Cloud
Essentials

How to future-proof your email retention strategy as you exit Mimecast

A Cloud Essentials eBook
2023

Welcome

If you're reading this eBook, chances are you've already decided that exiting Mimecast makes strategic and financial sense for your organisation. It's a realisation that has been dawning on a lot of businesses where Microsoft 365 services have become their IT backbone (particularly since Microsoft's email security and continuity offerings became a real force to be reckoned with).

Of course, deciding it's time to make the leap often creates more questions than it does answers.

This eBook will help guide those questions in the right direction to cover all the major bases and kick off a streamlined and successful migration journey.

All details correct at the time of going to press (January 2023).

Inside, you'll find:

- Important questions to ask when choosing a new home for your legacy email data.
- An outline of Microsoft 365's approach to email retention, archiving and journaling.
- Top tips for preparing a successful migration.
- An overview of the three migration stages and key considerations for each.
- Advice on what to do next.

Not a fan of DIY?

Our one hour Email Preservation and Migration Workshop will guide you through all the elements covered in this eBook (and then some) and clarify the best strategy for your business moving forward. The agenda is customised to your particular needs, but typically includes:

- A review of your business and legislative requirements for email capture, retention and disposition.
- A comparison of options for journal capture going forward, including the operational and compliance strengths and weaknesses of each.
- Recommendations for your data migration approach.
- Best practices for servicing eDiscovery requests during and after migration.
- Advice on the best extraction formats to preserve vital metadata from any third-party journal services.

Book a workshop now

> "We're being asked how organisations can future-proof their next steps with email and archives, ensure security and compliance, and minimise cost. In our minds, the two biggest questions to answer are 'Where is it going?' and 'How will you get there?' Answer those correctly, and the puzzle pieces begin to fall into place."

