SECURE FILE-SHARING AND COLLABORATION

SUREDROP®

SUREDROP® SECURE BY DESIGN

The file-sharing and collaboration marketplace is crowded with applications promising to deliver on the potential of a work anywhere, with anyone, culture. Solutions like DropBox, Box and OneDrive all offer a degree of security but, for many organisations, they don't meet their standards for maximum data protection. Increasingly, data sovereignty, which is to say 100% data location control, is also being considered as a serious security issue.

SureDrop is different. Secure by design, it was developed as a security application, featuring end-to-end encryption and data sovereignty control. Customers can also opt to include the most advanced and effective Content Disarm and Reconstruction (CDR) technology to protect against malicious content.

USERS
- Simple, secure file-sharing and collaboration
- Unlimited file size and type
- Integration with Office 365 and Azure Active Directory

SECURITY & COMPLIANCE
- End-to-end encryption
- Role-based user management

IT & OPERATIONS
- Cloud or on-premises deployment
- 100% data sovereignty control

CONTENT DISARM & RECONSTRUCTION
- Protect against disclosed and zero-day attacks
- Retain 100% file functionality
- High performance, low latency solution

THE FILE-SHARING APP YOUR IT DEPARTMENT WILL APPROVE OF

SureDrop offers the flexibility of deployment as an on-premises solution or SaaS from the cloud. Customers are also free to choose where they want their files stored.

SureDrop also integrates with Votiro Disarmer to provide best-in-class protection against malicious content. Vitiro's patented Content Disarm and Reconstruction technology provides protection against the full range of malware, including unknown and zero-day attacks.

SureDrop is developed for organisations that have strong security policies around file storage, but still need the productivity benefits of a fully-featured file-sharing solution.

It allows people to store, share, sync and collaborate on all their files in the cloud with an enterprise-class solution and end-to-end security, featuring standards-based encryption.

SUREDROP FOR MANAGED SERVICE PROVIDERS

SureDrop provides the ideal opportunity for Telecommunications cloud, SaaS and Managed Service Providers to add value to their customers by offering secure file-sharing and collaboration as a custom add-on.

Optimised for as-a-service deployment, SureDrop may be added to any customer's service provision without management overhead.

SUREDROP'S CREDENTIALS

SureDrop is brought to you by Senetas, a global leader in the development of end-to-end encryption solutions. Our products secure data networks and protect network data for commercial, industrial, government and defence customers in more than 40 countries.

They offer maximum data protection without compromising network or application performance and user experience.

SENETAS SECURED™

SECURE FILE SHARING AND COLLABORATION FOR ALL

No matter where or how the people in your organisation work, there is always the need to share, collaborate and sync files - both internally and externally. While you want to enable collaboration, data security should always be the first priority. If it's not, the risk of non-compliance and data breaches become a serious problem.

Our customers have been telling us that their mobility and productivity initiatives are frustrated by insufficient levels of security delivered by existing file-sharing solutions. While many are user friendly, elegant and effective, they're simply not safe enough because:

- They lack true end-to-end encryption
- Key management is not state-of-the-art
- They cannot enable 100% file location control

SureDrop is secure by design, it provides end-to-end encryption with state-of-the-art key management to ensure maximum security, without compromising performance or user experience.

In design, features and functionality, SureDrop addresses the security issue associated with file-sharing and collaboration, to the highest standards required by governments and large enterprises.

If you've come to enjoy the familiarity of Dropbox, Box, OneDrive or Google Drive, you'll love the security, elegance, convenience and flexibility of SureDrop.

ENJOY THE SUREDROP EXPERIENCE. DESIGNED TO BE BETTER.

Effortless file-sharing without compromise

SureDrop provides all the tools and functionality you've come to know and love from solutions like Dropbox. We've simply added the surety of end-to-end encryption security and data sovereignty control, so people who can't use existing solutions can use SureDrop.

Robust, standards-based encryption

SureDrop is different because it has been designed and built from the ground up using defence-grade security. For example, SureDrop uses AES256 standards-based encryption algorithms because our developers support the view that it gives longer term protection than 128 bit keys.

A fully integrated, autonomous solution

SureDrop is fully self-governing and does not require external appliances to generate or distribute encryption keys. SureDrop all happens securely within the local area network, so your internal users enjoy the speed and efficiency of sharing files across the LAN.

State-of-the-art encryption key management

SureDrop gives you peace of mind that your encryption keys cannot be accessed by anyone but you. Senetas encryption key management delivers 100% control of your encryption keys. Your IT department is free to implement and manage the most stringent key storage security.

High performance and high availability

SureDrop delivers the highest possible resilience to data network or device failure because it has designed-in fault tolerance and self-healing capabilities. SureDrop's architecture and built-in redundancy minimise the inconvenience of communication failures. This ensures your files are always available and in sync.

Malicious content protection

Votiro Disarmer* leverages patented Content Disarm and Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks and malware. Votiro sanitises incoming files, eliminating the risks associated with all malicious content including zero-day or unknown attacks, whilst preserving 100% file functionality.

