# Proofpoint Enterprise Archive for Federal Agencies

## Simplify Data Collection, Search and Retrieval with Modern Archiving Solutions

### PRODUCTS

- Proofpoint Enterprise Archive
- Proofpoint E-Discovery Analytics

### KEY BENEFITS

- Enforce retention policies automatically
- Manage data preservation efficiently and with full transparency
- Refine search strategies and instantly respond to FOIA requests
- Save time by automatically exporting content in PST, CSV, Relativity or EDRM XML formats
- Monitor, review and manage employee messages with intelligent supervision

Proofpoint Enterprise Archive is a FedRAMP authorized, cloud-based email archiving solution. It provides a central, searchable repository to help your federal agency:

- Simplify legal discovery
- Respond to FOIA requests
- Implement email records management according to NARA Capstone guidance

## Keep Up with Compliance and Discovery Features

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

### Easy-to-enforce retention policies

Enterprise Archive helps you create and maintain information retention policies. And more important, you can consistently enforce them, with automatic enforcement that's based on configurable rules. When data has reached the end of its retention period, you can quickly purge it. And every policy change and disposition action is tracked. This gives 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. And you can assign access to search exclusively within data that's assigned to a hold. What's more, our easy-to-use interface provides you with full reporting and an audit trail. With these unique features, you get more efficiency and transparency in managing data-preservation requirements.

### Fast access for early case insight

Enterprise Archive has high-performance search features that 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.

This 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

With Enterprise Archive, your legal team benefits too. They can 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 helps 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. You can select content for review—either as potential policy violations or through a random sampling process. And then it's automatically routed to the users who are authorized to act on it. Intelligent Supervision also provides you with 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. And 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. So you have always access to your data, regardless of how large your archive grows or how complex your searches get.

### The most secure archive in the industry

Available as an option, we can also ensure the data leaving your site is always encrypted, using our patented DoubleBlind Key Architecture. This gives you uncompromised data security. We make sure 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. You can also manage the encryption key for full control over who can access your data within the archive.

## Delivered as a Fully Managed Service

We provide you with more than just a breakthrough approach. We have unique operational and security practices that are SSAE-16 certified. Combined, they give you complete data privacy and uncompromised security. And our certification isn't 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. And in many cases before you're aware of the problem. Also, 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<br>(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. | • Support for multiple policies; apply retention, limit access, search within these groups<br>• Can be based on Active Directory groups for ease of management<br>• 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. | • Compliant (WORM) storage, immutable copy of data<br>• Security is based on existing Active Directory groups<br>• Encryption of data in transfer and at rest<br>• 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. | • Email is captured through journaling to ensure completeness of capture<br>• 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, or FOIA/Privacy Act, or other access requests. | • SLA-backed search response times<br>• Self-service exports (PST, 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. | • Search can be limited to Capstone users<br>• Info Tags (categorization) can be applied upon ingestion to identify newsletters or potentially personal or privileged email<br>• Manually cull data further before transfer to NARA through the use of folders and categorization<br>• 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. | • Support for PST, CSV, Relativity Loadfile, and XML via SFTP<br>• Self-service export and 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. | • Separate retention policy for permanent and temporary accounts<br>• One-touch disposition, apply exceptions through legal hold |

## LEARN MORE

For more information, visit **proofpoint.com**.

**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 for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.