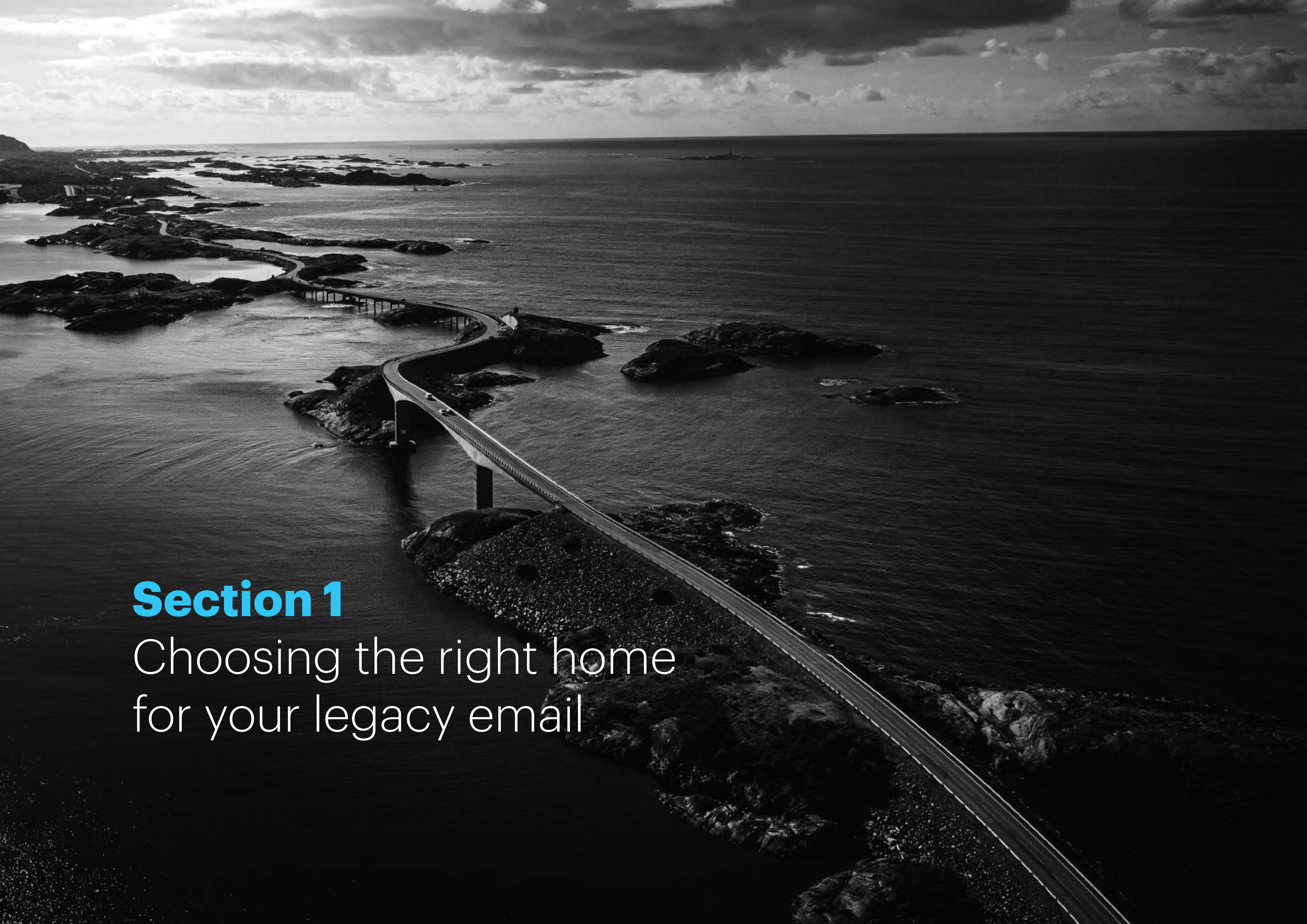
Chris Hathaway

About the authors

Chris Hathaway is a content expert. As well as experienced in IT risk, he's overseen the successful completion of many complex cloud migration, content management and compliance projects during his decades long career. He combines his in-depth knowledge of the Microsoft ecosystem with an understanding of today's tech space and a passion for collaborating with clients to find the best solution to their challenges.

Johann van Schalkwyk is an MCP, MCSE and MCSA certified professional with Microsoft Preferred Partner Solutions Expert accreditation. He's the Cloud Essentials technical guru when it comes to security, governance, migration and compliance solutions, and his 17 years of experience spans Microsoft and non-Microsoft technologies. Johann is able to use his know-how to bring the technology to life, easily conversing with both technical and business teams to solve our clients' cloud technology challenges.

Contents



Section 1
Choosing the right home for your legacy email

Choosing the right home for your legacy email

There is no one-size-fits-all solution for storing legacy email. Finding the best destination for your organisation will depend on a lot of factors.

Typically, you'll have three options when coming from Mimecast. These are:

1. Leave your legacy mail in static mode in Mimecast until it reaches its disposition date.
2. Migrate selected content to Microsoft 365 and/or alternatives.
3. Migrate all content to Microsoft 365 and/or alternatives.

How do you choose? We like to kick things off by asking these questions:

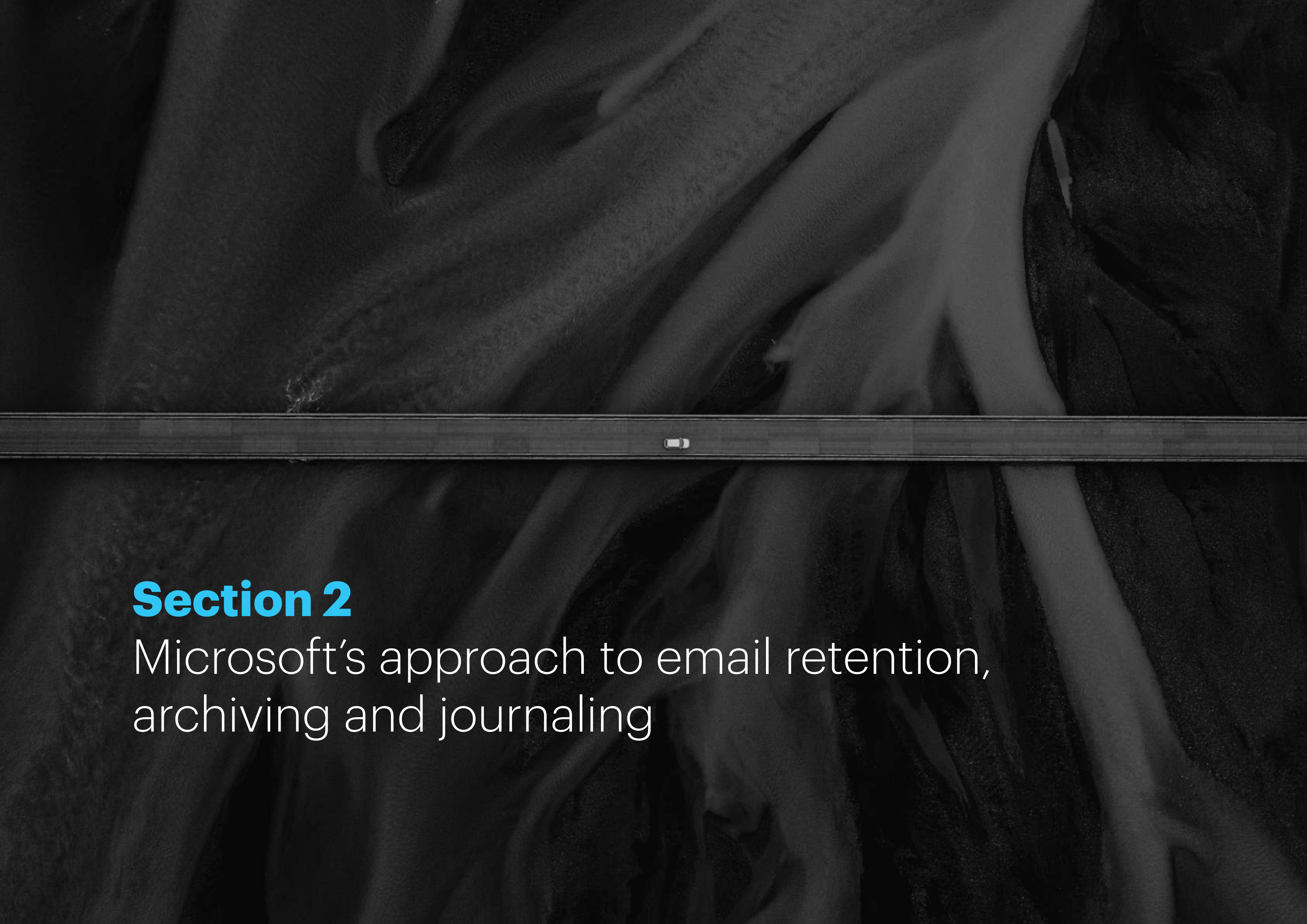
- What are your current operational/regulatory/user requirements for email retention?
- Could a selective migration work in your favour? Move some things, keep others where they are?
- Is traditional journaling still the right fit, or do you need more granular control over retention?
- What benefits could in-place archiving have in your context?
- How do you want to handle the processing and preservation of leavers' mailboxes?
- What does a typical eDiscovery scenario look like for you, and where could you benefit from doing things differently?
- What does your collaboration governance (Teams/SharePoint) strategy look like and who is its custodian?
- Which Microsoft 365 governance and compliance features are most relevant to you?
- Which Microsoft 365 security features are most relevant to you?
- What DLP policies and notifications do you need?
- What mail flow rules, blocking/bouncing etc. do you need?
- How confident are you in adopting Microsoft features and what barriers are in your way?
- What is the projected ROI of moving out of third-party solutions into Microsoft over an achievable timeline?
- What is your current Microsoft 365 licence plan and adoption/upgrade roadmap?

Don’t forget to consider how email fits into your wider governance and compliance perspective, too. Questions to ask here include:

- How disparate do you want your data estate to be? Do you need to work towards applying policies and controls consistently, even outside the Microsoft ecosystem?
- How accessible and agile do you want your data to be? What are the risks and potential cost implications of being locked into a vendor who charges exit penalties or ongoing access fees?
- How are you dealing with “Cloud Attachments” in email? (Cloud Attachments are links to documents that are typically stored in SharePoint and OneDrive. So instead of attaching an actual copy of a document in an email or a Teams chat, you have the option of sharing a link to the file. This creates problems for Retention and eDiscovery outside of the M365 ecosystem.)
- How valuable is your data? Is the price you’re paying for retention proportional to the benefits and are you sure you are collecting everything?
- How are end users accessing and collaborating on content? What risks and benefits could this introduce? E.g., Would using Teams in preference to email introduce any vulnerabilities?

What to look for in a legacy email preservation platform

- ✓ Zero lock-in
- ✓ Owned and managed by you
- ✓ Highly available
- ✓ Scalable
- ✓ Secure
- ✓ Storage efficient
- ✓ Compliance compatible
- ✓ Lifecycle management, including defensible deletion
- ✓ Accessible/available for eDiscovery
- ✓ Future-proofed and agile for future content strategy



Section 2

Microsoft's approach to email retention, archiving and journaling

Microsoft 365's approach to email retention, archiving and journaling

Where archiving used to be the blanket term for the capture and retention of email in a "move to manage approach", Microsoft 365 takes a more precise approach. Retention is one thing; Online archiving another.