Flexible deployment

SureDrop is available as an on-premises, SaaS or managed service provider solution. However you choose to deploy your solution, SureDrop's security features are the same.

Secure key management

SureDrop provides simple and secure encryption key management across the entire lifecycle; including key generation, storage, distribution and deletion.

Microsoft Azure

SureDrop is fully compatible with Microsoft Azure, enabling customers to deploy it as part of a IaaS, PaaS or SaaS solution.

Office 365

By providing fully compatibility with Microsoft Office 365, SureDrop enables simplified file collaboration on the world's best-known office software suite.

* Votiro Disarmer is a fully integrated extension to SureDrop available at additional cost.

IS SUREDROP RIGHT FOR YOUR ORGANISATION?

SureDrop is developed for organisations that take security seriously. If you have strong security polices around file storage, sharing and collaboration, but still need the productivity benefits of a fully-featured file-sharing and collaboration solution. You should consider SureDrop:

- Your data may contain personally identifiable information, intellectual property or other sensitive content that should not be exposed to potential data breaches.
- Your organisation is currently blocked from using applications like Dropbox because they don't meet your security and data sovereignty policies and standards.
- You want the ability to add best-in-class protection against ransomware, malware and other malicious content as a result of known, unknown and zero-day attacks.
- You need to leverage the productivity power of a mobile workforce, by securely sharing files and collaborating across multiple mobile platforms and devices, but at present you can't.
- You have a geographically dispersed workforce that needs to share files and/or collaborate easily and securely.
- You're currently using Dropbox, Box or an equivalent, but you're concerned that your staff are sharing sensitive files that are stored outside your control and off sovereign soil.
- You're concerned that your file-sharing and collaboration system is exposing your business to malicious content, serious attacks and potential data breaches.

Fully redundant storage

SureDrop has a fully redundant storage mesh of servers that may be configured to keep up to 10 copies of every file.

Files may be spread geographically as backups or just for caching purposes. It's up to you how much storage you install and manage. Regardless of how you need to configure your storage, SureDrop is disaster recovery compliant.

SureDrop on-premises

SureDrop has been designed as a secure on-premises solution using enterprise technologies, like Microsoft Windows infrastructure stack and SQL Sever (2008 R2 and above), so it will feel familiar to you from the start.

SureDrop integrates directly into Active Directory and even integrates into your current backup strategy, so you know your data is safe.

SureDrop automated components

SureDrop is broken down into a number of easy to manage components that may be installed on any arrangement of servers. We support scaling under load, and remote updates are designed to make your life as an infrastructure administrator easy. Once you install the SureDrop clients once, they never need to be manually updated again.

SureDrop extensions

For customers seeking additional layers of security, SureDrop is also available with the Votiro Disarmer extension. Votiro Disarmer leverages patented Content Disarm & Reconstruction technology to protect your files from the most advanced, persistent cyber-attacks and malicious content.

Votiro Disarmer sanitises incoming files, eliminating the risks associated with zero-day and unknown attacks whilst preserving 100% file functionality.

Systems requirements

To make the most of the benefits of SureDrop, we recommend the following minimum specifications for your Windows Server:

12 GB RAM, 80 GB HDD and any standard 1.4 GHz 64-bit processor for Windows Server 2016 or 2019.

One-click deployment using Docker

SureDrop provides one-click deployment using Docker for both on-premises and cloud environments. Customers can install and maintain their own highly secure, private instance of the application in their chosen environment to meet data sovereignty and security requirements.

SUREDROP FEATURES AND FUNCTIONALITY:

End-to-end encryption
SureDrop uses AES256 bit keys because our developers support the view that it gives longer term protection than 128 bit keys. What makes SureDrop more secure is its use of state-of-the-art key management - where the keys are securely stored client-side.

SureDrop Authenticated Proxy Server allows access to SureDrop from outside the corporate firewall and does not require access to Active Directory directly. Instead it authenticates via cached x509 certificates.

Secure fragmented file storage
When SureDrop stores an encrypted file, it breaks it into many pieces and randomly stores them. Only SureDrop knows where the pieces are and only SureDrop knows how to put them back together again and decrypt them. It's another layer of security that makes SureDrop so intelligent and so difficult to match.

Zero-touch management
The SureDrop client is remotely deployed using silent install option and automatically updates as required, without IT intervention. SureDrop database servers' (clustered) shared encryption keys are stored onsite in the database and are backed up as part of the database backup process.

Because the encryption key management is fully automatic and does not require intervention until the certificate is due for renewal, you enjoy the convenience and efficiency of zero-touch management.

Admin Console
The SureDrop Admin Console allows you to centrally manage users, groups and functionality throughout your business. So, in a situation where a user's laptop is lost or stolen, for example, you can easily remove their files.

You may also automatically provision new users to the organisation and automatically deactivate them when they leave.

Audit logs
SureDrop provides a full audit history of all your file changes, which are authenticated by SureDrop. Every file change is logged and recorded so you know who edited what document when.

