SOOKASA WHITEPAPER | **SECURITY**

www.sookasa.com

About Sookasa

The use of the cloud and SaaS security solutions among businesses has seen rapid growth over the past several years—and it's only going to continue to rise. By 2020, 78 percent of SMBs are expected to have fully adopted the cloud, more than doubling the current usage in just five years. What's more, 90 percent of companies are already using the cloud in at least some way. The cloud's benefits are substantial, and include the ability to employ file sync-and-share solutions with ease, allowing employees to share and store files instantly and access them from anywhere and on any device. This boosts productivity and makes collaboration seamless.

However, the widespread use of the cloud brings with it its own set of risks, and while the cloud's benefits are a boon to companies' workflows, its dangers can be devastating. As SaaS solutions become a given both at work and at home, employees begin to use their personal devices for work purposes, syncing sensitive files to their smartphones to access them at meetings or to work on the go. At the same time, employers become more lax about sanctioning work-approved solutions and enforcing security policies. But with so much sensitive corporate and client data proliferating on the cloud, managing it—and protecting it—is a must for management, not least in order to know how their company files are being stored, shared, and accessed.

But perhaps the biggest threat comes from the mobile devices themselves. Most of today's popular sync-and-share solutions provide adequate protection when files are at rest on their servers. But once a file is synced to a smartphone or a tablet, the default encryption disappears, and files that were once encrypted become vulnerable and easily accessible by anyone—including malicious actors.

In fact, most data breaches can be attributed to specifically this oversight in default security measures. 40 percent of enterprise employees and 80 percent of healthcare employees say they use personal mobile devices for work. However, 70 million smartphones are stolen annually in the U.S., and one laptop is stolen every 53 seconds. The numbers paint a bleak picture, indicating that unmanaged data is rampant and readily available for anyone to access. And they do—consistently and across industries, with the healthcare sector hit hardest. 68 percent of healthcare data breaches—and HIPAA violations—are due to lost or stolen devices.

Founded in 2012 by a team of leading security experts, Sookasa provides a solution to these problems by providing a full suite of detection, protection, and enforcement measures. As a fully integrated CASB platform, Sookasa's range of products apply DLP technology to maximize visibility; help administrators audit the way their teams use and access files; provide two-factor authentication to bolster security; revoke access to files and devices instantly when necessary; and provide end-to-end encryption on mobile devices. In this whitepaper, we'll unpack one of the pillars of Sookasa's holistic security strategy: transparent encryption. The company's patented file-level encryption differentiates Sookasa from other solutions on the market by allowing enterprises to protect data on Dropbox and Google Drive without disrupting how their end users work. It's unreasonable to think that we should rely only on default protections when data breaches have reached an all-time high.