Both form part of Microsoft's integrated ecosystem, however, and are subject to the same retention policies, labels and legal/eDiscovery holds.

> "Microsoft 365 was designed as an ecosystem. The real winners are those organisations embracing this approach, treating email not as an isolated workload, but rather one piece of a much bigger content picture."
>
> **Chris Hathaway**

Email Retention

Email retention in Exchange Online relates specifically to the prevention of premature deletion or alteration of email items. It involves a two-stage process that works best when governed by well-designed retention policies and labels.

> *Getting retention policies and labels right means understanding not only the 'whats' but also the 'whys' of retention within your specific environment. That includes industry best practices, compliance obligations, specific risk factors and operational requirements.*

Stage 1 – Deleted Items folder

When a user deletes an item from a public folder or mailbox, it goes to the Deleted Items folder. Here, it is retained for 365 days before being moved to the next retention stage.

Users can recover deleted items from the Deleted Items folder themselves, or bypass this retention stage altogether by pressing shift-delete from their mailbox. Users can also empty their deleted items folder, or delete selected items within it, triggering the next stage of the retention process.

Stage 2 – Recoverable Items folder

After 365 days (or manual deletion) items in the Deleted Items folder are moved to Recoverable Items (or RIF). Here, they are retained according to any applicable retention policies and/or labels. When these rules expire (or if none apply), items are permanently deleted after another 14 days (customisable up to 30 days).

Items within the Recoverable Items folder cannot be recovered by users directly. Admin/helpdesk intervention is required and the content is available to relevant eDiscovery search.

By default, Recoverable Items mailboxes are subject to a soft limit of 20 GB and a hard limit of 30 GB. This can be customised, but is also automatically increased if the mailbox is placed on Litigation Hold or In-Place Hold, or if a mailbox-level retention policy is applied.

Archiving

Archiving in Exchange (also called in-place archiving) is a mailbox management feature that enables users to move or copy messages from their primary mailbox to a secondary archive mailbox. This frees up storage space in the primary mailbox without compromising access to archived content. It is not a substitute for a third-party backup, but can be a useful hygiene and storage optimisation tool.

Journaling

While it's possible to configure journalling policies in Microsoft 365, journal mailboxes themselves cannot be hosted within the platform. Instead, organisations have the option to:

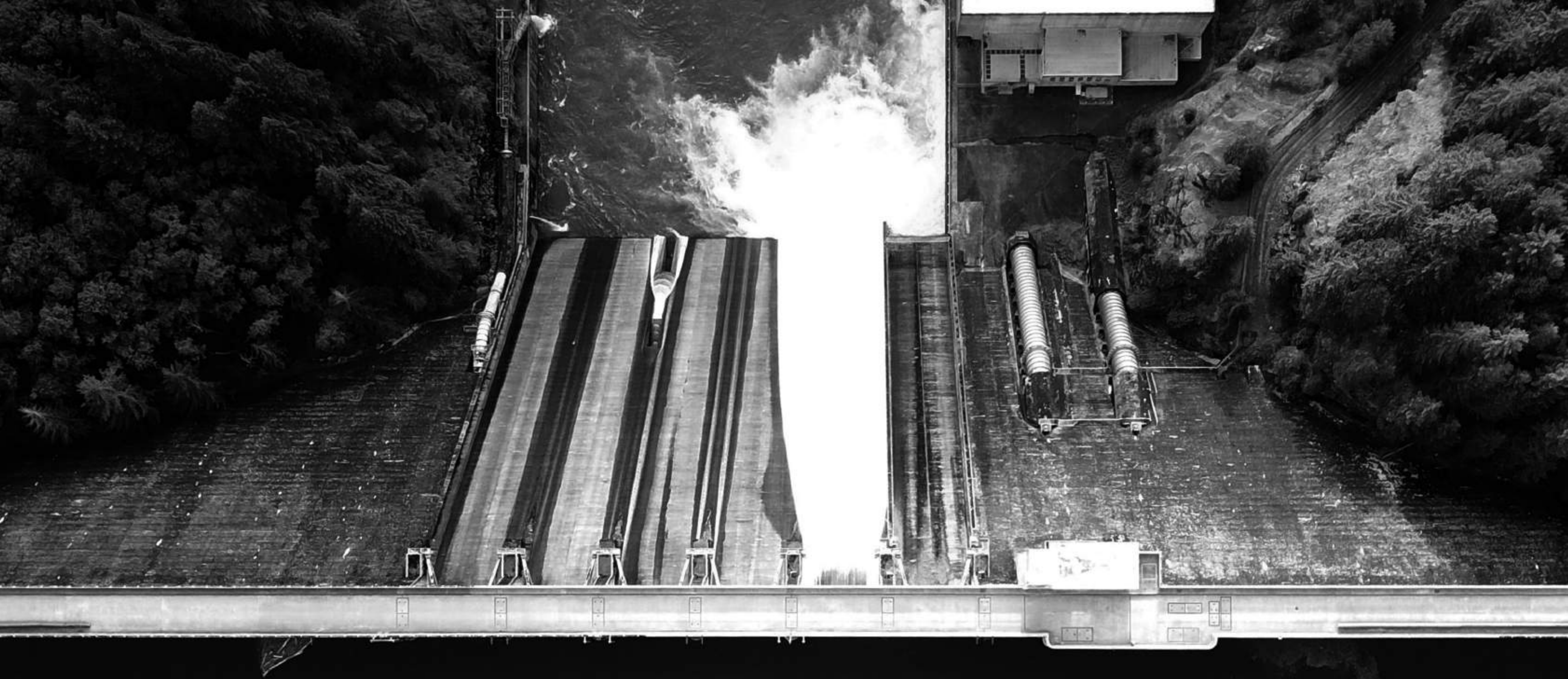
- Switch to a traditional journaling service using an external SMTP journal rule, typically to a cloud platform hosted by you or on your behalf in Microsoft Azure; or
- Simply use Microsoft 365 Litigation Hold or Retention Policies to achieve the same indelible compliance and retention results.

