

A man with brown hair and a beard, wearing a blue button-down shirt and blue jeans, is sitting on a wooden bench outdoors. He is looking down at a silver laptop on his lap and typing on the keyboard. The background is a blurred outdoor setting with stone steps and a railing.

Only the Best Will Do: Taking Advantage of Best-of-Breed Security

The technological evolution of the tools used to get work done has resulted in an interesting modern-day dichotomy. On the one hand, workers are less confined to a central location and more often able to work from remote locations that are separated from coworkers, in some cases by thousands of miles.

Organizations both large and small now share files via the cloud during their daily routines. Sharing information between workers, partners, contractors and end users is easier than it has ever been.

On the other hand, cloud technology has also exposed companies to some significant issues. Workers might upload or download malware or accidentally share malicious files with coworkers, or worse, clients! They might accidentally or purposely share confidential information outside of the organization.

Citrix ShareFile provides a secure, fast and convenient means to enable the sharing of documents. Every SaaS application, including ShareFile, must also protect customer data against any number of security threats including malware and data leakage. Citrix offers a range of powerful built-in defenses and partners with third-party solutions to provide complete security.

This paper describes a single-platform solution that can be used to effortlessly maximize the security capabilities of ShareFile and any other SaaS applications that an organization might deploy. It details features companies should look for when seeking to enhance the security built into Citrix ShareFile.





Business Challenge Summary

The advent of cloud computing has bestowed a wealth of economic benefits, enhancing productivity and slashing costs. In 2016, CIO reported that more than 90 percent of all companies use some form of cloud-based technology.¹

Enterprise file sync and sharing (EFSS) solutions have become some of the most common and most beneficial cloud-based applications. EFSS connects workers, partners and others to data in the cloud and puts it at their fingertips, wherever they happen to be.

Citrix ShareFile, a leading EFSS solution, provides industry-leading security, auditing capabilities, and compliance controls for safe content sharing, allowing organizations to safeguard data, documents, content, users, and devices with one solution. IT can control, authenticate, track, and report on

who accesses, views, shares, edits, deletes, downloads and uploads files based on user location, role, and device criteria. Lost, stolen or otherwise potentially compromised mobile devices can be locked or wiped remotely, ensuring that proprietary data is not leaked beyond critical borders. This is why Citrix has been named a leader in the Gartner Enterprise File Synchronization and Sharing Magic Quadrant Report.

Even so, there are some significant concerns facing companies using EFSS and other cloud-based services. In 2016, the Cloud Security Alliance published *The Treacherous 12*, a research report that detailed the top threats facing companies that utilize the cloud.² Coming in at #1 on the list of cloud-based concerns — data security threats.

Certainly, though, the concern about data security in the cloud is not news for most companies that use it. The potential risks to proprietary and sensitive corporate data are well known and many organizations are acting to mitigate that risk.

Unfortunately, few companies offer security for data in a SaaS environment. Those that do typically offer it only for a few popular SaaS solutions like Office 365 or Google and not for all the platforms a company would use.

Moreover, most cloud security companies only offer one feature or specialize in one. For example, a solution may be strong in DLP but weak in antivirus. This makes it difficult to create a full security stack.



¹ <http://www.cio.com/article/3018156/cloud-computing/cloud-adoption-soars-but-integration-challenges-remain.html>

² https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf



What if companies were not forced to choose between features? What if the very best features of the very best information security solutions could be incorporated into a single platform? Companies would no longer be forced to leave behind solutions that offered needed and desired features. Instead, they could pick and choose the best, most relevant, most desired features of the most advanced security solutions on the market: the best from this solution, the best from that solution.

