corporate email in the cloud	19%	56%	21%	70%	**2%**	**14%**
Voice conversations (not voicemail)	19%	12%	20%	19%	**1%**	**7%**
Work-related content from employees' IM accounts	16%	10%	13%	31%	**-3%**	**21%**

Figure 2 (concluded)
Types and Methods of Electronic Content Archiving, 2017 and 2019
Based on Percentage of Organizations

	2017		2019		2017-2019	
Content Type	Archive On-Prem	Archive in the Cloud	Archive On-Prem	Archive in the Cloud	On-Prem Change	Cloud Change
Personally managed file sync and share content	16%	10%	13%	26%	**-3%**	**16%**
Corporate social media pages	14%	15%	18%	41%	**4%**	**26%**
Work content from employees' personal mobile devices	7%	12%	12%	30%	**5%**	**18%**
Work posts from employees' personal social media accounts	6%	11%	10%	27%	**4%**	**16%**

Source: Osterman Research, Inc.

HOW IS CONTENT ARCHIVING CHANGING?

There are three key takeaways from the figure above:

1. The archival of electronic content of all types, not just email, is growing over time as decision makers increasingly appreciate the importance of retaining electronic records from a wide variety of sources. For example, relatively few organizations today archive text messages, despite the fact that many of these messages contain business records and should be archived just like email or any other form of electronic communications. A few regulatory organizations, such as the Financial Industry Regulation Authority (FINRA), have determined that text messages and other non-email content should be archived, and Osterman Research believes that this mindset will become more common over the next two to three years.

2. As shown in the figure above and the one below, archiving is shifting to the cloud as more organizations realize the benefits of letting a specialist provider manage the archiving process.

3. Despite the more rapid pace of cloud archiving adoption, on-premises archiving will continue to be a key method of archiving electronic content over the next two years and for many years thereafter.

In short, the more rapid growth of cloud archiving, as well as the continued use of on-premises archiving systems, points to a decidedly *hybrid* archiving future as both delivery models will be used for various types of electronic content archival.

Archiving is shifting to the cloud as more organizations realize the benefits of letting a specialist provider manage the archiving process.

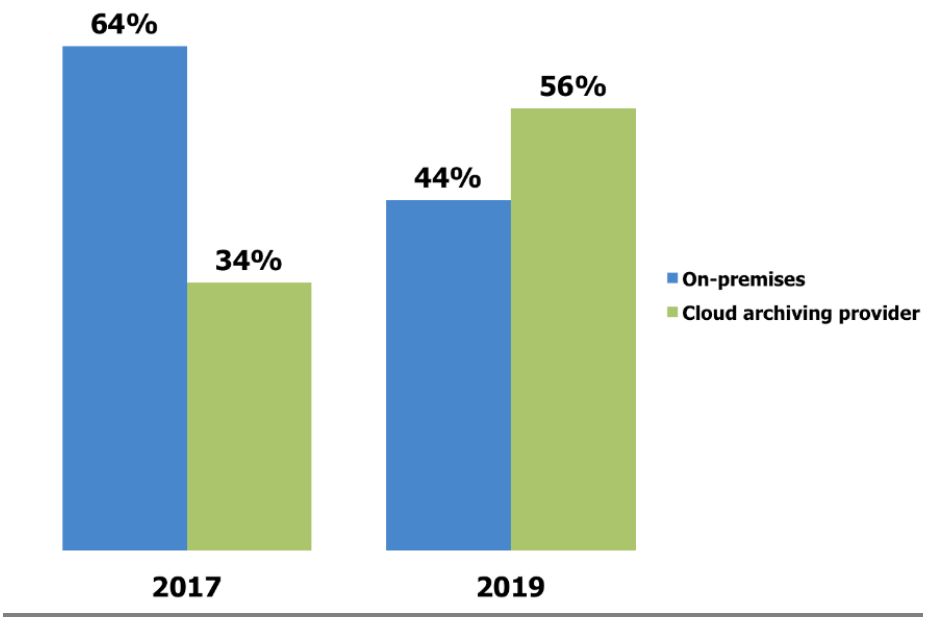
MORE ARCHIVED CONTENT IS MOVING TO THE CLOUD

Underscoring the shift of archiving to the cloud, while on-premises archiving will continue to a popular option for the archival of electronic content, is the data shown in Figure 3 on the next page. While the cloud will not displace on-premises archiving systems, we have reached a tipping point at which more content will be archived in the cloud during 2018.