Benefits of choosing the latter include:

- An optimised, multi-instanced storage model that allows each user to retain their copy of all emails sent/received with no performance penalty and no single point of failure.
- Highly configurable retention periods with no upper limit.
- Retention of emails deleted by users in out-of-sight folders where they remain available for eDiscovery.
- Indefinite retention of BCC'd recipients.
- Retained and discoverable distribution lists.
- Inactive mailboxes (i.e., leavers) available for indefinite hold with no licence penalty.
- Retention of specific versions with Cloud Attachments.

Keen to know more on how Microsoft measures up in terms of threat protection?

Check out our analysis of ***Microsoft's answer to threat protection*** and ***Office 365 vs Mimecast, Proofpoint & Forcepoint***.



Section 3

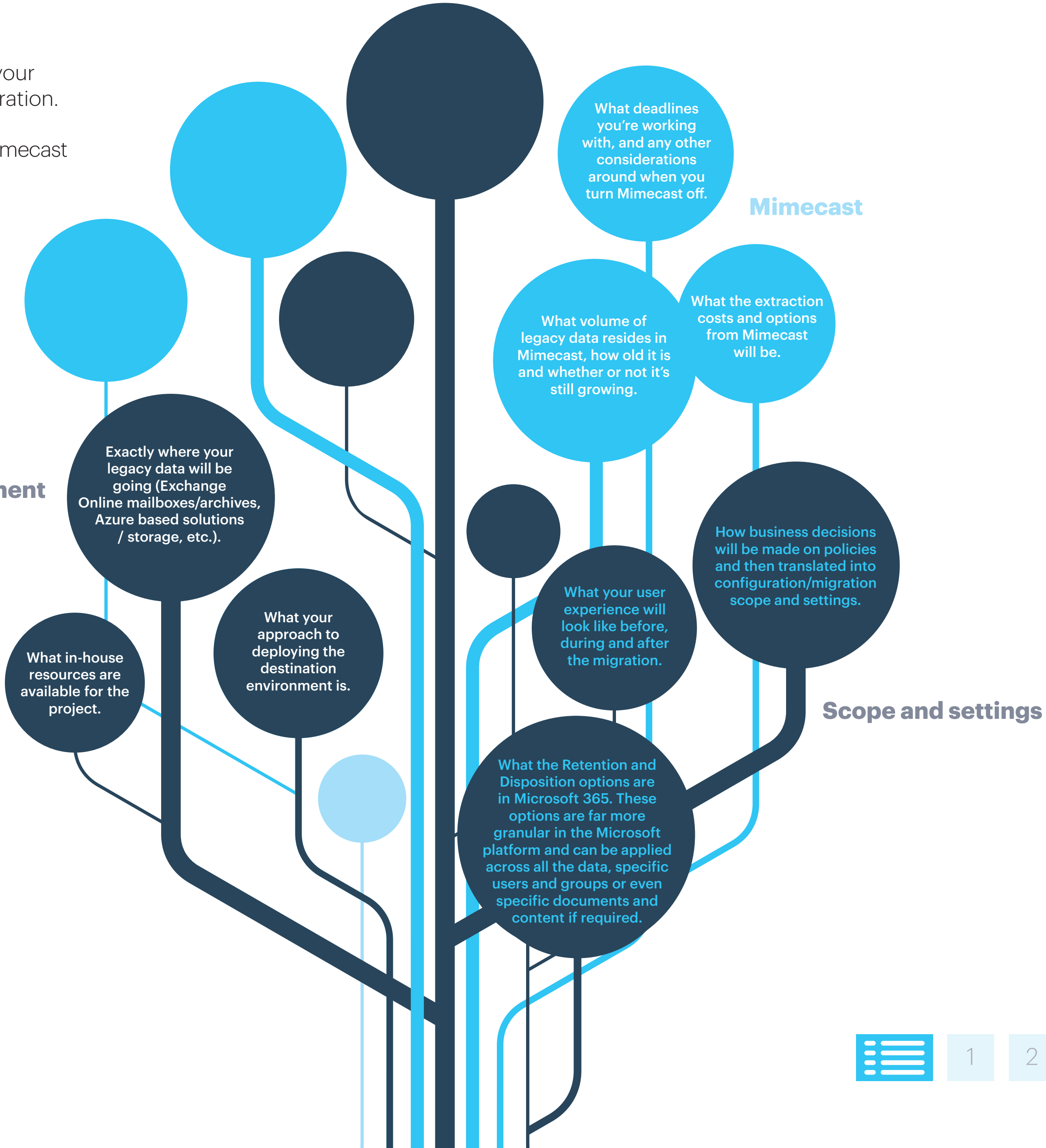
Top tips for a successful exit strategy

Top tips for a successful exit strategy

Prep, prep and prep some more

Like any migration, the biggest factor influencing your success as you exit Mimecast is going to be preparation.

Make sure you have started the conversation with Mimecast and get a firm handle on:



Mimecast

What deadlines you're working with, and any other considerations around when you turn Mimecast off.

What volume of legacy data resides in Mimecast, how old it is and whether or not it's still growing.

What the extraction costs and options from Mimecast will be.

Your environment

Exactly where your legacy data will be going (Exchange Online mailboxes/archives, Azure based solutions / storage, etc.).

What in-house resources are available for the project.

What your approach to deploying the destination environment is.

Scope and settings

How business decisions will be made on policies and then translated into configuration/migration scope and settings.

What your user experience will look like before, during and after the migration.

What the Retention and Disposition options are in Microsoft 365. These options are far more granular in the Microsoft platform and can be applied across all the data, specific users and groups or even specific documents and content if required.

Section 4

The four stages of migration

The four stages of migration

1. Extraction