Microsoft Office 365 and Active Directory
SureDrop appears directly in Microsoft Office's file menu, it's directly integrated into Office 365, making it easy to migrate your staff. The Microsoft Azure Active Directory Sync tool makes it easy to automatically manage users with your existing tools.

If you need to share files and/or collaborate with users external to your organisation, for example, there's no problem because you simply use X.509 certificates to authenticate them.

SureDrop also supports double byte characters and unlimited URL length; which means directories can be of any depth and directory names can be of any length.

Version history and undelete
SureDrop allows you to store as many previous document versions as you require. Retrieval of deleted versions is simple; no matter what the file type and who last edited it.

Additionally, thanks to intelligent conflict management you can be sure you'll never lose any of your changes.

Intuitive web interface
Like other "box" applications, SureDrop features a familiar web interface; enabling the intuitive file storage and management that users have come to expect from document sharing and collaboration tools.

Secure internet file-sharing
SureDrop provides the most secure encrypted document management solution for government and commercial organisations' local and wide area networks. It also provides secure document sharing with third party organisations outside the corporate network.

For clients seeking even greater levels of file security, SureDrop may be integrated with third-party security applications; including Votiro Disarmer and KeySecure.

Data sovereignty and location control
Increasingly, organisations require data storage to be confined to their sovereign location. SureDrop's file storage location control provides the flexibility required to ensure 100% data sovereignty compliance.

DEFAULT AND HIGH-SECURITY USER GROUPS FILE PRIVACY.

Your choice of using 'default' or 'high-security' user groups determines the level or privacy required for your SureDrop files. Selecting to add a 'default' user group for file-sharing does not compromise the security. But, 'default' user groups do not have the same maximum data privacy among authorised users.

Default groups

Default group files are accessible to your system administrator on your SureDrop server.

High-security groups

High-security groups are exclusively accessible to members of the group. This is similar to a 'for your eyes only' document policy.

Default groups in action

If you do not select the 'high-security group' box when a group is created, the group created will be a default group, and will have the default group sharing and security properties outlined below. Default groups are just as secure and use client-side encryption with shared keys.

An administrator may add users to a default group using the Admin Console. When an 'inactive' or new SureDrop user is added, they will have access to the group files as soon as they have activated their SureDrop Client.

High-security groups in action

Selecting high-security groups ensures maximum file privacy as well as security.

To create a 'high-security' group, you must specifically select that group type in the 'add group' menu.

High-security groups then have maximum possible privacy sharing and security features and privileges.

High-security groups use client-side encryption with unique (not shared) keys.

Only the administrator who initially created the high-security group may add users to that group.

The high-security group status requires that only active SureDrop users may be added to a high-security group.

When a new or 'in-active' (has not activated the SureDrop application) user is added to a high-security group, the user will not have access to the group. The user must first activate the SureDrop application and then be added to the high-security group again.

Without exception, only high-security group members will be able to see the high-security group files.

SureDrop ISP add-on

SureDrop is available from your telecommunications service provider as a custom security add-on.

The ease of implementation means SureDrop can be added to your as-a-Service proposition from your ISP with zero management overhead.

For your service provider, it's an opportunity to provide a value-add service that delivers unrivaled security. For you, it means secure document sharing and storage.

For government customers and service providers, SureDrop provides an ideal solution for the sharing of sensitive or classified information that requires a protective environment.

SureDrop has been specifically developed to meet the stringent security criteria of a protective environment; providing all the flexiblity and usability you have come to expect from a box-style file-sharing application, without compromising security.

Unlike the public box-style applications that are primarily developed as file-sharing solutions, SureDrop was purpose-designed as a solution for secure file-sharing and collaboration. This is reflected in the rigorous independent security testing applied to SureDrop.

SureDrop provides vital protection against:

- Non-compliant user behaviour
- Internet network eavesdropping
- Network routing table errors
- User transmission errors
- Vulnerable network devices

SUREDROP IN ACTION A TECHNICAL EXAMPLE.

