xift

5 difficult questions to ask your email security provider

Contents

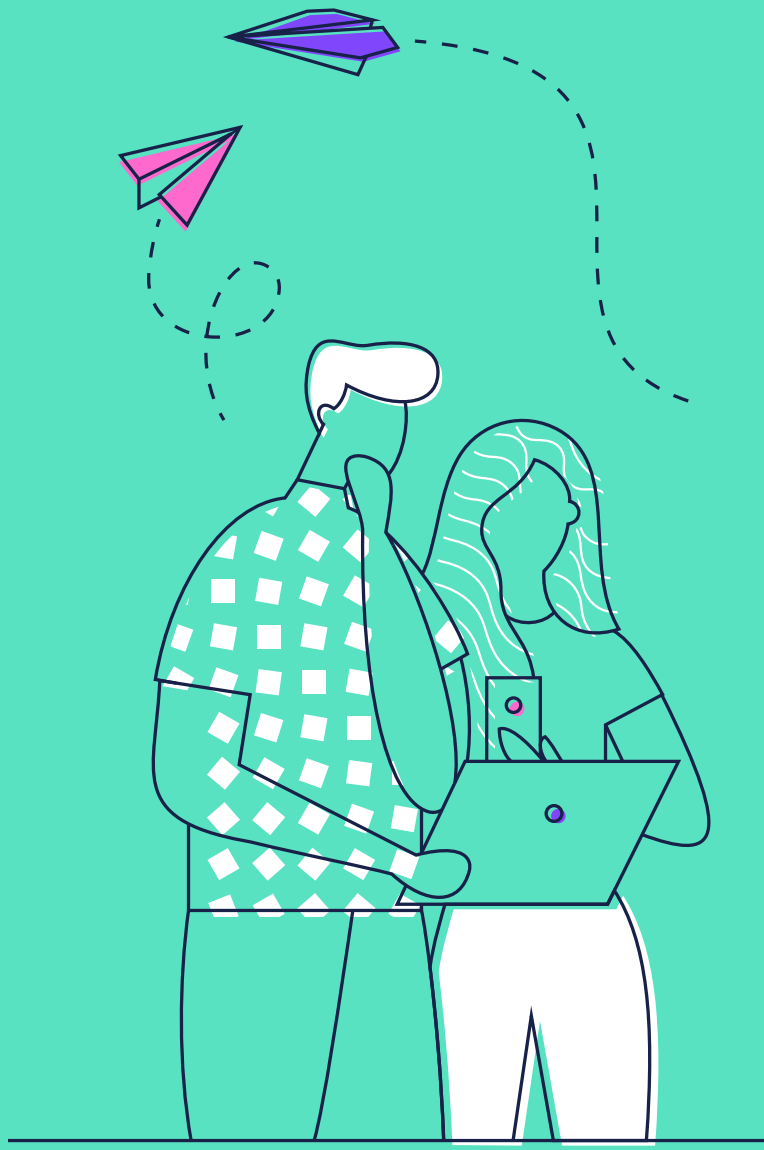
You’re paying too much for a poor quality service

Email is the go to method for communicating and collaborating at work. It’s also the most likely platform to face malware and phishing attacks.

The need for bulk email monitoring, filtering and archiving is universal. Yet, unlike other IT services, high market demand isn’t driving improvements in service quality. The need to protect, filter and archive large volumes of emails hasn’t changed. Yet many of the tools available are getting more feature-heavy and complicated to use.

It’s time for businesses with legacy email security and archiving systems to step back and reassess what they need from the solution - especially in context with newer cloud platforms.

These 5 questions will reveal whether you’re getting value for money from your provider. If they don’t have the answers, it could be time to move on.



1 Here's the problem with unnecessary features: you still pay for them.

Why should I pay for features I don't need?

This is the killer question for many email security and archiving providers. Fierce market competition has produced an arms race between vendors to bloat their services with features and functions that are rarely needed and almost never used.

It's price, rather than feature-count, which influences organisations investigating email security and archiving services.

The introduction of the utility computing model has changed expectations. IT services must provide transparent value to the business.

This means individual systems must become more focused, not more broad, in the ways they address challenges.