Done by: Mimecast and you

Mimecast may charge to extract your data. Make sure to get a quote and an idea of timelines in advance. You can do the extraction yourself, piecemeal, using search and export, but this isn't suitable for most bulk migrations. It can be useful for small scale testing purposes to begin with.

You should also ensure that you have accurate reports on volumes and metrics surrounding your data. You will want to have confidence in storage, processing and timescale projections around the project. Accuracy in this reporting will also be a means of validating receipt of all content, especially if it is released to you in batches.

In most cases the extracted data from Mimecast should be requested in Envelope Journal Format also known as "EJF". EJF format is a zipped container with a date range of emails in envelope format, which means it contains all the meta data including "BCC" and Expanded Distribution lists which would not have been in the original email and is a key compliance and forensic requirement.

Pro tip:
Have a temporary destination set aside for your export in advance. Confirming the projected export size beforehand will help ensure you have adequate space.

2. Migrate from Mimecast's Protection Service to Microsoft Defender for Microsoft 365

Done by: your migration partner (or you)

Planning and cutting over to the Microsoft protection and hygiene services are an important aspect of the transition and getting the return on investment for your Microsoft licensing.

Simply changing your MX records to point to Microsoft 365 without prior and thoughtful testing will result in many surprises like;

- It's almost a guaranteed certainty that not every customisation in your current protection service is required in Defender for Office 365. It's also very possible that Defender for Office 365 will introduce new issues (allows or blocks) that didn't happen or weren't required in your current protection service.
- Your help desk and security personnel need to know what to do in Defender for Office 365. For example, if a user complains about a missing message, does your help desk know where or how to look for it? They're likely familiar with the tools in your existing protection service, but what about the tools in Defender for Office 365?

