UNISYS

Ensure Data Privacy Compliance When Transferring Files

How to Transfer and Store Sensitive Files Securely With Unisys Secure File Vault Solution

Unisys Secure File Vault Solution

As organizations work to protect personal data against unauthorized processing, accidental loss, destruction or damage, there is potential for great risk if proper protocols for compliance and security are not in place.

What if you could enable secure file transfers easily into and out of the organization, with robust controls over who can access the data and what they can do with it, while every action related to the data within the file transfer solution is fully audited? With Unisys Secure File Vault, you can.

Unisys Secure File Vault is an online solution that uses only the standard HTTPS protocol for the web interface and file transfers, limiting potential attack vectors and avoiding the need for firewall changes. The solution is extremely easy to use and provides full auditing capability in line with data protection requirements.

Our solution offers the following features as standard, enabling the core solution to be rolled out quickly to achieve compliance and improve customer/user satisfaction:

- Cloud-hosted environment
- Fully managed service
- Fully auditable platform
- Data loss prevention
- Secure file transfer
- Automatic deletion of files on a scheduled basis
- Encryption of data at rest
- Robust access control measures, with all users having only access to the specific data they need and only for as long as they need to access it

The portal can be accessible securely over the internet, so users can access the vault whether they are working in the office, remotely or at a customer site. Alternatively, we can make the solution available over a private connection, such as a virtual private network (VPN).

For your organization's users, the portal can optionally be integrated with your existing identity provider (e.g., Azure Active Directory), so users can authenticate to the solution using their existing credentials with potential to enable single sign-on (SSO), allowing users to access the portal seamlessly if they have already logged in to the network.

All uploaded files will be automatically deleted according to the retention period set when the case status is changed to Closed within the Secure File Vault.

Audit logs from the solution can be made accessible to your organization by transferring them to a suitable location at a frequency to be agreed upon or, optionally, by direct integration to your security information and event management (SIEM).

If you have a need to localize your data in multiple places, for example, customers in different geographies who require their data to be stored and processed in a particular jurisdiction area, our solution can be configured with a specific location region for each case created in the system.

Secure File Vault Administration

Administrators of the solution, e.g., Service Desk users, have access to an Administration portal that allows them to create a case record in the Secure File Vault. They can input a unique case identifier, a short description and, optionally, an email address of a user to be associated with the case. If this option is selected, an email containing temporary credentials to log on to the Guest portal is sent to the Guest user when the case is created.

Administrator users are able to update cases if required and to change the short description and/or add a Guest user if one was not added at the time the case was created.

In addition, Administrator users can update the status of a case to Closed. At that point, a retention period will be set for that case after which the case and all files will be deleted from the system. There will be a default setting for the length of time for retention, but the Service Desk user will have the option of amending the retention period for that case.

Business Users

The solution provides an IN and OUT folder for each case. The IN stream is intended for receiving data into a case for analysis or processing, while the OUT stream is intended for sharing information with recipient organizations, often following the case analysis/processing. Business users can upload files to the IN and OUT folders for any case and also download files from the OUT folder for any case.

When Business users are connecting from a recognized (safe) network address, in addition to the above, they will be able to download files from any case's IN folder.

Guest Users

Guest users are typically people outside your organization that you want to receive files from or share files to on a time-limited basis. Similar to Business users, Guest users will have access to a login, password management and specific additional capabilities assigned to them.

Once logged in, a Guest user will have access only to the IN folder and OUT folder for the case they are associated with. They will be able to upload files to the IN folder, and if Business users put files in the OUT folder for that case, the Guest user will be able to download them. Guest users will not be able to delete any files, nor can they modify or overwrite an existing file, as multiple files with the same name can be stored in the same logical folder. When viewing files, users will see the file name, date and time it was uploaded, along with the name of the user who uploaded it, in order to distinguish between files.

Delete Role

Preventing accidental erasure or deliberate destruction of data is a key element in the Secure File Vault solution, but specific users can have the capability to delete files. The delete actions will be recorded for audit purposes, but the data will not be retrievable once deleted. This role will provide flexibility for your organization to manage instances where files have been incorrectly uploaded, but if it is preferred that no user should be able to delete any files, then the role can remain unassigned.