There are many drivers for this shift, including the general trend towards the adoption of the cloud for core applications like email and file management, the increasing maturity of cloud archiving solutions, and the increasing acceptance of hybrid archiving solutions. As indicated in the figure above, cloud-based email

content created in the near term will tend to be archived in the cloud, so there is a significant relationship between the location of the production system and the archive that stores it.

Figure 3
Proportion of Corporate Content Archived by Venue



Source: Osterman Research, Inc.

That said, it is important to note that there is value in many situations for organizations that are maintaining email and other unstructured data both on-premises and in the cloud (such as before or during a migration from on-premises Exchange to Office 365) to be able to archive their content in a single cloud repository. This can improve both operational efficiency in having a single archive of corporate content, and it can speed search and eDiscovery of this content.

ADVANTAGES OF CO-ARCHIVING DIFFERENT CONTENT SOURCES

With the growth in data types, as well as the explosion in the amount of data generated and stored over recent decades, many organizations are seeking a solution that will permit storage of multiple content types in the same archive. Such a universal archive can offer a number advantages in that it ingests and indexes data from different sources and offers a common management interface and one storage management infrastructure. Savings comes from management, administration, and training on one system and one vendor to manage.

DECISION MAKERS ARE OFTEN MORE COMFORTABLE WITH HYBRID ARCHIVING

There are a number of scenarios in which decision makers are more comfortable with hybrid archiving:

- Organizations may have data sovereignty or jurisdictional requirements to archive certain data types in specific locations (or anywhere that is not outside of those locations), and so may choose to use on-premises archiving for that data and cloud archiving for other data.

- Organizations may have specific regulatory requirements that lead to a specific archiving strategy. For example, some archiving requirements, such as SEC Rule 17a-4, require preservation of certain types of records for three to six years, "the first two years in an easily accessible place." Some organizations may opt to retain more recent records in a cloud-based archiving system and older records on-premises to reduce their storage costs.
- Archiving records on-premises at primary locations may be a priority for an organization for reasons other than cost (since cloud archiving is often less expensive), while records from satellite locations with no dedicated IT staff may be better served with cloud-based archiving solutions, although these other reasons are addressed by some cloud providers.

- Highly sensitive or confidential data may require a specific archiving treatment, such as archiving the most sensitive data assets on-premises and other data types in the cloud.

- Some customers will migrate to a cloud-based archiving solution, but will continue to maintain legacy archives on-premises after doing so. The rationale is that since the useful life of this legacy data will extend for a few years more, but will rarely be accessed, the cost of and labor associated with the migration is not worth the effort to move it to the cloud.

It is important to note that we are not implying that on-premises solutions are necessarily more secure than those in the cloud, or vice-versa, but there continues to be a mindset among many decision makers that content behind the firewall is more secure than content in the cloud. Consequently, a hybrid solution may be the best option in these situations.

One of the fundamental benefits of cloud-based archiving, including hybrid archiving, is the geo-redundancy that such an approach offers.

STRATEGIES AND BEST PRACTICES FOR HYBRID ARCHIVING

SHOULD A HYBRID PLATFORM BE SINGLE-SOURCED?