Citrix ShareFile customers that need advanced security have a number of options to choose from. When selecting the most appropriate solution, however, they should seek out the technology that meets these requirements:

- Seamless integration with Citrix ShareFile
- Seamless integration with other SaaS applications in use by the company
- Best-of-breed technology
- Unlimited scalability
- Client device/connection type independence
- Easy deployment and easy management





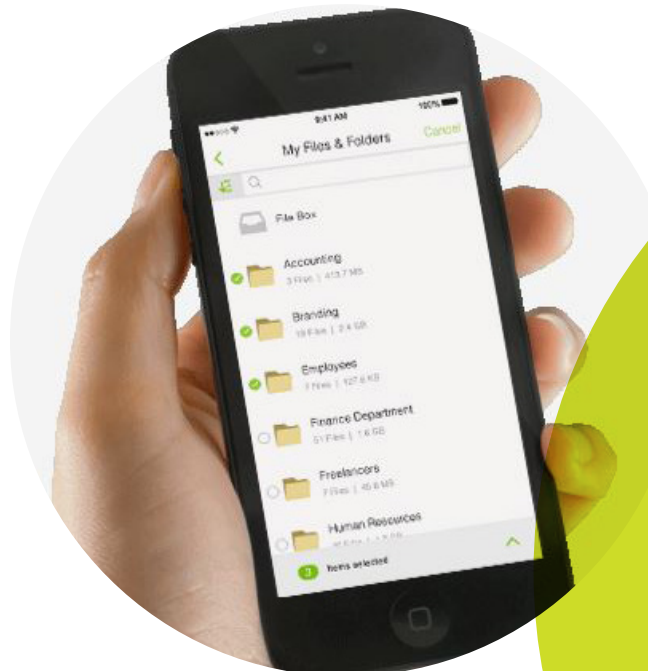
Citrix Ready Security Program for ShareFile

Citrix ShareFile offers tools that make it possible for employees and outside collaborators to share files. ShareFile is used for secure file-sharing and file storage by thousands of companies worldwide, including 99 percent of the Fortune 500.

On its own, ShareFile incorporates dozens of security features that work to keep files and data safe, including:

- **File transfer:** Employs SSL/TLS protocols to protect client authentication, authorization and file transfers.
- **High-grade encryption:** Secures files in transit with no less than 128-bit encryption using industry-standard encryption protocols.
- **File integrity:** A keyed hashed message authentication code is used to authenticate and ensure the integrity of intra-system communications (ShareFile verifies file size and file hash to ensure integrity).
- **Link generation:** SSAE 16 Type II accredited or ISO 27001 certified datacenters host the SaaS application and metadata.
- **Encryption:** ShareFile stores client files at rest using AES 256-bit encryption, a Federal Information Processing (FIPS) encryption algorithm.
- **Firewalls:** Files are processed using systems protected by securely configured firewalls that effectively limit and control access to network segments.
- **Redundant storage:** Files are stored in replicate with leading infrastructure as a service (IaaS) providers that ensure high file durability and availability.
- **Backup:** Files are backed up according to configurable file-retention and versioning settings.
- **Custom SMTP (mail) settings:** ShareFile enables clients to route email messages through their own mail servers. When enabled, all emails sent through ShareFile will be routed through the client's mail server, instead of through ShareFile mail servers. Clients may optionally configure the connection to support SSL.
- **Multi-factor authentication:** Clients may set up a multi-factor authentication process that requires submission of the account password and a secondary authentication.
- **File retention:** Users can choose to automatically delete files a selected number of days after upload in support of retention preferences and policies.
- **Remote wipe:** Users can remotely lock and wipe ShareFile data from a lost or stolen device.
- **View-only permission:** May be used to ensure that files cannot be downloaded, printed or saved. Access to documents is available only in ShareFile's web-based viewer.

The above list represents just some of the security features built-in to ShareFile (the complete list [may be viewed here](#)). Citrix ShareFile obviously takes security very seriously, and makes every effort to assure that customers' data is kept safe.



³ <https://www.sharefile.com/resources/citrix-sharefile-security-and-compliance>



Security features offered by Citrix ShareFile focus upon four key areas of concern for practitioners of corporate file sharing:

1. Reporting, auditing and control

- Enterprise-ready service
- End users and IT reporting
- Access control policies
- Storage quotas

2. Device security policies

- Remote wipe
- Poison pill
- Restrict modified devices
- Restrict third-party apps
- Passcode lock

3. Data security

- Secure file sync and share
- Storage and in-transit encryption
- Mobile device encryption
- Compliance
- Data loss prevention systems integration
- Read-only/view-only sharing
- Multi-tenancy
- Information rights management

4. Open and extensible platform

- API
- SDK connectors

To augment ShareFile's built-in security, the Citrix Ready Security Program for ShareFile was launched to highlight partners that go beyond even these high standards in promoting ShareFile security.

