WHITE PAPER

proofpoint.

MODERN ARCHIVING, COMPLIANCE AND THE CLOUD

THE ESSENTIAL GUIDE TO MIGRATING LEGACY ARCHIVING SYSTEMS

TABLE OF CONTENTS

INTRODUCTION 3

WHY ORGANIZATIONS ARE MIGRATING.......... 4

Forced upgrades from legacy on-premises vendor 4

Heading to the cloud.......... 5

MIGRATION STRATEGIES: FOUR APPROACHES.......... 5

Move all the data.......... 5

Put new data in the cloud, keep old data in existing archive 5

Migrate all important data 6

Migrate data that falls within your retention policy.......... 6

WHAT TO LOOK FOR IN A CLOUD ARCHIVE.......... 6

Experience—for IT, compliance, legal and users.......... 6

Fidelity and quality of the data 7

Data security 7

FOR MORE INFORMATION 7

TAKING YOUR FIRST STEPS.......... 7

INTRODUCTION

Organizations are generating more data—and more kinds of data—every day. Managing it in a way that is compliant, cost effective and efficient has never been more complicated.

Legacy email archiving software has not kept pace with data growth, new content types, or an ever-evolving list of regulations. As a result, organizations are spending too much time meeting their compliance obligations—or paying hefty fines when they don't.

That's pushing many companies to cloud-based archiving. Compared to aging on-premises the cloud is often less expensive, easier to manage and more reliable. But the switch can seem daunting, and it comes with its own challenges.

The good news: compliant data archiving is within reach. With the right approach and tools, you can dramatically reduce risk and improve your business efficiency, legal readiness, compliance posture—and (thanks to lower costs) bottom line.

This guide explores what to consider when migrating your archiving infrastructure, including timing, strategies, and common concerns.

WHY ORGANIZATIONS ARE MIGRATING

Many firms have amassed enormous amounts of data in on-premises email archive that are ill-equipped to address current needs, let alone future data challenges.

At the same time, external factors are triggering upgrades. Their legacy deployment may be reaching the end of its useful life. The organization might be looking to lower its data and infrastructure footprint. Or perhaps the IT department is moving everyone to Microsoft Office 365.

In all of these cases, cloud-based archiving is a logical next step.

FORCED UPGRADES FROM LEGACY ON-PREMISES VENDOR

Many legacy compliance archives are reaching the end of their useful life in terms of both software and hardware. In most cases, migrating to the cloud takes about as much effort as upgrading to a new on-premises archive.

New hardware is a huge capital outlay; breaking even on the investment can take years. So before deciding whether to keep their archive on premises or move to the cloud, organizations must consider not just their current business requirements but what they'll need three, five or even 10 years in the future.

The business case for upgrading existing on-premises archives is increasingly fragile. The upgrade isn't any less expensive than migrating to the cloud. It doesn't help people do their jobs better. And it doesn't equip organizations to adapt as their business needs evolve.

Cloud-based archives—which can easily adapt and scale to changing demands—make the most business sense for many organizations.

IS OFFICE 365'S MAILBOX ARCHIVING ENOUGH?

Microsoft Office 365 comes with built-in archiving for end-user mailboxes. It's a seamless, integrated experience that's easy to use. But it's meant for end users, not IT departments.

With Office 365's built-in archive, users may be able to easily archive and find old emails. But without additional services, administrators, auditors and legal teams can't adequately archive, search and supervise content across the enterprise.

With Office 365's native archiving features, enterprise-wide email searches are difficult. Supervisory reviews are slow. And compliance policies can be applied to only a limited set of content. That leaves out a wide range of employee communication that takes place outside the Microsoft ecosystem, such as social media and instant messaging.

For compliance, e-discovery, and corporate governance, most companies need a true enterprise-class archiving solution that augments the platform's native mailbox archiving features.

HEADING TO THE CLOUD

Other companies are moving their archives to the cloud to shrink their data and infrastructure footprint. Such a move can lower costs, because cloud services enjoy IT economies of scale that even most large enterprises can't match.

The move can also improve security and performance. Retrieving data for audits and legal requests from a cloud-based archive is usually much easier and faster than with on-premises vaults.

For companies already moving their email and collaboration infrastructure to Office 365, the choice is even clearer—even the best on-premises compliance archives can't archive cloud-based content efficiently.

MIGRATION STRATEGIES: FOUR APPROACHES

While staying with a legacy archiving system is a much worse option, migrating your data archive does cost time, money and resources. To streamline the process and reduce the risk of data loss, you need a migration strategy that fits your goals, needs and resources.

