TitanHQ™
ArcTitan

Mind the Gap:
How Microsoft Exchange Online Archiving compares to ArcTitan Email Archiving.

eDiscovery - legal protection - regulatory compliance

1. Introduction

“Email archiving solutions must be comprehensive and accessible. A flexible design that solves complex use cases where compliance and eDiscovery come into conflict is essential. This is why TitanHQ made ArcTitan highly configurable, with unlimited growth, and simple to use.”

In our hyperconnected world, where social media grabs so much attention, it may seem as if email is an outmoded technology. However, this could not be further from the truth. Email reigns supreme as a communication channel and is an essential business communication method, with over 347 billion emails sent and received daily in 2023. Email use seems unlikely to decrease anytime soon, with almost 400 billion emails expected to be sent and received daily by 2026[1]. Because emails often contain sensitive and proprietary information, this technology has come under the scrutiny of laws and regulations. Email is an information system that must be preserved for business continuity, regulatory compliance, and legal reasons.

This preservation comes under the auspice of email archiving systems. In February 2023, over one million companies worldwide used Microsoft 365. So, it’s a no-brainer to use the in-built email archiving of Office 365 via Exchange Online Archiving (EOA). However, an organization may have better email archiving choices as email archiving must be considered a holistic system.

Source[1] - STATISKA

This white paper dives into the whys and wherefores of email archiving and will include discussions on the following:

- Why email archiving is needed
- Misconceptions in email archiving
- Compliance, laws, and email archiving
- Exchange Online Archiving (EOA) for Outlook 365 and its limitations
- ArcTitan email archiving solution
- A comparison between EOA and ArcTitan

347 billion

Over 347 billion emails were sent and received daily in 2023.

2. Why does an organization need to archive emails?

eDiscovery - legal protection - regulatory compliance

A business turns upon the information it generates and communicates. This information must be easily accessible, secure, and have demonstrable integrity. As email enters or leaves an organization, a data trail is generated. By archiving emails, this trail is auditable, and the data is available. An email archiving system will preserve email data, ensuring it is immutable and tamper-proof. Security of the stored emails should be an intrinsic value of any email archiving system. However, the reasons for archiving emails extend beyond a simple repository; as such, an **email archiving solution is an ecosystem of capabilities** that preserve and deliver the following:

Data and business continuity: access to emails is critical for business communications. Organizations must be able to quickly and accurately locate an email conversation or attachment to keep business flowing.

Recovery: unfortunately, attacks that involve data integrity, such as ransomware, can interrupt this flow. Email archiving must provide fast, accurate retrieval of emails and attachments.

Intellectual property (IP) preservation: emails and attachments often contain IP. Email archives that are accessible and secure preserve IP and allow it to be quickly and accurately retrieved when needed.

Proof of communications: legal actions often require evidence. eDiscovery provides proof of communication to help organizations deal with legal requests. Organizations that are fully prepared can handle eDiscovery requests promptly.

Regulatory compliance and law: email is a heavily regulated area that can be complicated for a business to comply with. Many jurisdictions come under a Venn of regulations and laws that an email archiving system must handle correctly.

This ecosystem of capabilities is not an on-off switch. **Email archiving is a must-have, not a nice-to-have,** but a solution must embrace and deliver all these attributes in a controllable and accessible way.

3.Misconceptions in email archiving

Laying down the foundation stone of email archiving is vital in establishing what capabilities are critical to providing best-practice email archiving. Having a handle on misconceptions about how email archiving works and the requirements of such a system helps to ensure that you choose the ideal email archiving solution for your needs. Some of the most common misconceptions that lead to the incorrect email archiving solution choice include the following:

Email archiving is just a backup system.

Archiving emails is not simply about backing up emails. Placing emails into a separate Archive folder does not make those emails comply with regulations or make them easily discoverable during legal cases. Legal requirements, regulations, and business continuity must have tamper-proof evidence that emails are preserved unchanged. Also, email archiving systems must have granular controls over search and retrieve and supply a complete audit trail.

Any Archive can achieve legislative compliance.

Email archiving systems must expand to handle the vast number of emails a business generates. Auto-expansion capabilities can still be limited, meaning emails cannot be archived seamlessly, potentially leading to an incomplete archive. Unless the email archiving solutions have tamper-proof capability, emails could be changed, making them meaningless in the event of legal action.

