SOOKASA WHITEPAPER | **CASB OVERVIEW**

www.sookasa.com

Sookasa Overview

Nearly 90 percent of enterprises currently use the public cloud, and by 2020, practically every business across the country is expected to have fully integrated the cloud into everyday operations. As both scientific and anecdotal evidence has shown, companies using the cloud experience higher productivity, a smoother workflow, and satisfied customers, who are able to communicate more effectively with their business representatives.

However, the rise in cloud usage has also led to a puzzling problem: a decrease in visibility. Creating, storing, sharing, and syncing files has become incredibly simple, and as such, data seems to proliferate endlessly on the cloud. As a result, business leaders soon began losing track of how many files they had on the cloud, which ones contained sensitive information, and which team members had access to them. All of a sudden, it was hard to know how many copies of a financial report existed and whether anyone had synced the file to a personal smartphone, for instance. The lack of visibility really becomes an issue when company files are synced to mobile devices, where file sync-and-share providers don't offer the same encryption protections by default as they do when the files are at rest. That leaves files exposed and vulnerable, contributing to record-high numbers of data breaches.

The expected increase in cloud usage is only exacerbating this problem—and no organizations are immune. In 2015, the United States Office of Personnel Management suffered an immense data breach, exposing the personal information of 22 million people, that was due simply to an inability to control data. The OPM admitted that an incomplete inventory and a lack of awareness of where their data was being stored contributed to the breach.

Keeping files organized and maintaining visibility is a major obstacle to secure cloud usage that's rapidly becoming a universal problem. The first step to mitigating it is being able to identify and classify all files that contain sensitive data. Then, creating a protocol for how those files can be shared and with whom is a key element to maintaining security.

As a fully-integrated cloud access security broker (CASB), Sookasa offers a holistic suite of security solutions that help detect sensitive information using Sookasa's patented File Scan product; protect information using measures like file-level encryption and two-factor authentication; and enforce security measures by enabling access revocation and audits. All of Sookasa's products integrate seamlessly with popular cloud providers like Dropbox, Google Drive, and Microsoft Office 365. Features are also integrated with platforms like Zendesk, Salesforce, and Box to provide robust security for all enterprise needs.

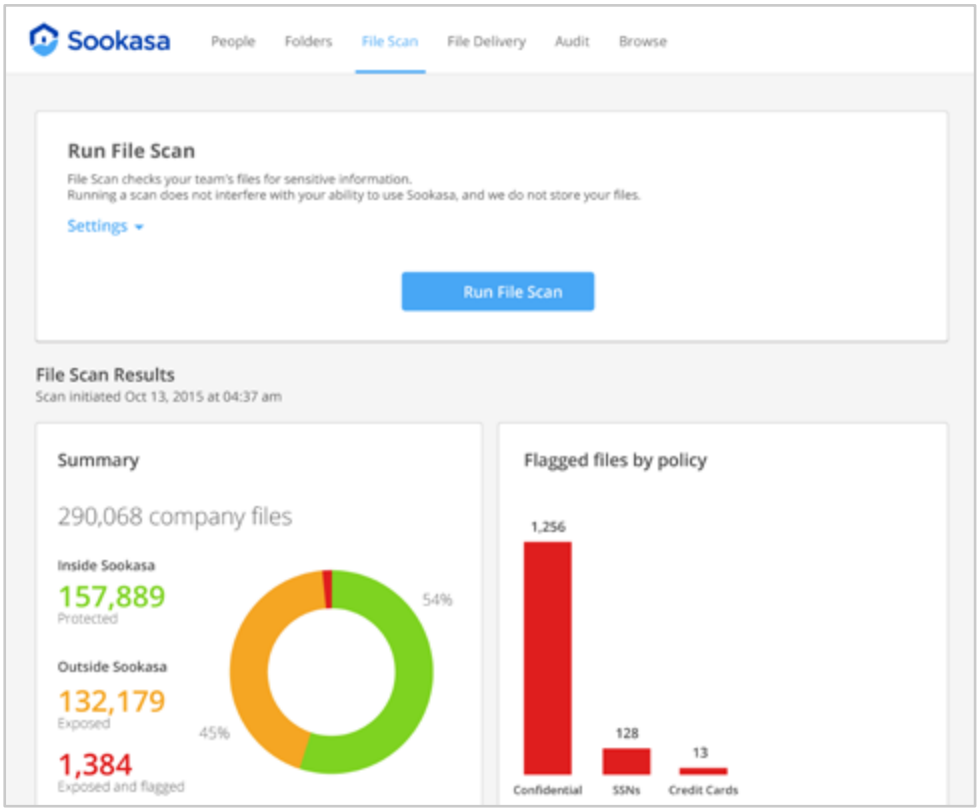
For information on Sookasa's file-level encryption solution and an explanation of how it works by leveraging cloud providers' APIs and employing bank-level encryption technologies, please read our Security whitepaper. The whitepaper you're currently reading will omit encryption but discuss the three remaining tenets of Sookasa's security solution: the File Scan data loss prevention product, access control, and auditing.