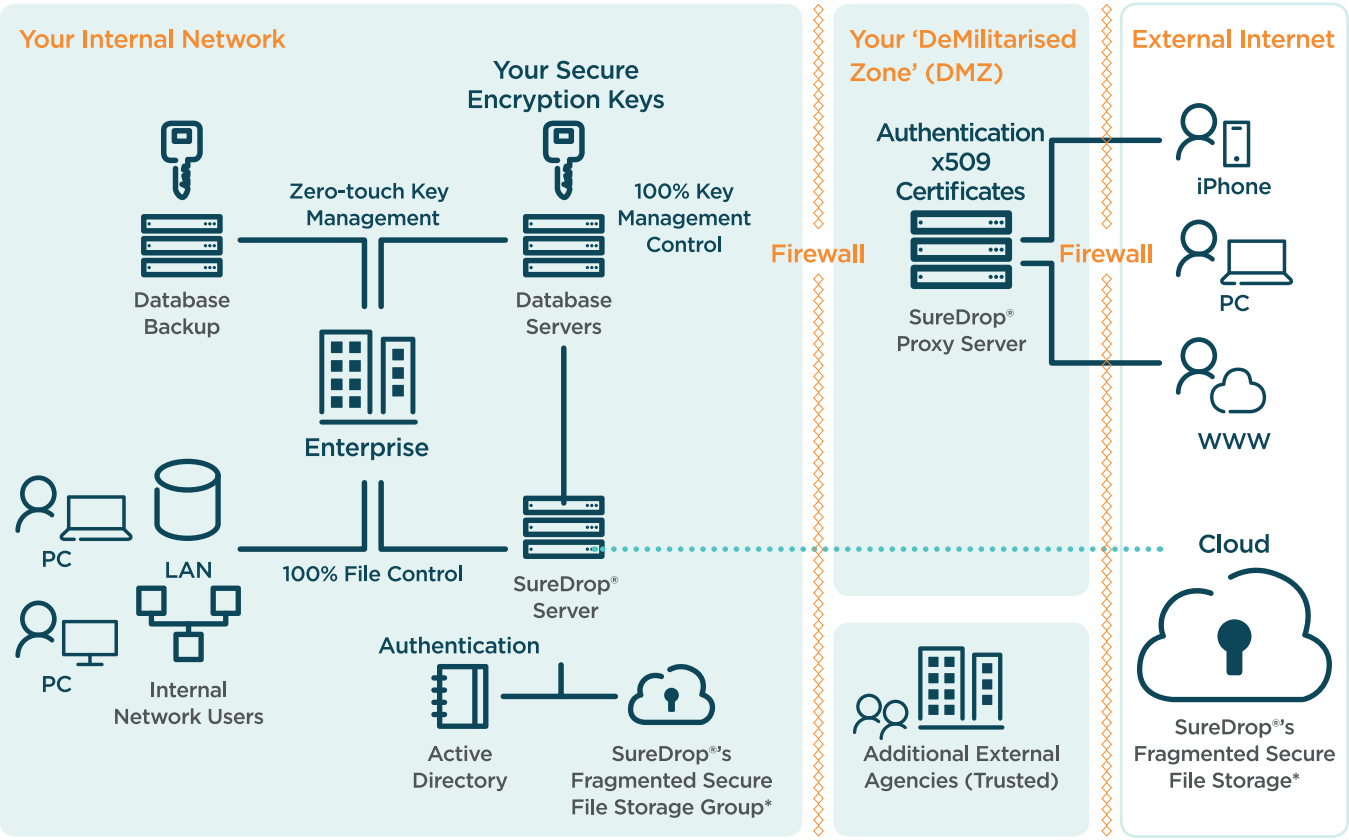
IT departments face some common challenges around secure file-sharing and collaboration solutions:

- File control
- Data sovereignty
- Information security
- Secure collaboration
- Workforce productivity
- Malicious content

Architecture example and illustration

The diagram below illustrates the architectural design recently implemented for a major banking institution. In this example, the bank required an on-premises installation, but needed the storage layer to be implemented externally using Amazon Web Services (AWS).

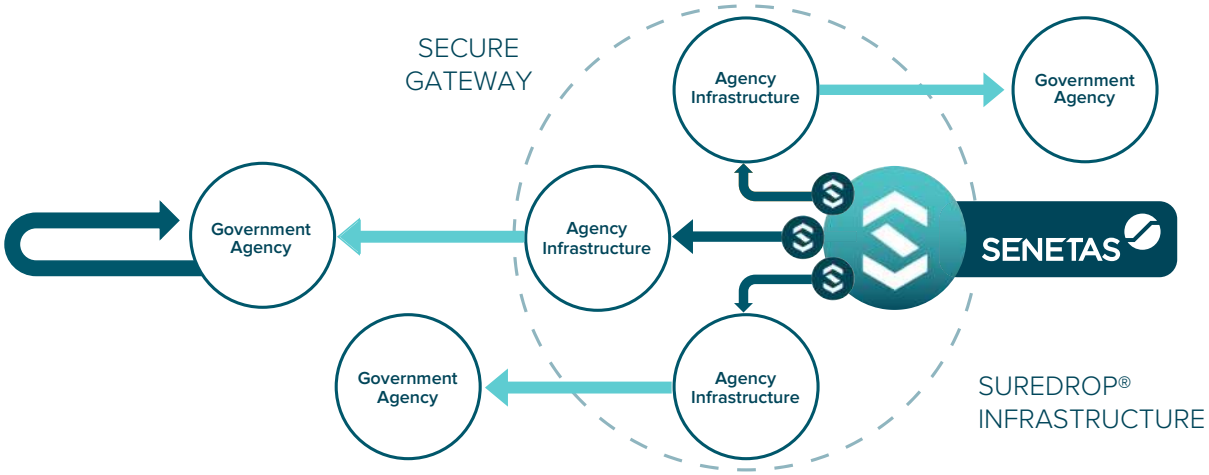
SureDrop storage is anonymised, compressed, encrypted and de-duplicated with all encryption keys securely stored (on-premises) behind the bank's own firewall. This ensured the bank controlled the security solution, and ensured that SureDrop cloud storage met the bank's most stringent security requirements, including data sovereignty and file security.

