WHITE PAPER

Acronis®

activEcho™

Driving Secure Enterprise File Sharing and Syncing

activEcho™ Overview

In today's enterprise workplace, employees are increasingly demanding mobile and collaborative solutions in order to get their jobs done. Enterprise employees need to be able to access their individual files independent of the device – desktop, laptop, tablet or smartphone. In addition, individuals want to be able to easily share and collaborate on files with their colleagues or business partners. Enterprises are also recognizing the significant advantages these tools can deliver – greater information access, increased teamwork, more engaged employees, etc. These advantages can lead to significant benefits to the business - better customer service, improved products, faster production cycles, increased revenue/profitability, etc.

However, the current solutions in the marketplace, many of them consumer-based services, expose the enterprise to significant and unacceptable risks – data leakage, non-compliance of regulations, security risks, loss of data, etc.

activEcho™ is the industry's only Enterprise File Sharing solution that balances the need for simplicity for the end user, and the security, management and flexibility required by the enterprise. The enterprise, and more specifically IT, requires the ability to manage and control file sharing activities to protect the critical information and data assets of the organization. IT also needs the freedom to choose the most appropriate deployment model for their use case – on-premise inside the firewall, in the DMZ, or in a private cloud. This deployment flexibility, plus activEcho's high level of security and control, make it a great fit for security and compliance-sensitive organizations, including regulated industries.

activEcho and Security

The activEcho enterprise file sharing and syncing solution provides easy to use functionality and managed security capabilities. It was designed with consumer-grade simplicity and enterprise-grade security, management and flexibility. activEcho addresses a variety of security, compliance and governance needs in both the activEcho server and the client. With activEcho, the enterprise gains control over all critical aspects, including management via AD groups, freedom of deployment options, enterprise controlled encryption and whitelisting/blacklisting of approved internal and external users and domains.

activEcho Server

activEcho starts with infrastructure flexibility. It has several deployment options for the enterprise. IT can decide where the activEcho server software is installed and where activEcho files are stored - on premise in the data center, in the DMZ, or in a private cloud (ex. Amazon EC2 and S3). activEcho gives IT and the enterprise the freedom to choose the infrastructure model that is most appropriate for their organization.

After the initial deployment, IT sets policies that govern the activEcho server as it performs the following functions:

- Authentication
- Encryption
- Service provisioning to users
- Storage
- Management
- Syncing

Authentication

activEcho allows for internal users and external users. For internal users, access to activEcho requires authentication with Active Directory (AD) credentials. The user enters their AD credentials into the activEcho client agent or web browser interface per policies set by IT. Once the user is validated, activEcho then checks the management polices specified in the activEcho management console for that AD user or the groups of which they are members. These policies are explained in the Management section below.

For external users, access to activEcho requires authentication with accounts that are automatically provisioned when the user accepts an activEcho invitation to share. Such invitations are only sent to email addresses allowed by policies set by IT with the whitelist and blacklist functions. The bottom line is that IT, or its designate, determines what external users are allowed access. The credentials for the external users are stored encrypted in the activEcho database.

Management Based on Active Directory Users and Groups

Enterprise IT sets policies in activEcho that govern users and groups maintained in Active Directory. It has a number of policy controls, including:

- Access based on Active Directory group membership
- Whitelist of invitees by domain or email address
- Blacklist of invitees by domain or email address

For example, IT might create an activEcho policy for members of the "Accounting" AD group or for an individual such as Ben.Franklin@F500Ent.com. This policy governs the functions available to members of the Accounting group regarding who they can invite inside and outside the company.

Enterprise IT also sets policies that can control the special environments for users accessing activEcho from their mobile devices such as iPhone and iPad.

Encryption

All data in activEcho, at rest and in transit, is encrypted. The administrator defines the encryption cipher depth and owns the encryption keys. Data at rest in the activEcho repository is encrypted with a cipher such as AES-256 specified by IT. Each file has its own unique encryption key which is stored in the database. Those encryption keys are encrypted themselves with a master key for the entire solution. When using S3 to deploy the repository, all communications between clients and the repository use HTTPS and X.509 certificates.