4. Compliance, laws, and email archiving

Email archiving must be done in a manner that covers a variety of laws and regulations. Unified and comprehensive email archiving solutions must provide functions that meet regulatory requirements. These functions should include the following:

- Documentation and traceability for audit and investigations
- Business continuity and disaster recovery
- eDiscovery for legal requirements in litigation
- Records management
- Encryption and access control to emails and attachments
- Secure storage

Sometimes, specific regulatory requirements can conflict with the remit of robust email archiving; for example, the EU's General Data Protection Regulation (GDPR) includes the "Right to be forgotten." This conflicts with the need to retain data for eDiscovery. Meeting this requirement while ensuring the retention of data can take much work. As you will see as you read this paper, while Microsoft Exchange Online Archiving (EOA) fails to ensure these conflicting requirements are met, ArcTitan's flexible design allows conflicting requirements to be adhered to.

Some of the laws and regulations that affect email archiving are outlined below. This mosaic of regulations and laws underpin the need to archive emails in a way that allows eDiscovery but protects information, demonstrates the importance of a flexible design remit for email archiving.

400 billion

emails are expected to be sent and received daily by 2026.

General Data Protection Regulation (GDPR)

The GDPR includes specific requirements that impact the protection and restoration of personal data (including email-based data). These requirements come under the list of data subject rights and data protection. For example, personal data, including archived email-based personal data, must be secured and access controlled. In addition, article 32 of GDPR states that the organization must have the "ability to restore the availability and access to personal data promptly in the event of a physical or technical incident." [2]

Locating and deleting a customer's data is a core tenet of GDPR, covered under the data subject right to be forgotten. Any customer or other personal data in an email must be easily and quickly searchable to enable this GDPR rule to be undertaken. Audited deletion is a crucial requirement of GDPR. Organizations must prove that all emails have been deleted when requested, for instance, during a Subject Access Request (SAR). Article 17 states:

> **"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay(...)."**

Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA)

FINRA and SEC are the two central regulatory bodies for financial services in the USA. Both bodies require stringent email retention regulations. The requirements revolve around the security, integrity, and accessibility of financial information in emails sent and received by financial institutions and their associates.

SEC Rule 17a-4 requires financial services organizations to archive emails, and archived emails must be immediately accessible for two years and stored for at least six years. [3]

In 2017, 12 companies, including Well-Fargo and RBC Capital Markets, were fined a combined $14.4 million by FINRA for "significant deficiencies relating to the preservation of broker-dealer and customer records in a format that prevents alteration."[4]

Email archiving is a must-have, not a nice-to-have

- **Data and business continuity**
- **Recovery**
- **Intellectual property (IP) preservation**
- **Proof of communications for legal actions**
- **Regulatory compliance and law**

Sarbanes–Oxley Act (SOX)

The Sarbanes–Oxley Act of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations[5].

Under SOX, organizations are required to establish and maintain internal controls and procedures for financial reporting. These controls extend to retaining and preserving records, including email communications and material to financial statements or audits. The Act emphasizes the importance of accurate and reliable record-keeping and mandates that these records be accessible for inspection by auditors and regulatory bodies.

To comply with SOX, organizations must implement measures to ensure the integrity, security, and accessibility of email data. This includes implementing email archiving solutions that capture, retain, and protect email communications in a tamper-proof manner. Organizations must establish policies and procedures to retain and manage email records, including defining retention periods, access controls, and audit trails.

Furthermore, SOX requires organizations to demonstrate the effectiveness of their internal controls and processes through regular audits. Auditors must be able to access and review relevant email records to examine financial reporting accuracy and compliance. Organizations should ensure that their email archiving solutions enable efficient search and retrieval of email data to facilitate audits and regulatory inquiries.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA applies across a broad range of organizations, including most healthcare providers and healthcare contractors. HIPAA has two core rules that apply to email-based data: the Security Rule and the Privacy Rule. [6]

The HIPAA security rule requirements imply that an email archiving solution is needed as covered organizations must securely back up exact copies of electronically protected health information (PHI), and this information must be able to "restore any loss of data." The retention period for emails is six years, and archived emails must be accessible for audit. Audit controls prevent inappropriate access, alteration, or deletion. The HIPAA Privacy Rule allows patients to request a copy of their PHI, which must be available within 30 days.