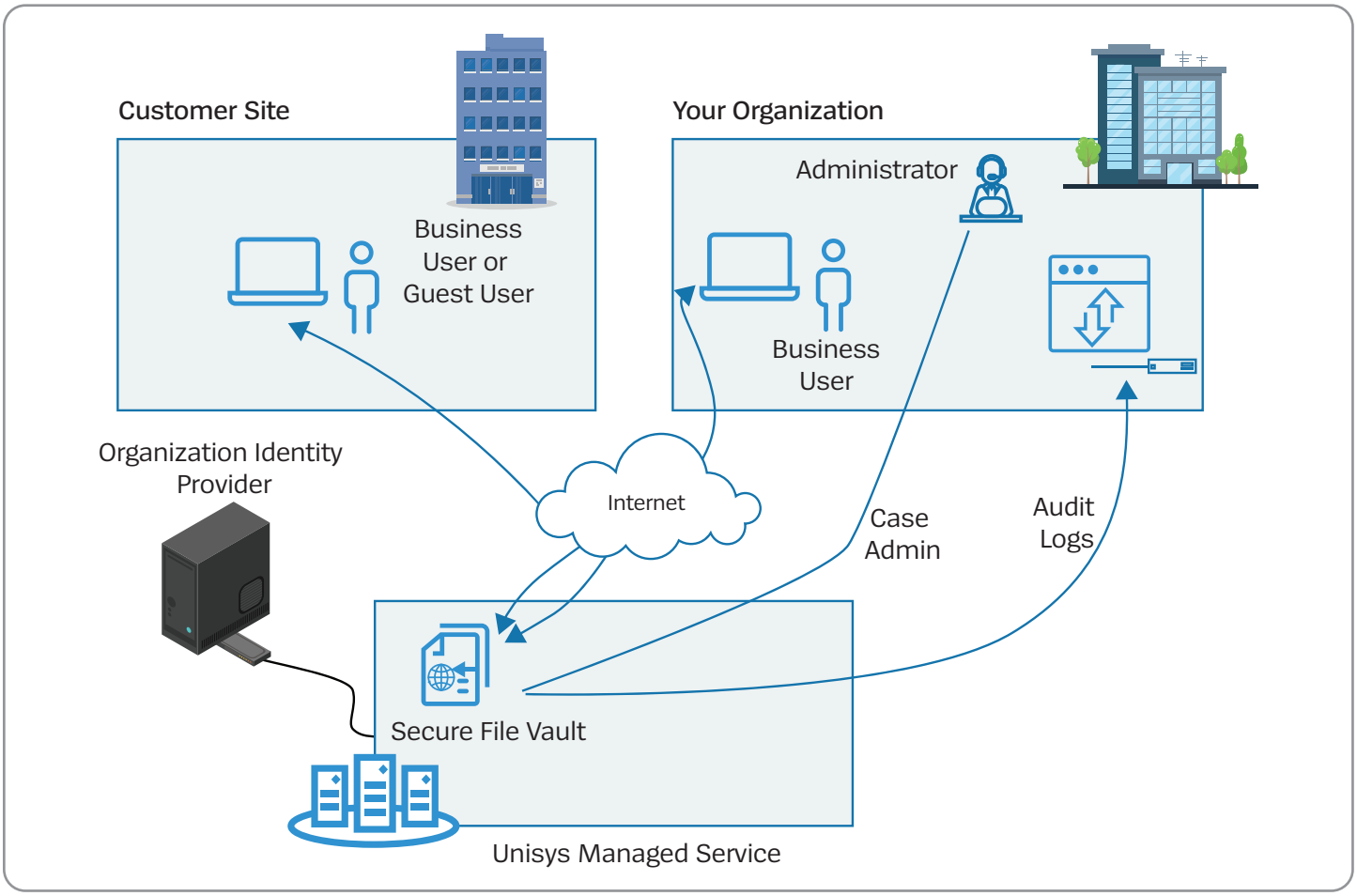

Figure - Sample Core Configuration

Why Choose Unisys?

This solution is all about providing you something that is not only simple and easy to use, but is also designed and built specifically to handle sensitive data and integrate into your business processes.

It is software as a service, plus more – we can tailor the solution to suit your business needs, including single sign-on (e.g., active directory integration) and synchronization with your security operations center and case management system for automated risk and data management. Such flexibility is not available in commodity solutions. Unisys brings decades of experience in delivering mission-critical, highly secure solutions to some of the most demanding governments and businesses in the world.

Learn More: Visit us online to explore how Unisys can help with your secure file transfer requirements.

unisys.com

© 2022 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.

09/22 22-0339