Infrastructure Model and Storage

The activEcho server stores files in its own secure repository. IT selects the repository location that is appropriate for the expected uses, storage availability and security requirements. activEcho gives the enterprise the freedom to choose the most appropriate infrastructure option for their organization.

The options include:

- Local Storage on the Server
- Network Storage accessible by UNC path over SMB or CIFS
- Amazon S3 storage accessed via REST over HTTPS.

For many security- and compliance-sensitive organizations including regulated industries, the ability to run activEcho on-premise is a significant benefit as it allows the enterprise to maintain maximum control and security.

Syncing

The activEcho server is the hub for the synchronization of shared files to clients. The activEcho server tracks all versions of shared files so that it can respond to client requests for any changes that need to be synced down to clients. All communication between the server and clients, including the actual transfer of files, is SSL encrypted.

Clients

activEcho provides users with automatic background synchronization by using agents that communicate with the server to synchronize changes as they occur. There are native client agents for Windows®, Macintosh®, iOS® (iPhone® and iPad®), as well as access via all mainstream web browsers. The Windows and Macintosh clients are software agents with a very small footprint on memory and CPU.

Enterprise IT manages these Windows and Macintosh clients as follows:

- An activEcho software agent is installed on each user's Mac or PC.
- An individual's activEcho shared and synced files are stored in the Mac® or PC file system, so standard OS security practices apply - user login, file system encryption and local file permissions.
- activEcho configuration and passwords are stored in an encrypted data store, i.e., the Keychain on Mac OS X®, or within the registry on Windows.

On mobile devices, Acronis's secure and managed mobilEcho™ app can be used to access activEcho shared files. This capability is included in the activEcho server license. The app can be downloaded from the App Store for free. Mobile users are also managed through Active Directory. Files and other configuration elements are encrypted in the mobilEcho app's secure "sandbox" for complete secure mobile access to activEcho. IT can control provisioning the app and perform a "remote wipe" of the app on mobile devices as needed.

Web Access

Users can also gain access to activEcho using any supported mainstream web browser. activEcho's web interface provides access to shared files and folders and other functionality, like viewing the transaction log, inviting other users (if permitted by IT's defined whitelist/blacklist policies), and defining email notification preferences. activEcho uses a bundled version of Apache Tomcat server to provide these web services.

Enterprise IT manages web access through the settings in the activEcho server. activEcho web access provides security by:

- Requiring AD credentials for access.
- Encrypting all data in motion with HTTPS with a cipher such as AES-256 and a X.509 encryption certificates.

Backup and Disaster Recovery

activEcho can be backed up as a part of normal operations to provide reliable data protection of the server data. Since all of the data stored by activEcho is encrypted all the time, the security of the backup copies of the data is preserved.

IT uses standard backup tools to:

- Backup the repository which is a structure of encrypted folder names, file names and files with encrypted content.
- Backup the encrypted SQL database.
- Store a copy of the encryption keys with the backups so that the restore process can access the encrypted files.

Summary

Increasingly, a vast number of business activities revolve around the collaboration and sharing of information, data and files, and the way employees and the enterprise want to share and collaborate is evolving to a newer, much more effective paradigm: Enterprise File Sharing. Acronis's activEcho is the industry's only Enterprise File Sharing solution that balances the need for simplicity for the end user, and the security, management and flexibility required by the enterprise. The enterprise, and more specifically, IT, requires the ability to manage and control file sharing activities to protect the critical information, data and file assets of the organization. With activEcho the enterprise can address all the critical needs of all key constituents - users, the business, IT, security, and compliance groups.

For additional information please visit http://www.acronis.com

To purchase Acronis products, visit www.acronis.com or search online for an authorized reseller.

Acronis office details can be found at http://www.acronis.com/company/worldwide.html