Source[2] - GDPR

Source[3] - SEC

Source[4] - Finra

Source[5] - Sarbanes

Source[6] - HHS

Further examples of email retention times (USA only)

Legislation	Industry	Email retention period
Freedom of Information Act (FOIA)	Federal, state, and local government bodies	Three years
Food and Drug Administration (FDA) Regulations	Pharmaceutical and food	Five to 35 years
Payment Card Industry Data Security Standard (PCI DSS)	Credit cards and related processors	One year
Federal Deposit Insurance Corporation (FDIC)	Banking	Five years
Federal Communications Commission (FCC)	Telecoms	Two years
Gramm-Leach-Bliley Act	Banks and Financial Institutions	Seven Years
Internal Revenue Service (IRS) Regulations	All companies	Seven Years

> “
>
> **Archiving alone is insufficient to support a legal case; tamper evidence is essential, this is costly, and difficult to achieve in EOA.**

5. Exchange Online Archiving (EOA) and its limitations

Microsoft Exchange Online Archiving is a cloud-based email archiving solution that works directly from an Outlook client. The adoption of Microsoft 365 is buoyant, and when companies adopt one part of MS 365, they often opt to deploy other elements in the suite. Microsoft Exchange Online Archiving (EOA) is one such element. EOA is a Microsoft 365 cloud-based, enterprise-class archiving solution. Organizations with licensed Microsoft Exchange Server 2019, 2016, or 2013 or subscribe to specific Exchange Online or Microsoft 365 plans can license EOA. On the surface, it would make sense to license this in-built email archiving for Outlook 365. **However, best practice email archiving that meets compliance and eDiscovery is rarely solved as a bolt-on solution. Companies who use EOA should be aware of some shortcomings of the solution.**

General Limitations of EOA

The complex landscape of Microsoft Exchange Online Archiving licensing.

> **“ We regularly see full primary and archive mailboxes where auto-expansion is enabled and increasingly find that the busiest mailboxes fill the expanded online archive. ” - TitanHQ.**

One of the complexities inherent in EOA is the licensing model. To utilize EOA online archiving, you must have the correct license. Email is archived in an archive mailbox known as an In-place Archive. One of the inherent problems with Exchange Online Archiving is understanding what license you should choose for your business needs. EAO is available for the following packages, although there are varying limitations within packages:

License plan[7]	User archive mailbox limits
Microsoft 365 Business Basic and Standard	50GB
Microsoft 365 Business Premium	1.5TB
Microsoft 365 Enterprise E3/E5	1.5TB
Office 365 Enterprise E1	50GB
Office 365 Enterprise E3/E5	1.5TB
Office 365 Enterprise F3	Exchange Online Archiving add-on Required
Exchange Online Plan 1	50GB
Exchange Online Plan 2	1.5TB
Exchange Online Kiosk	Exchange Online Archiving add-on Required

Source[7] - Learn.microsoft

Source[8] - Learn.microsoft

Capability and storage limits

"One of the core issues of storage limitations in EOA means that when the archive storage limit is reached, archiving stops." - TitanHQ.

Gapless and uninterrupted archiving is essential for many compliance scenarios, and limited archive storage can prohibit this. Exchange Online Archiving mailboxes are limited in size, and archiving stops once the limit is reached for a given mailbox. This can be mitigated using the Auto-expanding Archive feature to enable an archive mailbox to grow to 1.5TB. However, the auto-expanding archive has a maximum expansion rate of 1GB/day and prevents the mailbox from ever being delegated or restored.

eDiscovery and user control

"Archiving alone is insufficient to support a legal case; tamper evidence is essential, costly, and difficult to achieve in 365. For example, users can override default policy, and admin actions are not logged." - TitanHQ

An essential element of eDiscovery to support legal actions is traceability and a robust audit trail. As noted in the analysis by TitanHQ, EOA allows an individual user to override default policy settings, causing issues in eDiscovery and questions around traceability and tamper-proofing of located evidence. The combination of a lack of traceability and eDiscovery, with the fact above that archiving, stops when an archive storage limit is reached, can result in an information gap, which can be catastrophic for compliance and lead to adverse legal outcomes.

User training

"Messages not in litigation hold can be edited or deleted from the archive by users or via the 365 portal or PowerShell by administrators." - TitanHQ.