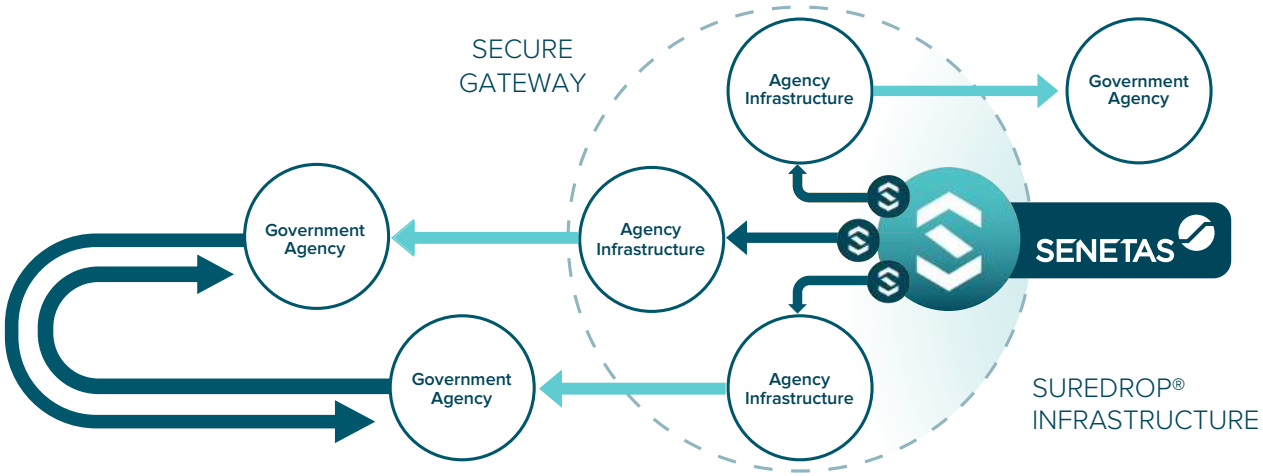


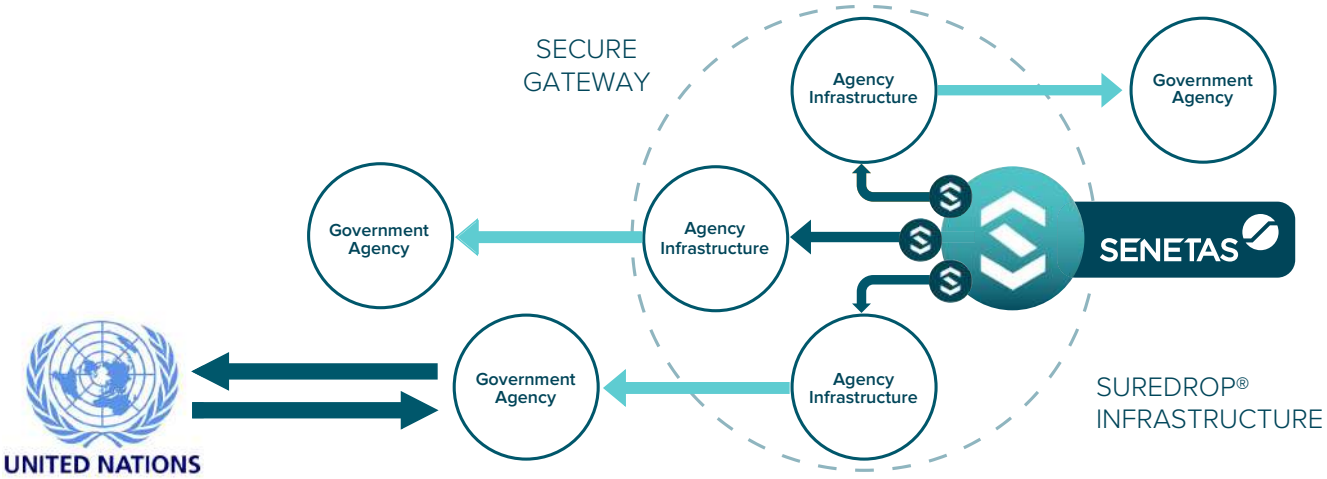
* Optional external storage service.

SureDrop® is available with secure file storage or use your own storage.

TELECOMMUNICATIONS DEPLOYMENT OPTIONS.







FULLY FEATURED SECURE FILE-SHARING AND COLLABORATION.