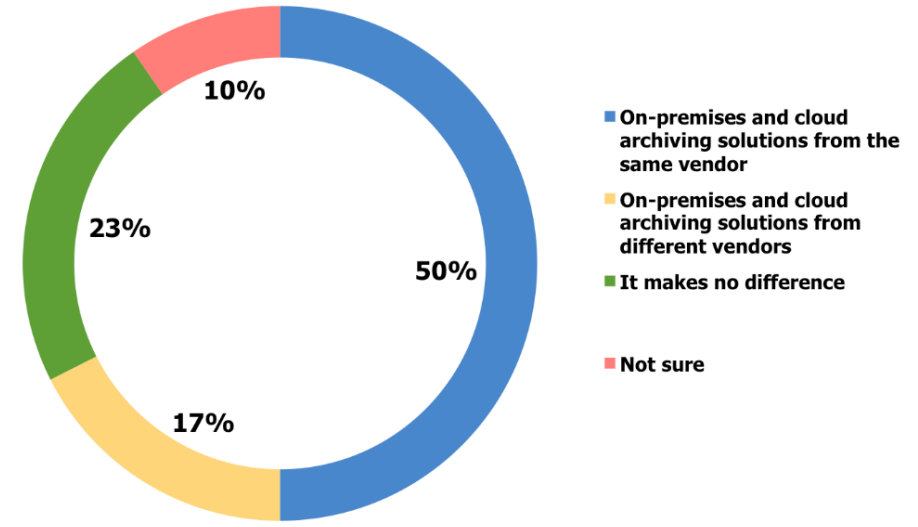
As part of the survey conducted for this program, we asked decision makers about their preference for vendor selection if they were to deploy a hybrid archiving solution. As shown in Figure 4 on the next page, we found that one-half of those surveyed prefer that the on-premises and cloud components of a hybrid archiving solution are sourced from the same vendor. However, 17 percent prefer that these components be sourced from different vendors, 23 percent don't have a preference, and another 10 percent are not yet sure.

What this indicates is that single sourcing of a hybrid archiving solution may not be an important requirement for a large segment of the prospective market. What will be much more important, however, is the ability to have a single view into all of the data that an organization has archived rather than an independent view into individual siloes.

THE BENEFITS OF GOREDUNDANCY

One of the fundamental benefits of cloud-based archiving, including hybrid archiving, is the georedundancy that such an approach offers in the event of a natural disaster, major power outage or some other event that renders access to a primary location inaccessible – and the on-premises archives it contains. This is particularly true for organizations that either must continually archive their content for regulatory reasons, as in the case of broker-dealers; or for organizations that provide access to archived email and other content for purposes of business continuity.

Figure 4
Preferences for Hybrid Archiving



Source: Osterman Research, Inc.

BENEFITING FROM THE BEST FEATURES OF ON-PREMISES AND CLOUD ARCHIVING

Some organizations may want to deploy a hybrid archiving solution to capitalize on the best features of on-premises and cloud archiving. The differing nature of on-premises and cloud archiving go beyond archiving the content where it is originated, although that will clearly be a trend for many organizations. Key issues to consider in the context of hybrid archiving include:

- **Lower cost of ownership**
  A hybrid archiving solution may offer moderately to significantly lower cost of ownership relative to a solely on-premises or cloud solution if an organization has a legacy archiving solution that it does not want to replace. For example, an organization may opt to maintain its existing on-premises archiving solution for older, infrequently accessed data that it must retain, while maintaining more current, frequently accessed data using a cloud-based archiving platform. This can reduce the cost of ownership by maintaining large amounts of older data without the expense of migrating and maintaining this data in the cloud. Admittedly, maintaining a legacy, on-premises archiving solution is not without cost, but avoiding the cost of migrating data to the cloud is preferred by some decision makers.

- **Synchronizing on-premises data with cloud archives**
  The ability to synchronize data stored in on-premises archives with that in the cloud is an essential best practice in order to eliminate duplicate data, which can drive up the cost of storage, eDiscovery and regulatory audits; and which can have a significant and negative impact on search performance.

- **Bandwidth optimization**
  A key advantage of a hybrid archiving platform is its ability to reduce the bandwidth required for content archiving, an especially important consideration in places where bandwidth is either not plentiful or is expensive, such as remote or satellite offices. While that's not necessarily a reason to consider on-premises archiving over cloud-based archiving, it must be part of the consideration in choosing an archiving platform.

- **Flexibility**
  Another important advantage of a hybrid archiving approach is the ability to use archiving in a way that best matches the requirements that will be placed on the archived data. For example, data that is accessed frequently can be stored in a cloud-based archive, but as it reaches a certain age and becomes less relevant it can be migrated to an on-premises archive for long-term, lower cost archival and reduced cost of storage. That said, the opposite can also be true: organizations will often need to maintain structured data in close proximity to production systems for reasons of maintaining good performance, while data that is less frequently access is better managed in the cloud.