Users might change administrator-enabled policy settings because of a lack of understanding of the archive system unless significant effort is expended configuring and maintaining retention policies in 365. According to Microsoft, user training for the Microsoft EOA is essential, which recommends that companies "inform them (users) about the archive policies that will be applied to their mailbox and provide subsequent training or documentation to meet their needs." By contrast, ArcTitan is intuitive and designed to suit compliance models with minimal configuration. This is achieved by journalling all mail and taking the user out of the process.

What about inactive mailboxes?

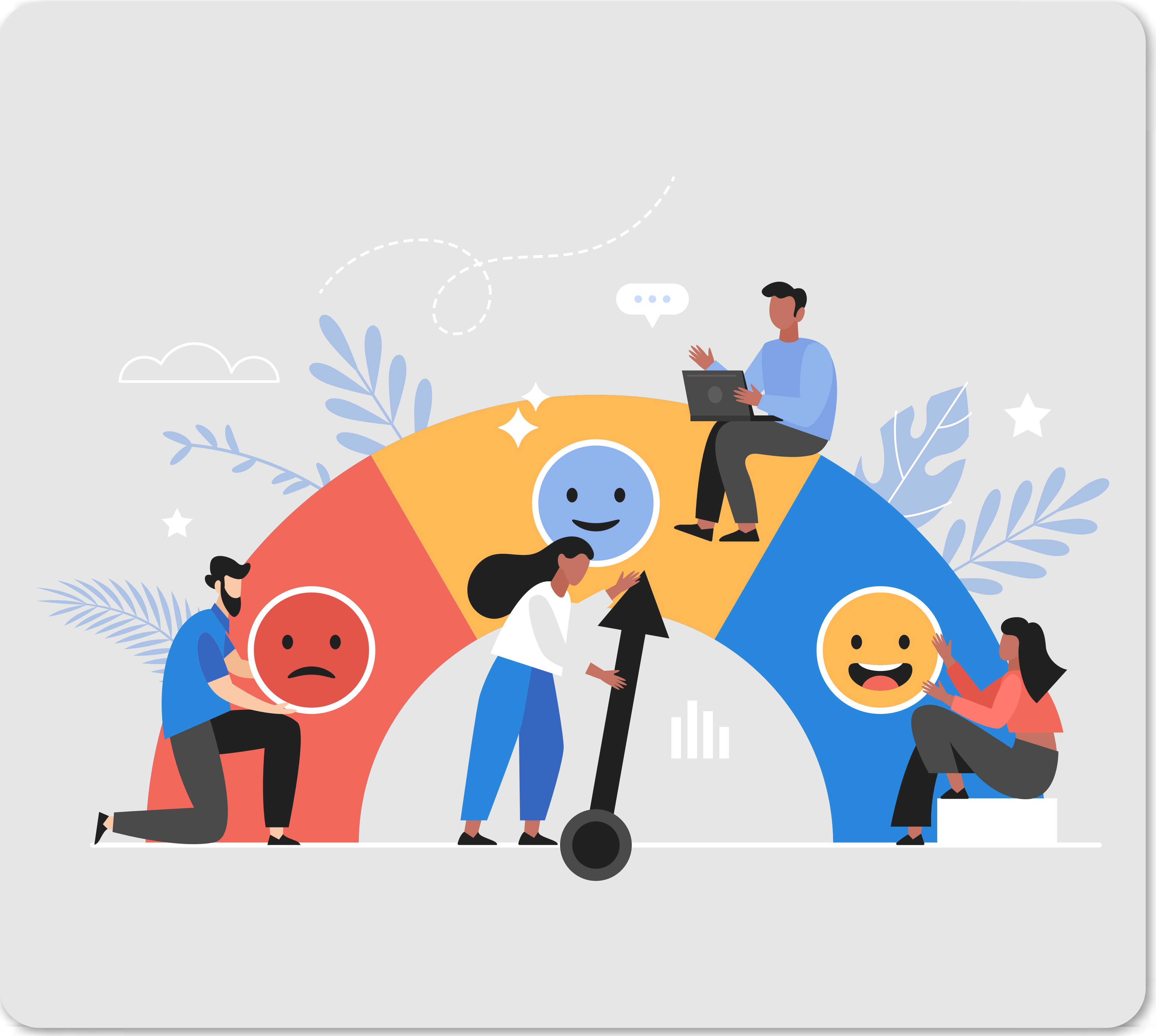
“Auto-Expanding Archive can never be disabled, and the mailbox cannot be restored or recovered if made inactive.” - TitanHQ.