Applied to email security and archiving services, we can break down the needs they must address into 3 core competencies:

1. Security (Anti-Virus & Anti-Spam)
2. Continuity
3. Archiving

Services that provide robust solutions to these three core areas, whilst removing as much complexity as possible, will see the highest rates of adoption in the future.

2 Cloud native email security services offer the best of both worlds: enterprise-class security and a straightforward user experience.

How am I protected from spam and viruses?

Spam and virus attacks have come a long way in the past decade - malware attack vectors have shifted towards targeting individuals.

However, it's a fallacy that security software must become more complex to keep pace with more sophisticated threats.

Quite the opposite – there's a risk that feature-heavy email security solutions obscure the best practice principles they allegedly promote.

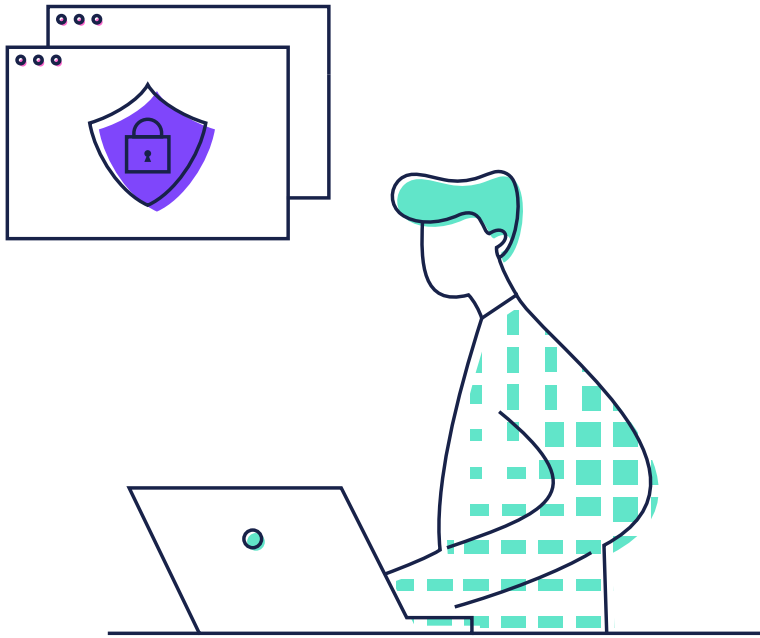
A common symptom of feature bloat is management complexity. If left unchecked, this can be just as risky as having no security at all. Heavily customised admin policies and user-permissions are created with the best intentions, but they regularly go untouched beyond set up.

This complexity is more than overworked sysadmins need. Consequently, these solutions often fail to evolve with the business and end up posing more risk than convenience.

Conversely, cloud native email services can offer the best of both worlds: enterprise-class security and a straightforward user experience.

Cloud native services should also be flexible. This means mailboxes are transparently priced, and can be added or subtracted at will, with no additional charge.

Services that balance these factors can deliver the best protection, whilst reducing management time.



3 Many services today aren't designed to cope with factors like data sovereignty.

Where's my data?

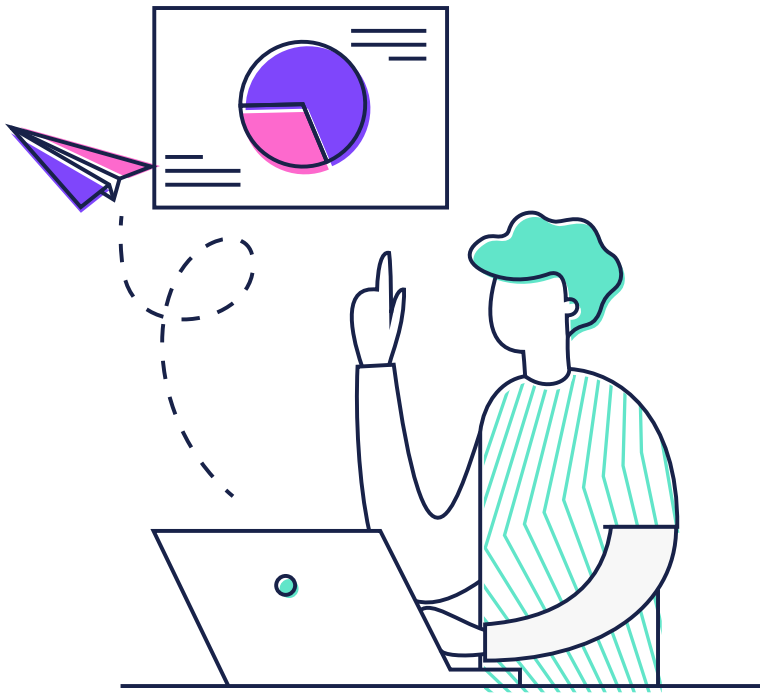
As a critical office function, the location of email data is a common concern for organisations considering cloud email security and archiving services.