Partners that have been selected to participate in the Security Program for ShareFile have demonstrated the ability to add layers of security, privacy and compliance.



1. Cloud security



2. Data security



3. Identity and access management



4. Security analytics

More information on the Citrix Ready Security Program for ShareFile is available [here](https://citrixready.citrix.com).



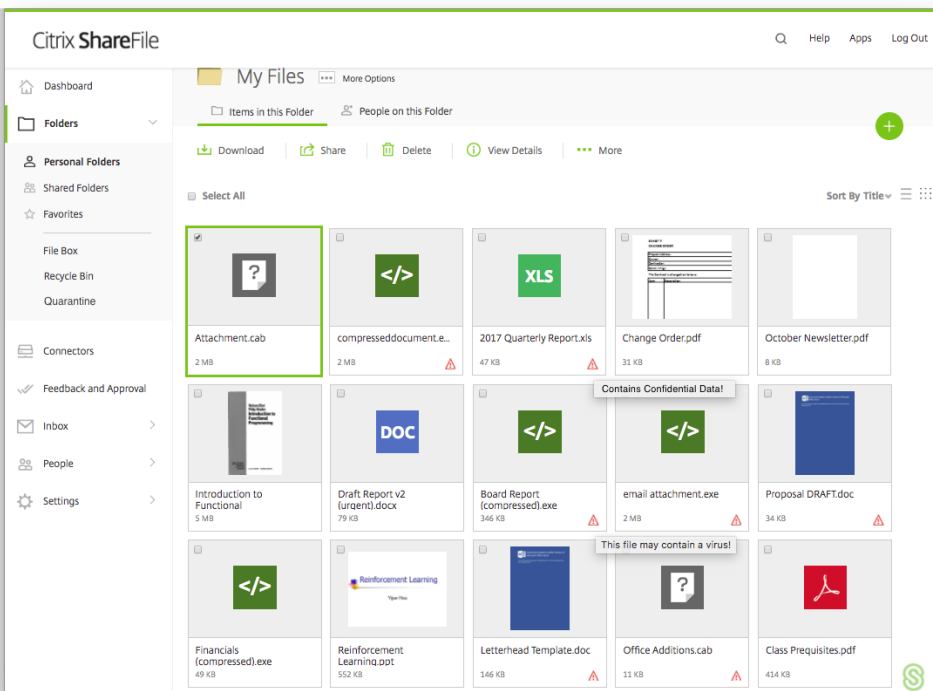


Overview of Avanan

Avanan has been selected to participate in the Security Program for Citrix ShareFile because it provides a full suite of security solutions for data within ShareFile. It is also compatible with other SaaS applications that might be used by their customers so that security policies used within ShareFile can be applied across all their data in the cloud.

Avanan augments ShareFile's native security features by adding the following capabilities:

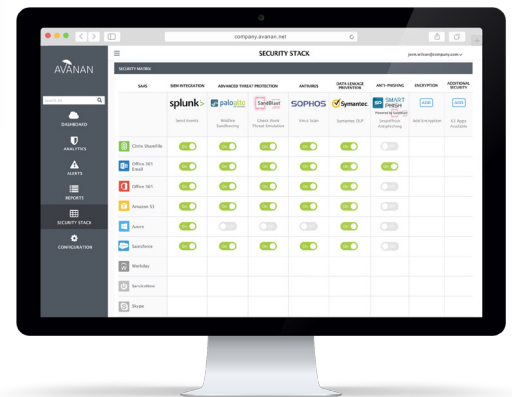
- Antivirus scanning
- Malware sandboxing
- A.I. predictive malware detection
- Data leak prevention/file classification



Avanan is not a single security technology but a platform of tools from multiple companies across a range of security categories.