Detect risks with File Scan DLP

Sookasa's File Scan product provides a seamless approach to data loss prevention that easily finds and classifies an organization's important and sensitive data. File Scan works with Dropbox for Business and Google Drive, leveraging the cloud providers' APIs to make security cleaner and easier for a company already storing and sharing their files in the cloud.

An administrator can use the product to scan all files across team accounts for conventionally sensitive information like credit card numbers, Social Security numbers, and addresses. The software can also be customized with company-specific keywords that will help administrators flag files that contain intellectual property, client account numbers, or information pertaining to a confidential project.

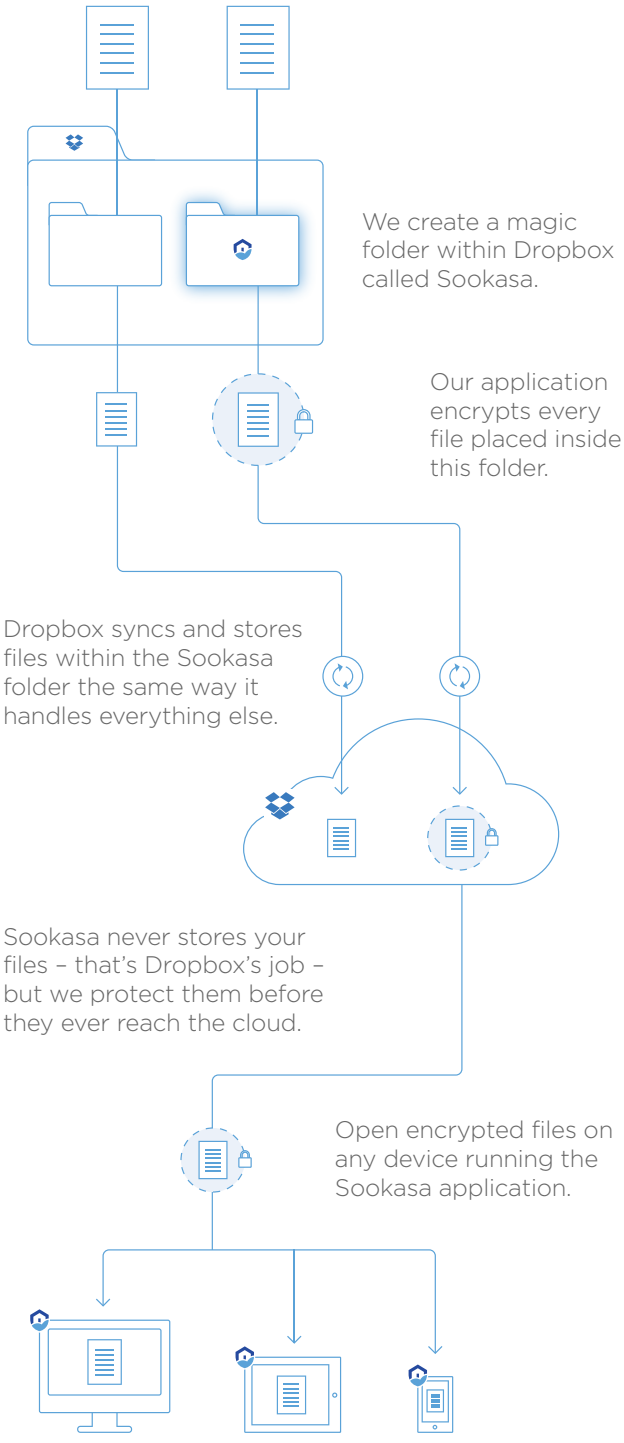
Once files have been tagged as containing certain keywords, they can easily be classified, which then lets all employees know how to proceed. For instance, anything that contains customer data might get labeled as "top secret," anything that contains business data as "secret," and anything that can be released publicly doesn't get labeled at all. Employees would then know that anything labeled "top secret" cannot be shared externally and cannot be downloaded without encryption. Having a DLP product do the hard work of identifying and classifying files relieves employees of this responsibility—and ensures that nothing slips through the cracks.