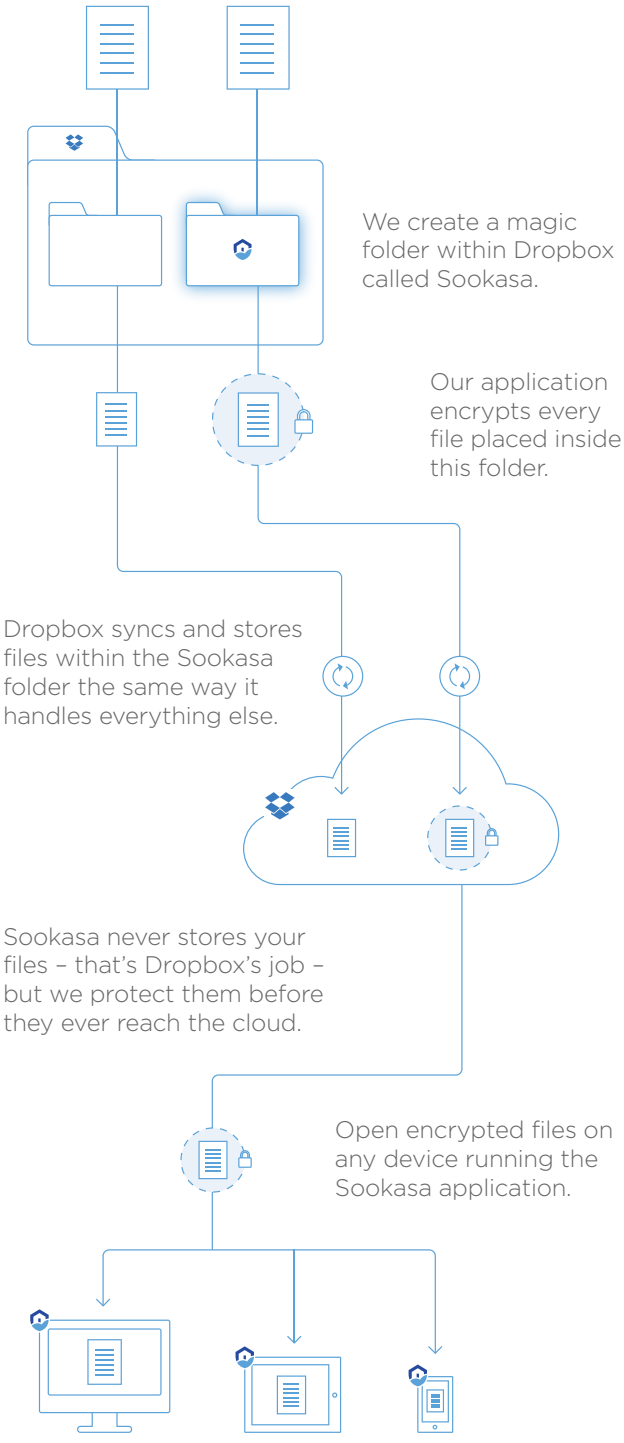
And with Sookasa, you don't have to.

Overview

The company's patented file-level encryption enables enterprises to protect data on Dropbox and Google Drive without disrupting how end users work.

Here's how.

How It Works



Key Features

Robust security. Sookasa employs file-level encryption on devices and the cloud with AES 256-bit encryption and uses SSL for transmission.

Automatic encryption on devices. Any file placed in Sookasa is automatically intercepted and encrypted. Because Dropbox and Google Drive sync only encrypted versions of files, data stays protected everywhere.

Easy access control. Sookasa enables administrators to have real-time control over company files both inside and outside the organization.

Data and key separation. Sookasa's encryption scheme decouples the data, which is stored by Dropbox and Drive, from the encryption keys required to access it. Sookasa manages encryption key distribution, access control, and audit trail collection.

Native Dropbox experience. Sookasa is the only fully transparent file-level encryption solution for Dropbox and Drive, enabling end-users to interact normally with the cloud service.

Full audit visibility. Sookasa logs every modification, copy, access, and share operation made to encrypted files and associates each with a user.

Security overview

With its patented encryption and key distribution mechanism, Sookasa brings unprecedented security to Dropbox and Google Drive.

Features that facilitate Sookasa's security include:

- **Data and key separation**. Sookasa does not store files. It simply manages the encryption key distribution, access control, and audit trail collection.
    - **Robust encryption**: Sookasa employs file-level encryption to protect data on the cloud and devices with AES 256-bit encryption.
    - **Secure data transmission**: Sookasa uses SSL to communicate between the device applications and Sookasa's cloud service.
- **Access control**. By encrypting files and granting access based on authenticated credentials, Sookasa ensures that only authorized parties can access information.
    - **Unique user identification**: Sookasa assigns unique credentials to users to identify and track user identities.
    - **Automatic logoff**: Sookasa terminates a session after a pre-set period of inactivity, which administrators can customize.
    - **Encryption and decryption**: Sookasa allows information to be encrypted and decrypted via its PC, Mac, iOS, and Android clients.
    - **Simplified off-boarding**. To prevent access to files, administrators can revoke the keys for a device or user at any time with the click of a button, even when a device is offline.
    - **Real-time permission modifications**. Sookasa enables administrators to control access to company files both inside and outside the organization with real-time permission modifications.
    - **Emergency access**. From Sookasa's web-based Dashboard, files can be downloaded and decrypted in urgent matters.
    - **Offline access**. Sookasa securely caches keys for a set period of time to enable offline access to encrypted data. Once a key expires, device must move online to access files.
- **Audit Controls**. Sookasa logs every modification, copy, access, or share operation made to encrypted files and associates each with a user. With a simple reporting tool, Sookasa provides complete audit trails on all operations associated with encrypted files, even after they've been downloaded to devices or shared externally.
    - **Integrity controls**. Dropbox and Drive store a complete version history of each file, allowing enterprises to track and recover changes. Sookasa validates the integrity of each version by using a hash-based message authentication code (HMAC), rendering it impossible to modify files without access to the private encryption keys.
    - **Transmission security**. Sookasa encrypts the files before they are transmitted via secure HTTP (HTTPS) to Dropbox and Drive, thereby protecting the files in transit and at rest. The encryption scheme employs an HMAC to ensure that the data cannot be modified or destroyed without detection.