Feature	SureDrop*	Dropbox	Box
Developed from a 'secure by design' principle	✔	✘	✘
Additional file fragmentation and key security	✔	✘	✘
Sync, share and collaborate anytime, anywhere	✔	✔	✔
100% file location control for data sovereignty	✔	✘	✘
Secure, encryption key management	✔	✘	✘
Support for all file types, sizes and formats	✔	✔	✔
AES 256 encryption standards	✔	✔	✔
Unlimited file copying for backup and recovery	✔	✘	✘
Full integration compatibility with KeySecure	✔	✘	✘
Integration with SaaS/communications and managed service providers	✔	✘	✘
Support for anti-virus and data loss prevention APIs	✔	✘	✘
Flexible billing	✔	✘	✘
Automated file-sharing response URL	✔	✘	✘
Support for Google Authenticator, Active Directory and ADFS	✔	✘	✔
Forensic super-user profile, above administrator role	✔	✘	✘
Optional integration with Votiro Disarmer (CDR)	✔	✘	✔
Compatible with MS Office 365 & Azure AD	✔	✔	✔
Support for Amazon Web Services (AWS) S3 and Windows SMB shares	✔	✔	✔
One-click deployment using Docker	✔	✘	✘

Feature	Description
Active Directory Integration	Users can be established from your Microsoft Active Directory (via LDAP) or established within the SureDrop file system.
Automatic Conflict Resolution	Automatic conflict resolution is required for any Sync application to ensure that changes are not lost if multiple edits are done to a document when offline.
Client-Side Encryption	All encryption/decryption is done client-side when using the thick client; or server-side when using the mobile or web clients.
Client-Side Key Management	State-of-the-art key management supports secure, on-premises (client) or cloud key storage for greater data security.
Compression	Combined with de-duplication support, this can reduce the client storage requirements to 10% of the original size for some document types.
Custom Reports and Analytics	Choose from a range of standard reports or create a custom dashboard to suit your specific reporting needs.
Data Leakage Protection (DLP)	For many, DLP is a mandatory requirement. SureDrop natively supports the DLP system of your choice, or can be provided with a configurable DLP solution.
Deduplication	Built-in functionality to allow deduplication of duplicate data.

Feature	Description
Distributed Geographic Storage	Storage of encrypted documents is maintained across multiple geo locations for redundancy and security. Depending upon the facilities provided by the host system, file replication can be enabled.
File Expiry by Date	Files may become unavailable after a defined date, an important feature where the Governance requires date ranges for accessibility of legal documents.
Flexible Document Ownership	SureDrop documents are saved within folders that make up named security groups. Group owners have control over document ownership and group members can be assigned both access and deletion rights.
Flexible Storage Management	SureDrop allows user files to be stored either on-premise or in the cloud. A SureDrop instance can be configured to provide storage replication.
HSM (Key Management) Support	Support for Open Standards Hardware Security Modules (HSMs) ensures that Key Management is secured to FIPS and CC standards using an open standard without trusting your key management to the individual vendors proprietary system.
Intuitive Web Interface (Thin Client)	The SureDrop Web interface is like those generally provided by similar products. The layout is contained on a single screen and is both intuitive and efficient.
KeySecure Integration (Optional)	SureDrop may be configured to use SafeNet KeySecure for encryption key lifecycle management. KeySecure may be located either on-premises or in the cloud.
Mobile Client	iOS client support.
Multi-Version File Support	When files held within SureDrop are updated, new version numbers are assigned and the previous version is hidden from the user. A forensic user is able to restore earlier version if this is required.
Native Windows File-system Encryption Support	Support for Windows Encrypted File-system ensures that even when a document is at rest and opened for editing on the desktop, it is still encrypted and secure.
Non Destructive Deletes	Being able to recover deleted files is important and a standard feature.
Offline File Access	SureDrop comes with offline file access as standard. Providing users with access to content in a secure offline environment, or where network access is limited.
On-Premises Data Cache	Options provided to maintain an on-site data cache to improve performance for customers with large data requirements.
Regional Caches (Option)	Users may opt to create fully encrypted regional data caches (distributed globally) to enhance performance for larger files or datasets.
SAML Integration	Support for SAML and ADFS.
Storage Management – Quota Support	Ability to limit storage for groups of users.
Thick Client	Thick client provided for Windows Desktops.
Thinly Provisioned Local File Copies	When using the thick-client, support is provided to only have a shadow file or shortcut locally, rather than the entire file. This improves performance and ensures that large datasets do not need to reside fully on the client workstation.
X.509 Certificate Authentication	Client authentication via X.509 certificates.
One-click Deployment Using Docker	Customers may install and maintain their own highly secure, private instance of the application in their chosen environment (both on-premises and cloud) to meet data sovereignty and security requirements.

SUREDROP CASE STUDIES PROFESSIONAL SERVICES & BANKING.

TWO DIFFERENT BUSINESSES; THE SAME PROBLEM AND SOLUTION.

Banks and architects may not appear to have much in common on the surface of things, but they do share the same data security challenge: How to securely collaborate in real-time and share commercially sensitive documents, both internally and externally.