The migration process to migrate from Mimecast's Protection Services can be divided into three phases as describe below:

Prepare
Configure
Onboard
Monitor

Prepare

- Inventory the settings at your existing protection service
- Check your existing protection configuration in Microsoft 365
- Check your mail routing configuration
- Move features that modify messages into Microsoft 365
- Define spam and bulk user experiences
- Identify and designate priority accounts

Configure

- Create pilot groups and policies
- Configure user submissions
- Configure Enhanced Filtering for Connectors

Onboard

- Onboard security teams
- Gradually enable pilot protection, observe and iterate
- Extend protection to all users and switch your MX records

Monitor

- Normal operation and maintenance of Defender for Microsoft 365
- Review user reported messages
- Review overrides in the threat protection status report
- Use Advanced Hunting queries to look for tuning opportunities and risky messages

3. Processing

Done by: your migration partner (or tooling)

In order to be rehomed accurately, your email that is received from Mimecast will need to be analysed in a process called "recipient collection". This is so that you can restore the individual emails from the Mimecast Journal stream to the correct Exchange Online mailboxes. The email migration itself is processed "in-memory" and in a multi-threaded process to overcome throttling in Exchange Online and for security and efficiency – we often send the Mimecast data to Azure servers in our clients' tenant, so that the data is close to Microsoft 365 and never leaves their custody.

Every migration has "orphans" – invalid users, misspellings, strange BCC fields etc. that can't be mapped to current mailbox accounts. These will need to be assigned to a "catch-all" location in order to remain available for future eDiscovery.

As for leavers, you can either provision a temporary Microsoft 365 account for each (to be removed post-migration after placing the data on permanent hold – see Microsoft's Inactive Mailbox feature) or rehome their data elsewhere if available licences are limited.

Pro tip:
Migrations are always complex. Keeping a full audit log of the process is essential for investigating queries from users, security, chain of custody and compliance, ensuring nothing falls through the cracks.

Where you have live eDiscovery cases you'll need to identify and handle the transition of the eDiscovery workflow to Microsoft 365 as part of the project.

4. Import

Done by: your migration partner (or you)

Where and how you import email data varies depending on the source. These are the three main categories you'll need to consider.

Pro tip:
If possible, it's good practice to keep your Mimecast service running until your data is safe and sound in its new location.

Live users

Email items belonging to live users are typically migrated to a hidden "purges" folder in the Recoverable Items Folder (discussed earlier in this document). This prevents users from having all kinds of unexpected emails popping up in their active mailboxes and causing unnecessary confusion.

Leavers

Microsoft's inactive mailbox feature makes it possible to provision a Microsoft 365 account for each leaver, import their email data, place the data on permanent in-place hold and then delete the account again. This is a great way to retain leavers' data in an easily discoverable format without having pay for inactive licences indefinitely.

Pro tip:
Don't have spare licences to use for importing leavers' data? Try migrating leavers first and then reusing the same licences for your live users.

Legacy Journals

In order to map legacy journals accurately into Exchange Online (and keep everything in the right place for compliance and eDiscovery) you need to address the following:

- **Multi-instancing:** Single instanced journals will need to be converted back into a multi-instanced data stream with a copy of the original email for each recipient listed in the email envelope.
- **Deleted items:** Most journal migrations include emails that have been long-since deleted. If these belong to active users, they will need to be migrated to a hidden area to prevent them from reappearing in those users' mailboxes unexpectedly.
- **BCC data:** To preserve the confidentiality of BCC recipients, emails with BCC fields will need two versions generated – one for the sender including BCC details, and one for the recipients with no BCC info.
- **Distribution lists:** Historic distribution list information is mapped in the hidden header field included in the sender's version of the message.

Considering using shared mailboxes as alternative storage for legacy journals? Read this first!

We get it: exploding a single-instanced journal into the multi-instanced Exchange Online looks like a huge data volume and storage quote issue. Done right, this shouldn't be the case. But if you're thinking of using multiple shared mailboxes as a journal workaround, nonetheless, you should keep the following caveats in mind.

1. **It likely breaks Microsoft's licencing rules:**
   Documentation on this point is a little fuzzy, but all signs point towards Microsoft prohibiting the use of shared mailboxes for the preservation of email journals. If you're going this route, we highly recommend getting explicit permission first.