Email must be preserved to avoid exposing an organization to legal and financial risks that can lead to adverse legal judgments, sanctions, or fines. Microsoft EOA uses the concepts of “Litigation hold” and “In-place hold” for inactive mailboxes. A Litigation hold preserves all items in a mailbox, whereas an In-place hold is associated with search queries to determine the content to be preserved. However, some overriding issues cause issues for inactive mailboxes that can limit eDiscovery; this includes:

- Inactive users must be licensed to retain access. The existing archive will persist, but new mail will not be archived unless the mailbox is licensed.
- Litigation Hold & Auto-Expanding Archive prohibit delegation of inactive mailboxes.
- Messages not in Litigation hold can be edited or deleted from the archive by users or via the 365 portal or PowerShell by administrators unless retention policies are configured.

Exchange Online Archiving (EOA) usability

“To be effective and comprehensive, email archive search must be accessible and unified across Outlook and Web for all user types.” - TitanHQ.



Usability is an essential ingredient for any complex service, including email archiving. Usability typically revolves around accessibility and the user interface that controls policies, settings, and other configurations. Not surprisingly, the search capability of eDiscovery is where usability meets accessibility. Having an intuitive interface that allows complex and deep searches to take place using a unified interface is critical in accurately responding to legal challenges and providing evidence of compliance. There are four main places to search for emails in Microsoft 365:

- Outlook Search
- 365 Content Search
- eDiscovery Standard
- eDiscovery Premium

Each has limitations; for example, the standard search limitation includes a limit of 1000 items found across all user mailboxes that can be displayed. Any organization that wishes to avoid limitations must purchase a license that offers eDiscovery Premium, such as Microsoft 365 E5 or F5.

"The user experience is inferior. Users must click through several screens before being able to complete a search, and then the search itself takes at least 10 minutes; sometimes longer searches can take hours." - TitanHQ analysis of EOA search experience.

The user interface for 365 eDiscovery adds complexity to email archive search. A different UI is used with each solution, and other indexing methods generate variable results. This lack of unification across systems results in further restrictions and a variance in scope. Unfortunately, the positive aspect of 365 eDiscovery, which offers rich features, is lost in the lack of intuitive search with an unfriendly UI and poor accessibility. In other words, EOA can provide a good eDiscovery service, but configuration and usability costs are intensive and time-consuming, and training needs are heavy.

Microsoft EOA and compliance limitations

TitanHQ evaluated Microsoft EOA based on our extensive knowledge of regulatory compliance requirements for email archiving. The results below demonstrate severe limitations when using EOA to comply with regulations:

The larger the organization, the bigger the hurdles

Limits on storage and search can cause larger enterprises compliance headaches. Limitations such as 50GB eDiscovery Result Limit and 10,000 mailbox eDiscovery Search maximum means that enterprises that may have many 10's of thousands of mailboxes will meet a barrier to compliance. The result is that the enterprise will be required to perform multiple, resource-hungry, and time-consuming searches.

Audit and traceability

Poor audit and traceability of administrator actions is an area that can cause compliance issues. Audit logs are turned off by default, so none of these actions would leave a trail:

- Admin login
- Disable Litigation Hold
- Delete email
- Enable Litigation Hold

Archiving alone is insufficient to support a legal case; tamper evidence is essential, this is costly, and difficult to achieve in EOA.

Logs only generate alerts with additional configuration or the use of third-party tools.
In addition, audit logs are deleted after:

- 90 days by default
- one year for users assigned an E5 license
- ten years for users with an “E5+10 Year Audit Add-on” (additional monthly cost)
- Logs can be shipped to a 3rd party SIEM or compliance system, which is an additional cost.

GDPR and the right to be forgotten

The right to be forgotten is a complex requirement to meet. The EOA falls short of complying with this GDPR mandate as it states that “…in the context of deleting Customer Content in response to a DSR: if an item is hard deleted from a content location that is on hold, the item is not permanently removed from Office 365. That means an IT admin could conceivably recover it.”