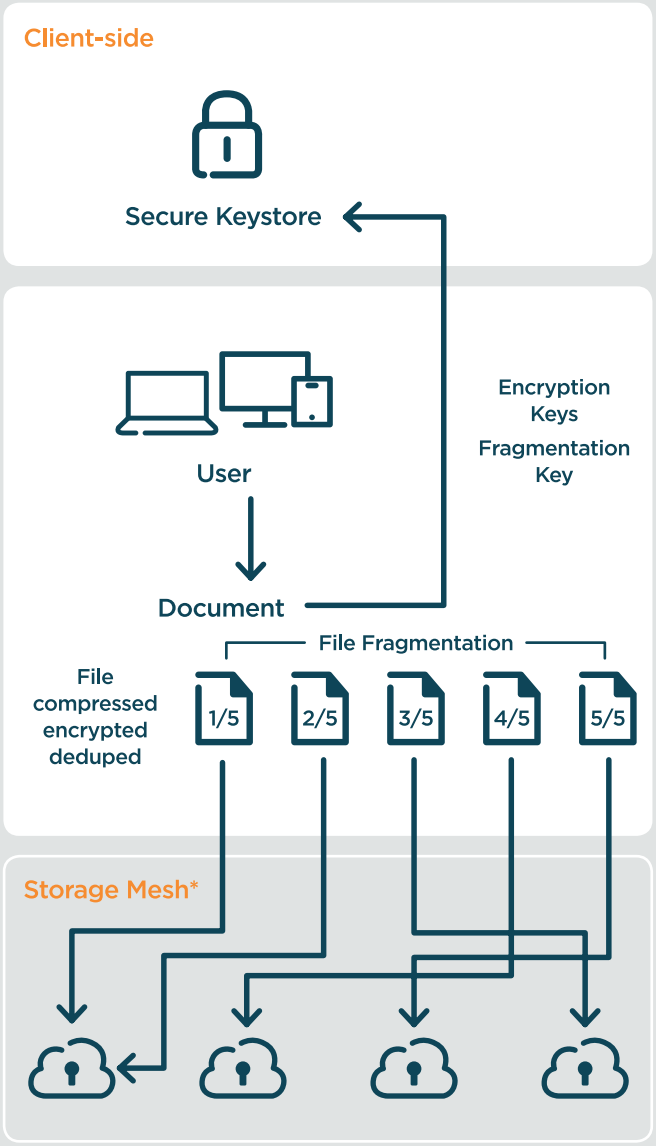
Whether the need for best practice data security is driven by 'commercial in confidence', privacy, or protection of valuable intellectual property; the reality is the regular file-sharing tools are not secure enough.

Before SureDrop, financial and professional services organisations would rely upon email, or even hand-delivery, to share documents. Each party may then have a different version of the files, and no one could really be certain of having the latest version.

Sharing hard copy documents and other large files is inefficent. Emailing them is unsafe and often not possible due to file size limits. In every case ensuring all collaborating parties have the latest version in realtime is neither practical nor safe.

Since then, a number of 'file sync and share' tools have offered user-friendly solutions. But, the world of cyber-crime has rapidly developed, making the risks and the data security component critically important.

Like many enterprise and government organisations, these customers no longer allow staff access to regular drop box tools... until they found SureDrop.



* Based on chosen storage architecture.

A common challenge

Both organisations required a document sharing platform with real-time file syncronisation:

- Specifically developed for secure file-sharing
- Providing state-of-the-art encryption security
- Enabling internal and external file-sharing without compromising security
- The flexibility of on-premises or off-premises file storage

The fundamental security issue for both SureDrop customers stemmed from the awareness that encryption key management is essential to both maximizing data security and ensuring 100% control over their data.

The customers' staff, and the internal and external parties with which they collaborate, were getting frustrated by file-sharing limitations. They resorted to opening their own public cloud-based file-sharing accounts despite the data security risks. But the public cloud services gave staff the convenience, productivity and flexibility they wanted.

To remove the data security risks the bank and architects were exposed to, the public cloud services' domains were blocked across the organisations. Then the search for a more secure tool began.

One solution

SureDrop enables all the file-sharing and collaboration features required; is built around zero-touch standards-based encryption algorithms and key management; offers an on-premises file sync; and provides end-to-end data security.

Both customers required a solution they were able to control and provided them with 100% file control. They did not want encryption keys to reside in a service provider's environment and needed to be certain that service provider could not see the data nor access the keys.

One customer director commented: "We needed a solution that people were familiar with, that could be used when builders were onsite that would allow architects to edit plans even when there was no internet connection."

Consistent results

"SureDrop allowed us to take 100% control of our file-sharing among internal and external parties.

SureDrop automatically keeps every version of every document. But most importantly it automatically encrypts all documents and secures the encryption keys client-side before they end up on the server.

Both customers were impressed by how SureDrop fragments and randomly stores file fragments whilst ensuring that the key is also securely stored on-premises along with the encryption keys."