Avanan integrates seamlessly with ShareFile, using Citrix's existing authenticated API. The user's work routine is unaltered and uninterrupted, with Avanan working behind the scenes to ensure the security of data. In response to each user action, Avanan performs the tasks necessary for maintaining security: file scanning, file moving, permission changes, etc. are all done automatically according to company policy.

Once the IT administrator has initiated the single-click deployment process, Avanan handles everything; no further input is required. Administrators can monitor the process if they wish via the Avanan interface, but even that degree of involvement is unnecessary. Neither IT administrators nor



users will have cause to interface with Avanan — or even be aware of its presence — as all Avanan alerts appear natively within the ShareFile interface.

Because the Avanan platform requires no software agent or redirection of traffic, it is device agnostic: the user's experience does not change whether using a desktop web browser or endpoint agent.



Avanan Solution Detail

Avanan provides a full suite of security solutions for data within Citrix ShareFile as well as any other SaaS application in use by the customer. It does this by connecting cloud-based versions of third-party security tools directly to the SaaS provider's infrastructure, using Avanan's native application programming interface (API).

In essence, the Avanan platform is an app store for cloud security, offering one-click shopping for organizations looking to fulfill their cloud security needs.

Avanan has established partnerships with today's top security vendors and proactively seeks new technologies to counteract the latest threats. No matter tomorrow's attacks, Avanan will have the next-generation tool to defend against it.

Organizations deploy Avanan to protect data in the cloud using:

- **Zero-day malware protection:** Malicious files can spread through shared files and synchronized documents. Avanan offers the industry's most advanced malware protection for zero-day malware and targeted phishing attacks.

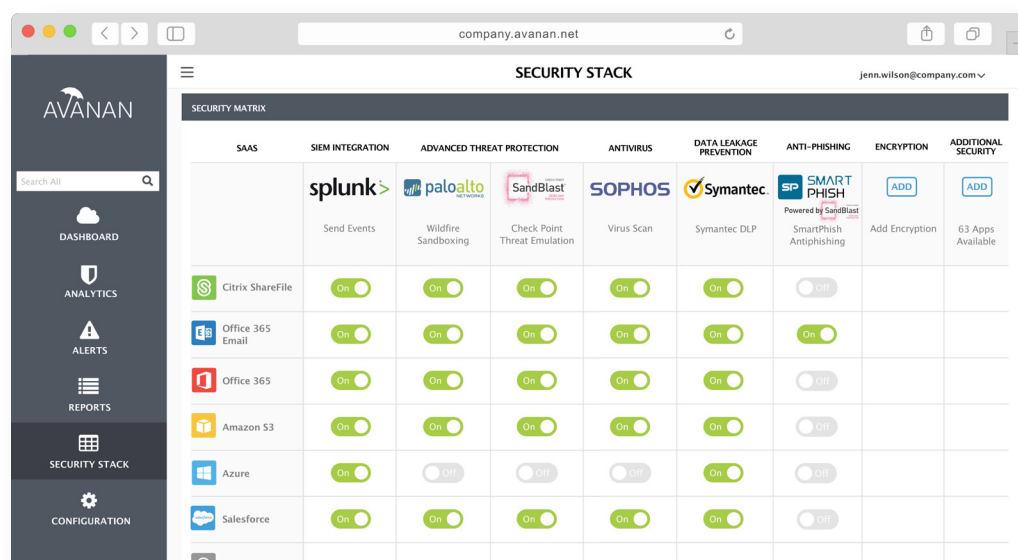
- **Data leak prevention:** Identify and protect confidential information to ensure data compliance with all cloud operations.
- **Insider threat detection:** Avanan analyzes both real-time and historical events, to identify anomalous behavior.
- **Policy-based encryption:** Ensures that organizations are able to maintain control of their files, even after they leave the cloud.
- **SIEM integration:** Organizations may view all events within ShareFile and other SaaS applications using their existing security incident event managers.⁴

Avanan's offers several innovative and unique features that are not available within any single product:

- **Best-of-breed:** On the Avanan platform, customers can select the most advanced features from multiple security vendors to incorporate them into a single solution. Avanan actively seeks out new technologies and adds next-generation features as new threats emerge.