Encryption Technical Overview

Sookasa controls access to files by granting authorized users and devices access to keys for specific files. Files remain encrypted and are tracked by Sookasa even if they are moved outside the cloud storage provider application (e.g., if they are sent by email).

Sookasa automatically creates a folder called “Sookasa” on each user’s Dropbox or Google Drive account. The secure Sookasa folder is a safe haven for any sensitive content, and separates the data, which is stored on Dropbox or Drive, from the keys required to encrypt them. Any file that is placed within the Sookasa folder is automatically encrypted, thereby providing the administrator full control over user access to the file, whether that user is within or outside the organization.

Some key elements of our encryption mechanism include:

- **Automatic encryption on devices**. Any file placed in the Sookasa folder is automatically intercepted and encrypted by the Sookasa client applications, available for Mac OS X and Microsoft Windows. Sookasa continuously monitors the Sookasa folder and ensures that data is encrypted before it is synced by the cloud storage provider. Because the cloud storage provider syncs only encrypted versions of files, data remains protected everywhere—whether it is synced to another device, or even if it is later removed from the Sookasa folder. Sookasa is the only solution that provides a synced encrypted drive.

- **Automatic encryption on the cloud**. Our service encrypts files that are uploaded by users via Dropbox and Drive’s web interface as well as those uploaded on devices that do not have the Sookasa client installed.

- **Bank-level encryption scheme**. Sookasa uses Advanced Encryption Standard (AES) with 256-bit encryption, the highest commercially available standard, which is also used to secure financial institutions and bank accounts.

- **Seamless integration with cloud storage providers**. As a Premier Partner in Dropbox’s Partner Network, Sookasa is seamlessly integrated with Dropbox, and our Google Drive integration is similarly transparent. Sookasa is designed to leverage and preserve your chosen cloud service’s user interface and capabilities. Files are encrypted by Sookasa, but syncing and sharing is performed and managed by the native enterprise file sync-and-share software.

Technical Overview: Key Management

The combination of a cloud storage provider and Sookasa decouples the encrypted data from the keys required to decrypt it. Neither the cloud storage provider nor Sookasa has access to the user's raw data.

Sookasa does not store any files, which all reside on the cloud storage provider's cloud and device storage service. Sookasa simply manages the encryption keys, which are not available to the storage provider. Only a user who has access to and permission for both systems can successfully view or modify the data.

Sookasa manages access to files by distributing encryption keys with a centralized, web-based server.

Here's how it works:

- **A user attempts to access a file**. When a user tries to open a file from a computer or mobile device, the Sookasa client requests the encryption key associated with that file.
    - Along with the request, the client sends the server the signed unique fingerprint of the file, the user's credentials, and a unique identifier for the device.

- **The Sookasa server authenticates the request**. It validates the signatures, verifies that the user and device are authorized to access the file, and logs the request.

- **Encryption keys are provided as appropriate**. If the user has the proper permissions, the Sookasa server will provide the file key and the file will open automatically. If user isn't authorized to open the file, he or she will not be able to view or modify it.