Another executive commented: "SureDrop is also about empowering our staff and their customer relationships. They are able to work efficiently, on and off-site, and collborate with all parties involved without delays. Our IT department need not worry about staff creating non-compliant public file-sharing accounts to work around our data security limits.

"Importantly, SureDrop is not a 'one size fits all' product. Its implementation is tailored to our systems architecture and our best practice security needs."

"Not only did SureDrop meet all our criteria regarding security, integration, ease of use and management and control; we overcame the weaknesses shared by the current crop of file-sharing and collaboration solutions, which are all managed by the cloud vendors."

YOUR SUREDROP QUESTIONS ANSWERED.

How do I share files using SureDrop?
When implemented, a SureDrop folder is available on your device. Within the SureDrop folder, users folders of any other groups in which the user is included. Saving files to these folders will save them to your SureDrop storage location.

May I access SureDrop from outside my company's network?
Yes, SureDrop is configured to enable secured access anywhere you have an internet connection.

What happens if I accidentally delete a file?
Our 'non-destructive delete' feature is active by default. The deleted file and all previous versions are available from the Admin Console.

How does SureDrop handle multiple users working on the same file while offline?
SureDrop file synchronisation prevents file confusion. The changes made by the first user to reconnect online are considered the 'current' version. Then subsequent changes made by other users will then be saved as additional versions of that file in the same directory.

How is my data encrypted?
SureDrop files are always encrypted end-to-end using 256 bit encryption keys to the industry standard known as AES256. Then all encrypted SureDrop files are fragmented and then stored randomly in compressed files.

You may select to use SureDrop 'high-security groups' feature. This feature provides client-side encryption key management where decryption keys are securely stored only on your device. Hence, in the event of unauthorised access of your organisation's server, your SureDrop files remain secure.

Can the SureDrop 'administrator' read my files?
When using the SureDrop 'high-security groups' feature, only you can see your files. Your system administrator, your colleagues, and not even SureDrop can see your files.

When not using SureDrop's 'high-security groups' feature, only you and authorised users may see your files.

SureDrop's state-of-the-art data encryption and encryption key management, including SureDrop's secure file fragmentation key, ensure that no unauthorised parties will see your files at any time.

What is the significance of SureDrop's 'encryption key management'?
Independent data security experts repeatedly highlight that not all encryption solutions are the same. The critical issue raised is that to ensure encryption is 'unbreakable', cyber-criminals must not be able to obtain access to the data's encryption keys. Equally, third parties must not be able to obtain the encryption keys from your service provider under any circumstances.

Therefore, the encryption keys must be client-side, securely stored and backed-up – on-premises – behind the organisation's firewall; i.e. not in the cloud; nor any location that isn't 100% under your control, such as a cloud service provider.

Zero-touch encryption key management demands that the encryption keys not be accessible by any 3rd party; i.e. not your service provider, SureDrop, or any other entity.

Senetas has used this state-of-the-art encryption key management approach since it first developed its high-assurance network data encryptors. This is why Senetas encryptors are used by many of the world's most secure and data sensitive organisations.

What is 'file fragmentation'?
SureDrop's 'file fragmentation' feature is the third layer of data security that also sets SureDrop apart from other file-sharing solutions.

When your SureDrop file is encrypted, it is instantly fragmented into many parts, which are randomly stored. The fragmentation 'key' itself is also securely stored on-premises behind your organisation's firewall, along with the encryption keys.

Just like encryption, the best file fragmentation feature stores the fragmentation keys client-side. SureDrop is able to instantly encrypt, fragment and securely store your files and keys – all while managing other user updates and synchronising them. And all this happens while still making the latest version instantly available to you!

The beauty of SureDrop is that even with these three layers of data security, SureDrop's file-sharing, synchronisation and user collaboration performance is not compromised.

Does SureDrop need the customer to buy a Docker License, MSSQL license?
Docker is free as long as the customer has a valid Windows OS license. For any practical production environment SQL Server license is required.

How much RAM CPY and Storage does the Microsoft Server require to run the SureDrop management system?
12 GB RAM, 80 GB HDD and any standard 1.4 GHz 64-bit processor for Windows Server 2016 or 2019.

What file storage capacity is required for the SureDrop database?
The SureDrop database does not include file content. It only stores file metadata.

What meta data storage is required as a ratio for every 1TB of user files?
The ratio of meta data storage required is a small fraction of the overall data file volume (<10MB per 1TB).

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales.

Thales is the world leader in digital security and defense, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its SafeNet brand.

THALES

ANZ Partner Community

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers; including:

ADVA Optical Networking
AUCLOUD
Data#3
DATACOM
dimension data
DXC
IBM
macquarie GOVERNMENT
VOCUS communications

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has an encryption solution to suit. Our certified high-assurance encryptors protect data across networks operating at speeds from modest 10Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and and virtualised WAN, supports bandwidths of up to 5Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

SECURE FILE-SHARING

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with known, unknown or zero-day attacks, whilst preserving 100% file functionality.

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file-sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** info@senetas-europe.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

SENETAS SECURED™