However, given how infrequently organisations tend to assess their email security and archiving solutions, many services aren't designed to cope with factors like data sovereignty. These can seriously impact an organisation's ability to access its data.

Broadly, data sovereignty refers to the local laws, conditions and security standards that stored data is subject to. For instance, is your archived data stored in a country subject to the USA Freedom Act? What about the physical location? How vulnerable is it?

As more businesses adopt cloud-based email security and archiving services, the impetus will be on cloud service providers to operate with transparency. The location of stored data, the accompanying conditions it is subject to, and the degree of access customers have must be clear and available.

Equally, customers in the secure email and archiving market must interrogate potential cloud services thoroughly. Opt for solutions built on established public and true-cloud environments to reduce risk and ensure accountability.



4 Traditional solutions often limit the size and number of mailboxes protected.

Why am I paying so much for storage?

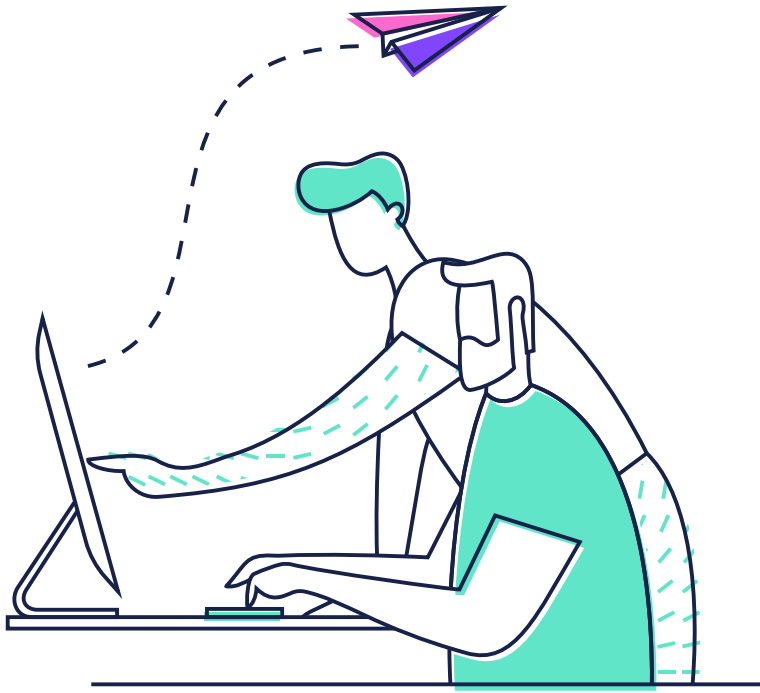
After licenses, storage is one of the largest costs of legacy email archiving solutions. Indeed, email is often the chief cause of storage growth across the whole organisation. And there's no indication that growth rates are slowing.

This isn't a problem that can be resolved with management and archiving policies alone, no matter how efficient. It requires flexible, cheap and tiered storage.

Traditional solutions often impose strict limits on the size and number of mailboxes protected and 'reasonable use' clauses around storage volumes. These restrictions can work against the growing needs of the market, and services that use them will struggle to scale. Fortunately, these challenges around size and availability form an excellent use case for the flexibility and scalability that cloud resources deliver.

The next few years will be interesting, as the differences between 'cloud-enabled' and 'cloud-native' applications become apparent.

In the same way, as some major vendors have 'cloudified' their standard email security and archiving services, they will have to compete with the flexibility and scalability of newer, genuine cloud-native services.



5 Traditional archiving solutions can't deliver flexibility without incurring costs.

How do I get my data back?

Businesses need uninterrupted access to email data. Even rarely-accessed and archived data needs to be accounted for, due to compliance and governance.