2. **You risk incomplete and/or complex eDiscovery:**
   Investigators typically put a hold on mailboxes relating to individuals under investigation. Shared journal mailboxes are frequently overlooked during this process, as investigators are unaware of their existence and/or contents. If and when shared mailboxes are included in eDiscovery, they often have to be included in their entirety as there is no way of knowing whose emails are where inside them. Improperly preserved metadata can also increase search complexity and decrease accuracy. All of this has a very real impact on risk, as well as eDiscovery timelines and costs.

3. **Governance can be tricky:**
   Being unable to separate email data by custodian makes it very difficult to apply records management policies on anything other than date. That means shared folders are usually subject to blanket "longest retention date" policies. That puts organisations at risk of retaining some data for far longer than required (or possibly permitted).

4. **You'll make clean divestitures difficult:**
   Shared folders also make for difficult divestitures, as they cannot be separated by operational unit.

A note on Exchange Online backup

No doubt you'll already have a backup strategy for Microsoft 365 in play, and if not, why not?

The most vulnerable content in Microsoft 365 is your files and folders within SharePoint, Teams and OneDrive. Therefore, your risk prevention and recovery tactics will likely focus on these workloads.

Gone are the days of traditional backup of mailboxes because the data resiliency architecture of Exchange Online delivers native high availability and business continuity.

As you expand the Microsoft 365 ecosystem to absorb legacy email it's often simply a case of ensuring your cloud backup platform includes Exchange Online.

Section 5
What's next?

What's next?

If you're wondering where to turn your attention next, we highly recommend taking a look at our *Microsoft 365 Security Assessment*.

During this workshop, we'll help you analyse your current security stance and security requirements and identify any gaps or opportunities that may have arisen pre- and/or post- migration. We'll also teach you how to configure and licence your Microsoft 365 environment to remediate any shortfalls.

It's a great way to ensure your post-migration security experience meets and exceeds that of your previous third-party service(s), and that you're truly taking advantage of everything your new environment has to offer.

Email preservation and migration workshop

A one hour workshop to guide you through all the elements covered in this book (and then some) and clarify the best strategy for your business. The agenda is customisable to your particular needs.

Find out more here and book your workshop now.

About Cloud Essentials

Getting your email data out of third party solutions and into your Microsoft environment is all in a day's work. We're long-standing and highly active Microsoft Content Services and Purview Compliance Gold certified partners, with decades of migration experience. What sets us apart is our commitment to achieving more than just a successful migration.

Our goal is to help you fully leverage the functionality available within Microsoft to not just replicate, but improve on the capabilities you had before. Together, we'll help you achieve a secure, compliant and consolidated environment, and lay the foundations you need to take advantage of future innovations.

What's included?

Clarity on Microsoft's capabilities and security and compliance approach.

Design and deployment of the migration to Microsoft online or alternative locations, including legacy data extraction, preparation, mapping, clean-up and import.

Future proof progression that positions you for optimal security and compliance, and prepares you for future innovations and technologies.

A competitive fixed price for the deployment phase.

Advice on security and compliance from both technical and legal experts.

Alternative archives with ongoing journaling, if necessary.

A fully managed, end-to-end process led by an experienced project manager.

Our favourite challenges:

Embracing Microsoft cloud for email retention requires a mind shift from the old days of traditional archives. Especially if you're fully embracing Microsoft 365 security features.

As you transition from your third party solution we can help you with:

- Legacy email with no logical home in Microsoft 365
- Surfacing legacy content for eDiscovery
- Clearing out the ROT (redundant, outdated, trivial)
- Aligning with retention and compliance
- Establishing ownership of emails (senders/recipients)
- Transferring from third party security features to native Microsoft 365

Get in touch

Cloud
Essentials

Our Locations

Bristol, UK

hello@cloudessentials.com
+44 (0) 1275 772490

40 Berkeley Square, Bristol
BS8 1HP
United Kingdom

Johannesburg, SA

hello@cloudessentials.com
+ 27 (0) 10 5912323

Unit 12, Somerset House, 11 York
Street Kensington B, Randburg, 2195,
Johannesburg, South Africa

Cape Town, SA

hello@cloudessentials.com
+27 (0) 11 781 2323

The Pavilion, Corner of Dock & Portswood Rd
V&A Waterfront, Cape Town, 8001
South Africa

www.cloudessentials.com