

PROOFPOINT ENTERPRISE ARCHIVE FOR FEDERAL AGENCIES

NEXT-GENERATION ARCHIVING

Proofpoint Enterprise Archive is a FedRAMP authorized, cloud-based email archiving solution. It provides a central, searchable repository to help federal agencies simplify legal discovery, respond to FOIA requests, and implement email records management according to NARA Capstone guidance. With Enterprise Archive, you know where your data is stored and you can quickly collect, search and retrieve that information on demand.

COMPLIANCE AND DISCOVERY FEATURES

Enterprise Archive is designed with the features, security and performance to meet the standards required for records management and discovery readiness for both Microsoft Exchange and Office 365.

Easy-to-Enforce Retention Policies

Enterprise Archive's policy management capabilities help you create, maintain and—most important—consistently enforce information retention policies. Enforcement of these policies is automatic and based on configurable rules. When data has reached the end of its retention period, high-performance disposition allows you to quickly purge data. And every policy change and disposition action is tracked, giving you a truly defensible disposition process.

Fully Automated Legal Hold Processes

With Enterprise Archive, your litigation hold process is simple and fully automated. Your legal team can instantly preserve data in legal holds beyond their assigned retention periods. You can assign access to search exclusively within data assigned to a hold. And an easy-to-use interface provides you with full reporting and an audit trail. These unique features give you more efficiency and transparency in managing data-preservation requirements.

Fast Access for Early Case Insight

Enterprise Archive's high-performance search features give you insights to help you refine discovery strategies and respond to FOIA requests. Your legal team can easily search in near real time across email and within more than 500 types of attachments. Instant access to data greatly reduces the time and cost of collecting, filtering and searching data collected through restored backup tapes, imaged hard drives and PST files.

Fast Self-Service Export

Enterprise Archive lets your legal team quickly export large volumes of relevant content in PST, CSV, Relativity or EDRM XML formats—without professional services fees. The system can also automatically upload the results to third-party service providers. This allows you to avoid delays and questions about compromised chain of custody.

Intelligent Supervision for Employee Monitoring

Proofpoint Intelligent Supervision is built on top of Enterprise Archive. This allows your staff to systematically review messages. Content can be selected for review—either as potential policy violations or through a random sampling process. And then it's automatically routed to the users authorized to act on it. Intelligent Supervision also provides reports that help you manage the review process and keep you ready for audits.

INNOVATIVE CLOUD ARCHITECTURE DESIGNED FOR SCALE AND MAXIMUM SECURITY

Enterprise Archive securely archives information in our innovative, FedRAMP Authorized, grid-based cloud storage infrastructure. This means you always have easy access to your data. You get the performance, scalability and cost savings of the cloud, along with the highest levels of security and privacy of archived data.

Failsafe Archiving Process

Unlike other cloud solutions, Enterprise Archive's unique "pull-and-confirm" method pulls messages from the journaling mailbox. That means your email will never be lost, even if the appliance or network goes down. We confirm that items received within the archive match those sent from the journaling mailbox before removing them from the journal. This ensures a complete, inclusive record within the archive.

Search Performance Guarantee

Our search performance is guaranteed. This ensures you have reliable access to archived data in seconds. Unlike on-premises solutions that experience performance degradations and require continual hardware upgrades as the data store grows, Enterprise Archive delivers scalability on demand. Our grid storage architecture and parallel search technology provide you with real-time search performance, regardless of how large your archive grows or how complex your searches get.

The Most Secure Archive in the Industry

Utilizing our optional patented DoubleBlind Key Architecture, we ensure data leaving your site is always encrypted. You get uncompromised data security—your information is protected both in transit from your environment and while under management within our cloud infrastructure. And data is encrypted with an encryption key that is unique to you. Optionally, you can manage the encryption key for full control over who can access your data within the archive.

DELIVERED AS A FULLY MANAGED SERVICE

This breakthrough approach, coupled with our operational and security practices that are SSAE-16 certified, gives you the assurance of complete data privacy and uncompromised security. And not just for our physical facilities, but for the service itself. This includes our global data centers and a world-class support and operations infrastructure that can proactively identify issues and take action—in many cases before you're aware of the problem. And our market-leading customer renewal rates and customer satisfaction ratings reflect our responsive, seamless customer experience.

CERTIFICATION

SSAE-16 Type II, FedRAMP

CONTRACT VEHICLES

GSA 70, GSA 36, SEWP

Capstone Guidance (as outlined in NARA GRS 6.1)	Proofpoint Solution
Categorize and archive email records as permanent (senior officials) or temporary, based on the position or work of an email account owner.	<ul style="list-style-type: none"> • Support for multiple policies; apply retention, limit access, search within these groups • Can be based on Active Directory Groups for ease of management • Indefinite retention licensing
Agencies must ensure the email repository has appropriate security measures in place to prevent unauthorized access and/or destruction of records. Records must retain authenticity, reliability, and trustworthiness throughout capture, maintenance and transfer.	<ul style="list-style-type: none"> • Compliant (WORM) storage, immutable copy of data • Security is based on existing Active Directory Groups • Encryption of data in transfer and at rest • Retention and disposition schedules based on policy/role
Required metadata elements include the date of the email and the names and email addresses of all senders and recipients particularly if the system uses nicknames, distribution lists, or a blind copy feature.	<ul style="list-style-type: none"> • Email is captured through journaling to ensure completeness of capture • Active Directory sync allows for all senders and recipients (BCC, DL) to be captured
Cloud service providers must also act to ensure that records are accessible so as to ensure agency responsiveness to discovery, FOIA/Privacy Act, or other access requests.	<ul style="list-style-type: none"> • SLA-backed search response times • Self-service exports (PST, EDRM XML, CSV)
Agencies are expected to cull the email of Capstone officials (permanent accounts) to the greatest extent possible before transfer to NARA. Culling refers to the removal—or otherwise excluding from capture—of non-record, personal or transitory messages and attachments. Culling typically includes the removal of spam, email blasts received (such as agency-wide communications), and personal materials (such as emails to family members not related to agency business). Culling may be manual, automated or a hybrid of both. Agencies may develop their own policies and procedures for the culling of temporary accounts.	<ul style="list-style-type: none"> • Search can be limited to Capstone users • Info Tags (categorization) can be applied upon ingestion to identify newsletters, potentially personal or privileged email • Manually cull data further before transfer to NARA through the use of folders and categorization • Include/exclude data from export based on categorization
Agencies must transfer to NARA the emails of Capstone officials captured during their tenure as an official.	<ul style="list-style-type: none"> • Support for PST, CSV, Relativity Loadfile and XML via SFTP • Self-service export, multiple export
Systematic destruction of temporary email based on an approved NARA disposition authority, reducing the amount of email that has no further value being stored by agencies.	<ul style="list-style-type: none"> • Separate retention policy for permanent and temporary accounts • One touch disposition, apply exceptions through Legal Hold

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint.combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.