- **Complete visibility:** Avanan connects directly into the SaaS infrastructure, capturing every user, file, event and policy change — both in real time and historical, whether performed by an employee or an external collaborator.
- **Proxy-free deployment:** Many cloud security vendors rely on a gateway — a potential point of latency or failure which can only monitor recent employee traffic. Avanan's cloud-native API offers complete real-time visibility and historical information that are vital for behavior analysis and eDiscovery.
- **One-click deployment:** Since the Avanan platform uses no proxy, endpoint agent or datacenter appliance, it can be deployed in minutes. Avanan's integration with Citrix makes it seamless.

Importantly, Avanan does not add to the burden of already-overworked IT departments. An administrator simply checks a box for each selected security solution, and Avanan is live within minutes.



⁴ <https://www.avanan.com/all-saas>



Citrix + Avanan: A Proven Partnership that Leverages an Entire Industry's Best Technology for Maximizing Cloud Data Security

Anyone charged with protecting an organization's data will find the most recent Experian *Data Breach Industry Forecast* to be quite a frightening read.⁵ The report details a number of chilling cybersecurity threats, discussing nightmares such as nation-state cyberattacks, aftershock password breaches and international data breaches.

But a couple of sentences particularly stand out: "While some tried and true attacks continue to serve as go-to methods for hackers, there are some evolving tools and targets that are likely to become front page news in 2017. Organizations can't wait until an attack happens to ensure they are protected — they need to look at the signs early on to start preparing for new types of security threats."

There is a problem with those tools: no single SaaS security solution provides the best solution for all possible threats. One tool might provide best-of-breed defense against

phishing attacks. Another might provide an antivirus defense. And many single-feature vendors offer mutually exclusive technologies that typically deploy as a proxy rather than as an integrated part of a complete security solution.

For the above reasons, selecting the best-in-breed defense against each type of threat would likely require that a company deploy dozens of security solutions.

Or just a single security solution platform: Avanan.

Avanan is changing the way that companies find, compare, buy and deploy security for the cloud. It makes best-of-breed solutions from more than 70 companies available through a single, one-click-enabled platform. Since Avanan constantly updates its security solution offerings to incorporate partners with the latest and best solutions, it solves the "evolving tools" problem. Organizations can

rely upon Avanan to always provide them with the best-in-breed solutions for current and constantly evolving threats.

Avanan's selection to participate in the Security Program for Citrix ShareFile means it can provide enterprises worldwide with a proven, reliable solution for enhancing the already-robust security features of ShareFile. In today's world, after all, it is simply not possible to have too much security.

For more information about Avanan cloud security for Citrix ShareFile, please visit: <https://citrixready.citrix.com/avanan/avanan-the-cloud-security-platform.html>

For more information about Citrix ShareFile, please visit: www.citrix.com/sharefile

For more information about Enterprise Security visit: <https://www.citrix.com/it-security/>



⁵ <http://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf>

Appendix

Learn more about the Citrix Ready Marketplace: <https://citrixready.citrix.com/>

Learn more about the enterprise security advantages provided by Citrix ShareFile at: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/sharefile-enterprise-security-whitepaper.pdf

To learn more about the Citrix Ready partnership with Avanan, please visit: <https://citrixready.citrix.com/avanan.html>

To learn more about cloud security and performance solutions enterprises, contact Citrix and Avanan.



About Citrix Ready

Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.

About Avanan

Avanan, The Cloud Security Platform, protects data in any SaaS application. Partnering with over 60 of the industry's most trusted security vendors—from Check Point and Cylance to Sophos and Symantec—Avanan offers cloud-native versions of their most advanced technology to protect against malware, phishing, ransomware, data leakage, insider threats and more. The cloud-based platform is completely out-of-band and can be deployed in one click.

© 2017 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).