Here are four approaches to consider when migrating your archive:

1 MOVE ALL THE DATA

At first glance, migrating all of your data at once would seem the simplest option. It isn't.

Imagine moving into a new house. You wouldn't waste time packing up your garbage, old paint buckets and the detritus that accumulated in your garage. And you certainly wouldn't move it all, unpack it and find room for it in to your new residence.

That's why this option isn't the best option for most companies.

PROS: You get the full benefits of cloud-based archiving without having to spend time and labor reviewing and separating records according to the retention requirements they're subject to. You also avoid the risk of losing any data you might be expected to review or retrieve later.

CONS: This is the most expensive approach to archive migration. You will likely end up migrating data that you don't need. And because of the sheer volume of data you're migrating, the process may actually take longer, delaying the benefits of a cloud-based archive.

2 PUT NEW DATA IN THE CLOUD, KEEP OLD DATA IN EXISTING ARCHIVE

In this approach, you might leave your existing enterprise vault in place for older data and archive new data with a cloud-based solution.

PROS: This strategy makes sense if you have a short retention period. If your legacy archiving infrastructure is already paid for, letting old data expire there can be less costly and time consuming than migrating it to the cloud.

CONS: You'll have two archives to maintain. And until the old data expires in your legacy archive, responding to an audit or e-discovery request may mean more work—you'll have to search and retrieve data from each archive separately.

3 MIGRATE ALL IMPORTANT DATA

This approach involves leaving most of your old data in your existing archive but migrating your most important data, including anything subject to a legal hold. (Even if your firm has a short retention policy, some data may need to be kept and referenced much longer.)

PROS: Migrating data subject to legal holds can streamline audits and e-discovery requests. You'll get most of the benefits of a cloud-based archive without the costs involved with migrating everything.

CONS: You'll have to review data to see what is subject to legal holds, which may be difficult with some legacy on-premises archives. It may be tough to get organizational buy-in for selective disposition. Some departments might worry about losing data.

4 MIGRATE DATA THAT FALLS WITHIN YOUR RETENTION POLICY

Even firms with a well-defined retention policy often don't dispose of data systematically. This option means moving just the data that your policies and business use cases can justify.

PROS: This approach can be an opportunity to clean up old data and start enforcing your archiving and retention policies on a go-forward basis.

CONS: The approach can take more time, delaying the benefits of a cloud-based archive.

WHAT TO LOOK FOR IN A CLOUD ARCHIVE

Enterprise archiving is fundamental to your organization's success. That's because your people are creating more data in different repositories every day, and you need to capture, preserve and monitor it all. Migrating to cloud archiving can give you the flexibility, efficiency, and compliance you need to succeed.

If you're ready to migrate now or are considering such a move, here are a few critical features to look for in a cloud-based solution.

EXPERIENCE—FOR IT, COMPLIANCE, LEGAL AND USERS

The ideal archive provides a centralized, searchable repository that gives users access to historical data.

At the user level, it should be simple and intuitive, with a familiar user experience that fits your organization's workflow and keeps employees productive. And search performance should be fast and accurate no matter how large the archive grows.

At the organizational level, it should help IT, compliance and legal teams reduce the cost and complexity managing and monitoring today's exploding data volumes.

FIDELITY AND QUALITY OF THE DATA

To ensure than you can demonstrate the chain of custody and every message that you need is preserved, your archive should be failsafe. Get a solution that can guarantee that no message is lost, even if the network goes down.

Insist that your cloud archiving vendor can prove that nothing is removed from the journaling mailbox until it is safely in the archive.

The solution should also provide full reporting and a transparent, unalterable audit trail that lets you demonstrate you've met all retention, chain-of-custody, and legal-hold requirements.

DATA SECURITY

If you archived data isn't safe, then you run the risk of not being compliant.

To keep it secure, any data that leaves your environment should be always be encrypted. Consider a solution that protects in transit and at rest in the cloud archive infrastructure.

Your encryption key should be yours alone—not shared with the cloud archive provider—so that you retain full control over who can access archives data.

Data centers used to house the cloud archive should be SSAE-16 SOC 2 Type II certified—not just for the physical facilities, but for service itself.

TAKING YOUR FIRST STEPS

Done properly and systematically, compliant data archiving can greatly reduce your risk while boosting your business efficiency.

Start by asking:

✓ *What information does your organization really need to keep?*

✓ *How long do you need to keep it?*

✓ *What archiving approach and tools will best ensure you stay compliant as your data grows?*

Your answers will help you evaluate whether you need to move any, all or just some of your historical data in your journey to a more modern archiving solution.

FOR MORE INFORMATION

To learn more about migrating to a cloud-based archive—and how Proofpoint can help—visit Proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.