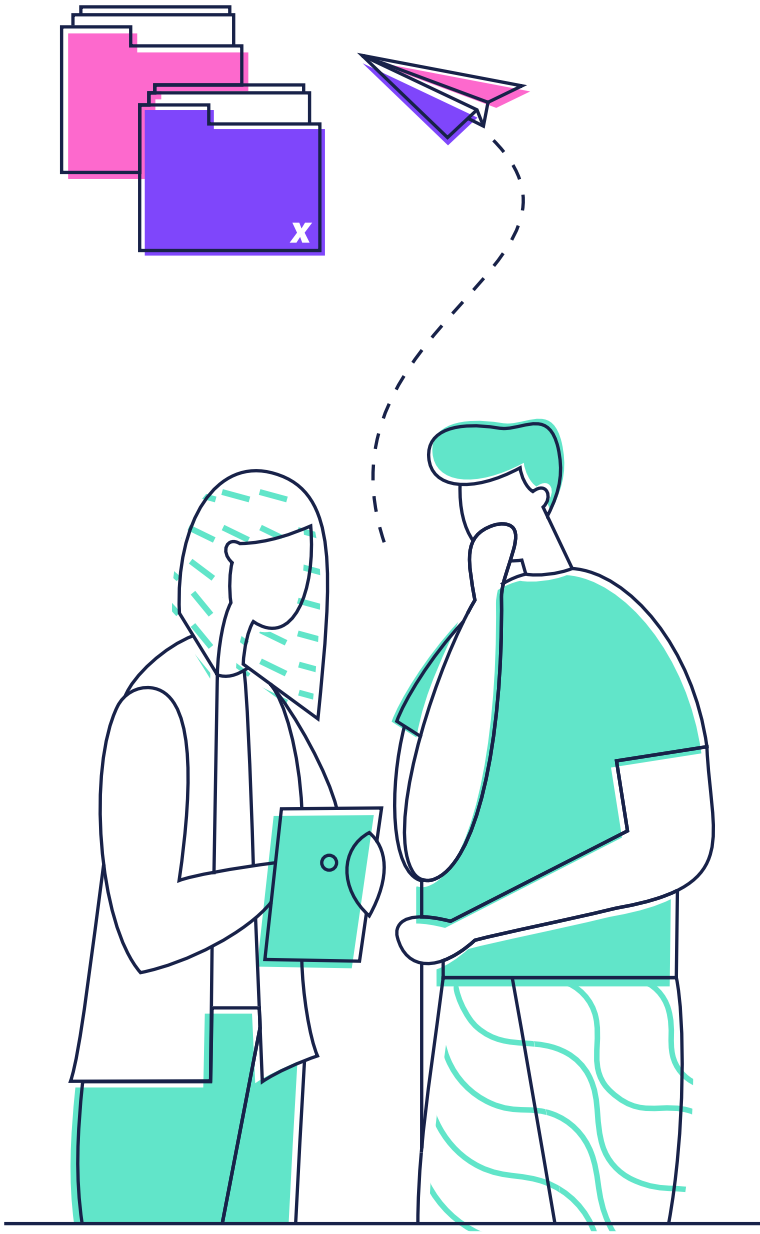
Unfortunately, traditional archiving solutions were not designed with the flexibility to retrieve, access and migrate archive data without incurring significant costs. The difficulties of accessing, let alone moving, data can paralyse businesses, and prevent them from meaningfully considering alternatives. This can result in a kind of unofficial vendor lock-in.

How easy is it to retrieve your archived data? And at what price? Were the terms ever discussed? It's worth asking these questions: your archived data could be much less accessible, let alone portable, than you thought.

As a general rule, cloud native services have been built from the ground up. They take advantage of the flexibility, scalability and low costs that established cloud infrastructures provide.

This flexibility extends to data portability – cloud storage offers you greater visibility, easier management and better control of archived data.

See how Xift can help your email security needs.



A bit about us

Xift was created to give businesses peace of mind. Large or small, you know your email is protected and will continue through disruption. The Xift team is dedicated to making that happen.

Our founders hail from business continuity specialist, Databarracks, HP and MessageLabs.

We bring experience in enterprise tech, focussed customer service and email security to deliver a modern solution fit for today's challenges.

With the team's years of combined expertise, your email is in safe hands.

Get in touch

0800 058 8555
sales@xift.com
www.xift.com

xift