e-share

SOLUTION BRIEF

E-SHARE EXTERNAL FILE SHARING AND SECURE EMAIL FOR OFFICE 365

EASY

Nothing to install – As with Office 365, there is nothing to install to rollout e-Share to end users. Integration with OneDrive, Exchange Online and Azure AD allows you to provision e-Share to all end users instantly.

RELIABLE

No Link Blocking – e-Share allows you to present a private collaboration service to your team, clients, vendors and partners, using your URL, logo, colors, terms of use, etc. Private branding strengthens your brand, instills confidence and trust on the part of those you are collaborating with, and eliminates link blocking.

SECURE

You Hold the Key – Unlike other cloud file storage services, e-Share's encryption system prevents e-Share and the underlying cloud file storage provider from accessing any and all data that is shared through the e-Share platform.

Microsoft Office remains the world's most popular and ubiquitous productivity application. Flexible Office 365 bundles and subscription options now provide organizations with even more attractive options for migrating to Microsoft's online services like OneDrive. But if these services are to be used to share highly regulated and proprietary data with outside parties, a new dimension of security and compliance requirements must be met.

Secure Email via Outlook – e-Share's Secure Mail Gateway works seamlessly with Exchange and Exchange Online so employees can use Outlook Web or Outlook Clients to send secure emails. Organization defined policies are triggered when emails meet the desired criteria. Emails are processed by e-Share's Secure Mail Gateway and are stored encrypted in the organization's OneDrive. Emails are secured by access control requirements, including online editing with Office Online, optional watermarking, automatic expiry, recipient file upload and more. With e-Share, a secure email can be the start of a bi-directional collaboration with a recipient, increasing user productivity.

Secure File Storage and Sharing via OneDrive – Encrypting files and maintaining detailed access audit logs are foundational security measures to meet regulatory requirements for the protection of PII (e.g. HIPAA and GDPR) and ITAR-controlled data. With e-Share, organizations could choose to encrypt data stored in OneDrive while also enhancing secure collaboration with internal and external audience. Any links to shared files/folders generated by e-Share are never blocked by the recipient's organization, as is frequently the case when links are generated by

OneDrive directly. Integration with Azure SAML – Organizations leveraging Microsoft Active Directory as a user identity repository, besides using ADFS for SAML authentication, can now enable access to e-Share through Azure Active Directory for all or designated employees thus making rollout of the e-Share solution to end users a quick implementation.

Universal Outlook Add-in – With e-Share's Universal Outlook Add-in, organizations have the option of presenting users in Outlook Web and Outlook Client interfaces with the organization's own list of policies to choose for secure emails. Installation of e-Share Outlook add-in is done on Exchange and can be deployed to all or selected users.