- **Consolidation of on-premises and cloud content in a single archiving platform**
  The primary benefit of having a single archiving platform, as opposed to multiple platforms for different types or ages of data, is the single view of data that such a platform affords. Having a single platform is essential for tasks like eDiscovery, early case assessments, regulatory audits and even just basic searches, for a couple of reasons. First, a single archiving platform will enable an organization to discover all of its data, ensuring that it has a complete record of essential communications, data files and other information. Second, a single platform will make the cost of search less expensive and faster by allowing legal counsel and others to access the universe of data that an organization possesses instead of serially searching one silo of information after another. This reduces the potential of discovering duplicate data or not finding relevant information.

- **Independence from individual cloud applications**
  Another important benefit of a hybrid archiving approach is its ability to consolidate archiving functionality under a unified platform instead of using individual archiving tools for different types of data, especially cloud-based platforms. For example, Microsoft's Exchange Online Archiving will enable archival of content from Exchange and some Office 365/Exchange Online plans (albeit with a more limited feature set than is available from many third party archiving providers). However, it will not enable other content to be archived, such as social media content, text messages, or content from non-Microsoft platforms, necessitating the use of additional, independent archiving solutions.

- **Improved capabilities for data analytics**
  Finally, a unified, hybrid archiving platform enables significantly better data analytics capabilities than if individual archiving platforms are used. As noted earlier in this paper, the fastest growing driver for archiving is extracting insight and intelligence from archived data. While it is technically possible to gain insight from individual siloes of archived data, doing so is cumbersome, time-consuming and fraught with error when using individual siloes of archived information and attempting to consolidate this data into a unified view. The use of a unified archiving platform that can extract data from on-premises and cloud-based archives is distinctly preferable.

- **Defensible disposition**
  Service providers that support cloud or hybrid archiving options are partners that can help improve archiving and management practices, including assistance in enforcing retention via defensible disposition processes. This will help reduce the overall archive costs and keep information managed going forward.

A unified, hybrid archiving platform enables significantly better data analytics capabilities than if individual archiving platforms are used.

SUMMARY

The generation and storage of a growing amount of electronic content is moving to the cloud and IT decision makers expect the majority of archived content to be in the cloud within the next 24 months. Many organizations are considering a hybrid archiving solution, using a combination of on-premises and cloud-based archiving

solutions in order to reduce their cost of archiving content, optimize bandwidth use, and to develop a unified approach to archiving.

SPONSOR OF THIS REPORT

At Proofpoint, we understand that building a modern archiving and compliance strategy isn't easy. Legacy solutions haven't kept up with changing requirements and regulations. Proofpoint Information Archiving is a proven, next-generation archive solution that leverages cloud intelligence for deep insight into your data to reduce cost, complexity, and risk. Proofpoint Enterprise Archive is a secure cloud-based archiving solution that simplifies legal discovery, regulatory compliance, and end-user information access without the headaches of managing an archive in-house. It provides a central, searchable repository of a wide variety of content types. With Enterprise Archive, you know where data is stored and can quickly collect, search, and retrieve that information on demand. It also helps establish and enforce policies and review processes that reflect specific regulatory and geographic market requirements. By streamlining these information management challenges, you can reduce the risk of costly fines, adverse inferences and damaged reputations.

Proofpoint is a strategic technology and business partner with proven solutions built on advanced analytics and a cloud architecture solving for advanced threats, compliance issues, and digital risk. We help organizations prevent, detect and respond to advanced threats. We make compliance easier, less costly, and we protect brands and the people who trust them.

We offer:

- Enterprise Archiving, a proven, next-generation archive solution that leverages cloud intelligence for deep insight into your data to reduce cost, complexity and risk.
- Intelligent Supervision helps streamline SEC, FINRA and IIROC compliance with easy capture, review and reporting across email, social and enterprise collaboration data.
- E-Discovery and Analytics offers more efficient in-house legal holds, workflow and streamlined review to dramatically reduce the scope of e-discovery costs.
- Social Media Compliance helps you combat risks and comply with data-retention regulations to protect your people, data, and brand.

Learn more about how to protect your people, data and brand at proofpoint.com.

proofpoint.

www.proofpoint.com

@Proofpoint_Inc

+1 408 517 4710