Protect with file-level encryption, access control, and blocking

Being able to identify sensitive information is half the battle, where the other half relies on administrators being able to react quickly in sensitive situations. With the rise of mobile devices and BYOD, we already know that files are being synced to the cloud in both sanctioned and unsanctioned ways quickly and easily. Sookasa's two-factor authentication allows files to stay even more secure by authenticating the user.

How It Works



As mentioned previously, File Scan lets administrators find the files that need protecting, and Sookasa's file-level encryption solution lets administrators and employees protect those files with the touch of a button. But even if an employee was granted access to a "top secret" file or project folder, does that mean she should have access to it forever?

There are a few situations in which the answer is a resounding "no." The employee might simply be taken off a project, in which case she no longer needs access to the files. She might leave the company—willingly or unwillingly—and still have files synced to her smartphone. Or as happens all too often, she might have her laptop or smartphone stolen or lost and the company's sensitive files might find their way into the wrong hands.

In any of these cases, Sookasa lets administrators block access to individual files, users, or devices with the touch of a button on the Dashboard. If an employee is taken off a project, the admin can revoke access to project files whether they're stored on the employee's work computer, synced to her Dropbox folder, or shared to her tablet. SImilarly, access to all files can be instantly revoked the minute an employee leaves the company, regardless what devices she'd used to access files in the past. And in the case of loss or theft, the moment she notices her phone is missing, her supervisor can block access to the phone instantly. Controlling access to files and devices allows Sookasa users to regain control of their files and let clients rest easy, knowing that their information is always in good hands.

Enforce policies

It isn't enough to have security policies in place—you need tools to verify that your team adheres to them and methods to actually enforce them.

Sookasa's Audit product identifies sharing patterns and activity across Dropbox, Google Drive, Box, OneDrive, Slack, Salesforce, and Zendesk. Audit is the final piece in the puzzle to ensure that your data stays secure even when it's being shared and synced across a number of platforms. It's no longer a guessing game. Rather, administrators and managers can monitor activity in real time to see who is accessing files and when, detect sharing patterns, and identify any anomalies. Unusual user activity can be spotted quickly, and unauthorized access to a file can be thwarted before any data is breached.

With Sookasa's Audit product, you can quickly check that your team is using and sharing data on SaaS solutions securely. Advanced enforcement options also let you enforce two-factor authentication, set automatic session timeouts, and instantly revoke encryption keys to block users or devices.

With data breaches higher than ever and their dangers only multiplying, taking control of your company's data and monitoring file activity is critical.