6. ArcTitan for email archiving

ArcTitan delivers cloud-based email archiving designed to provide email storage at lightning-fast speed backed by robust security. The flexible design of ArcTitan allows it to meet even complicated regulatory requirements, such as GDPR’s right to be forgotten. ArcTitan integrates directly with Office365, automating email archiving and making the process simple and reliable. This ‘set and forget’ capability removes human error and makes regulatory compliance simple and reliable. **Some of the features of ArcTitan include**

Scalability and performance

Unlike even the most costly of EOA plans, ArcTitan has no limits on email storage. ArcTitan storage is elastic, growing with your email archive. The size of the archive is independent of performance. Emails are archived in real time and automatically sent to the archive. Data security is paramount; encryption is used during transit and at rest (storage). Duplicate content is removed, and emails are compressed to reduce storage space and improve search efficiency.

Usability and accessibility

The ArcTitan archive is unified and accessible using almost any email client or a web-based interface. Access control is through an advanced delegation mechanism compatible with LDAP and Active Directory. Administrators can create a permission hierarchy for critical employees, reducing overhead on IT.

Data protection and compliance

ArcTitan enforces data encryption (in transit and at rest) during transfer and storage. ArcTitan enforces robust authentication and access control to protect data and tamper-evident audit trails to identify any unauthorized alterations to archived emails. Automation inherent in ArcTitan helps create reliable archiving to ensure regulatory compliance. In addition, the powerful and fast search feature allows ArcTitan to accommodate requests for information for legal or compliance reasons swiftly. Also, a comprehensive audit trail delivers the documentation needed to demonstrate compliance.

Speed

ArcTitan automates archiving, and search is fast; emails can be retrieved instantly. ArcTitan load performance handles more than 200 emails from the email server per second. Searches can be combined and saved, and multiple searches can be performed simultaneously.

Cost-effective

ArcTitan operates a flexible “pay as you go” email archiving model. Per live user subscription only with savings of up to 75% of email storage space.

7. EOA and ArcTitan comparison

	Exchange Online Archive	ArcTitan Archive
Growth Limit	1GB/day/mailbox	Unlimited
Storage Limit	100GB/mailbox (1.5TB with auto-expansion)	Unlimited
Automatic Archiving	Default is content > 2 years old, can be configured	All sent and received mail
Tamper Evidence	Archived items are editable and can be deleted by the user unless additional policies are configured.	No content is editable, and deletion requires authorization by a data guardian.
Inactive User Licensing	Inactive users must be licensed to retain access to their mailboxes and continue archiving.	Mail is archived regardless of licensing, and inactive mailboxes are not charged for.
Litigation Hold	A litigation hold can be enabled to prevent content deletion.	Litigation hold is only necessary to prohibit deletion by privileged users or by retention policy.
Search Performance	Slow, 20 minutes to find 2000 items from 10 mailboxes.	Extremely fast, under a second for the exact search on the same data.
Search Limits	50GB, 10,000 mailboxes, five jobs	There are no search limits, and 50,000 item export limit (can be exceeded via support)
Search UI	No preview, multi-window search parameters, cannot review results without export.	Instant preview, single pane UI, review, sort, and filter results before managing or exporting.
GDPR DSR Compliance	Litigation hold must be disabled to ensure deletion, breaking the compliance model for 21 days.	Default settings enable DSR to be completed and logged without affecting the compliance model.
Audit Logs	90-day default retention, limited actions logged. E5 required to improve.	All admin and privileged actions are logged automatically, and logs and transcripts are retained permanently.

TitanHQ ArcTitan vs

ArcTitan vs EOA costs

The cost differential between the two solutions is vast. Office 365 EOA costs cover requirements needed to meet compliance and legal including:

- 365 E3/E5 Licences + Add-ons
- Skills investment for admin and compliance staff
- Days to weeks of configuration effort
- Significant ongoing management costs
- Lost productivity for slow eDiscovery and Export
- Elevated risk of non-compliance
- Backup costs

ArcTitan's comprehensive, dedicated email archiving solution, which integrates directly with Office 365, starts from $4.59 per user per month. To achieve the same functionality as ArcTitan, this would require a global uplift from E3 to E5 and the 10-year logging addon for every admin and privileged user.

Want to know more about achieving comprehensive email archiving for compliance and legal? Contact TitanHQ for a demo of ArcTitan today.

GET IN TOUCH