SUREDROP®

THE SECURE FILE-SHARING APPLICATION

SUREDROP

SUREDROP® IT'S THE DROP BOX YOU CAN USE AND YOUR IT DEPARTMENT WILL LOVE.

With so many file collaboration products promising a work 'anywhere', with 'anyone', on 'any device' platform, you'd be forgiven for thinking that you're spoiled for choice. Unfortunately, the reality is very different. While solutions like Dropbox, Box One Drive all offer a level of security, for many organisations this is not enough to satisfy their demand for high-assurance data protection.

Only SureDrop provides 100% file control and data sovereignty. Increasingly, organisations see data sovereignty as an important security issue to ensure jurisdiction control over their information.

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 and sync all their files in the Cloud with an enterprise-class solution and defence-grade security.

SENETAS SECURED™ With SureDrop everyone in your organisation gets the mobile collaboration, interaction and productivity they need, but it all happens behind what is commonly referred to as 'unbreakable' encryption security.[1] This is why IT departments love SureDrop.

SureDrop enables any organisation to participate in secure file sharing across the Internet. Whether you are sharing with local or remote employees, customers or suppliers, SureDrop provides the assurance of robust, standards-based data encryption.

SureDrop is brought to you by Senetas Corporation Limited. We build high-assurance encryption solutions for enterprises and governments in more than 35 countries.

Senetas encryption technology and hardware have protected much of the world's most sensitive data without compromising data network performance for 20 years. Our expertise is in protecting your data, whether it's being transmitted across high-speed data networks, stored in multiple data centres or used with your Cloud services.

Our long established reputation in network data encryption, along with our long list of government and commercial customers, are the best assurance you could have that SureDrop is the most secure file-sharing tool available – without compromising your file sharing and synchronisation experience.

[1] As described by the FBI. Refer to: http://www.senetas.com/news/latest-news/senetas-view/the-fbi-used-to-recommend-encryption-now-they-wantto-ban-it/

THE MOST SECURE FILE-SHARING SOLUTION FOR ENTERPRISE AND GOVERNMENT.

No matter where or how the people in your organisation work, there is always the need to share 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 drop box file collaboration and sync and share solutions. While many are user friendly, elegant and effective, they're simply not safe enough.

Senetas provides SureDrop to deliver state-of-the-art, standards-based encryption algorithms, key management and 100% file control security - without comprising your user experience.

In design, features and functionality, SureDrop solves the security issue of convenient file sharing and synchronisation, to the highest standards required by governments and large enterprises.

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

ENJOY THE SUREDROP® EXPERIENCE.
IT'S DESIGNED TO BE BETTER. AND SAFER.

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 reliability, certainty and surety of 'unbreakable', defence-grade encryption security, so people who can't use existing solutions can use SureDrop.

Robust, standards-based encryption
SureDrop is different to other file collaboration solutions because it has been designed and built from the ground up using defence-grade security.[1] 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 the encryption keys. Additionally, because SureDrop all happens securely within the local area network, your internal users enjoy the speed and efficiency of sharing files across the LAN.

Zero-touch encryption key management
SureDrop gives you peace of mind that your encryption keys cannot be accessed by anyone other than you. Senetas encryption key management delivers 100% control of your encryption keys, giving you 100% control of your files. Your IT department is free to implement and manage the most stringent security and compliance policies applicable.

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.

Flexible options to suit your organisation
SureDrop comes in two different types to ensure you get the level of security and functionality you need. We'll engage with you to determine the best solution for your organisation. SureDrop delivers user licences and your IT department provides the storage. SureDrop Premium provides both the user licences and the secure storage.

Compatible with desktop and mobile
SureDrop is enabled for both desktop and mobile devices; allowing you to share and sync content with seamless interoperability.

SureDrop ofers the familiarity and convenience of secure, web browser file functionality.

On-Premises or MSP Deployment
SureDrop is available as an on-premises or managed service provider solution. Whether you prefer a SaaS or on-premises solution, SureDrop's security features are the same.

[1] High-assurance refers to 'best-of-breed' data encryption security solutions that meet government and defence organisations' security approval for their use. Senetas has been developing and manufacturing high-assurance data encryption hardware for governments and defence organisations for use in more than 40 countries for nearly 20 years. All Senetas encryptors hold independent international government testing authority certifications. Senetas encryptors are a best-of-breed solution, in part because their performance includes the use of industry standard encryption algorithms (e.g. AES 256bit) and a management process that gives customers 100% control of their data encryption keys.

IS SUREDROP RIGHT FOR YOUR ORGANISATION?

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

- Your organisation is currently blocked from using Dropbox because it doesn't meet your security policies and standards.
- You need to leverage the productivity power of a mobile workforce, by securely sharing files across multiple mobile platforms and devices, but at present you can't.
- You have a geographically dispersed workforce that needs to collaborate securely.
- You're currently using Dropbox or an equivalent, but you're concerned that your staff are sharing sensitive files outside your control.
- You're concerned that your file collaboration system is exposing your business to serious privacy and intellectual property breaches.
- You have professional practices that rely on safe file collaboration among internal and external parties.

SUREDROP STORAGE: FOR ORGANISATIONS WITH HIGH SECURITY STANDARDS.

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 in different locations as backups or just for caching purposes. It's up to you how many storage severs 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 moment you start using it.

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 a breeze. Once you install the SureDrop® clients once, they never need to be manually updated again.

SUREDROP SPECIFICATIONS AND FEATURES:
ALL THE TOOLS AND FUNCTIONALITY YOU NEED.

High-assurance 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 zero-touch key management - where the keys are securely stored client-side.

Industry standards-based encryption algorithms and zero-touch key management maximise security and ease of use; such as with third-party certificate authorities and enterprise authentication.

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.

Microsoft Office and Active Directory
SureDrop appears directly in Microsoft Office's file menu, so it's directly integrated into Word and Excel, making it easy to migrate your staff.

The Microsoft Active Directory Sync tool makes it easy to automatically manage users with your existing tools.

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

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.

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.

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.

‘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, its an opportunity to provide a value-add service that delivers unrivaled security. For you, it means secure document sharing, storage and collaboration.

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.

SureDrop provides vital protection against:

- non-compliant user behaviour
- internet network eavesdropping
- network routing table errors
- user transmission errors
- vulnerable network devices

SYSTEM REQUIREMENTS: BRINGING SECURE FILE SHARE AND SYNC TO EVERYONE, EVERYWHERE.

Microsoft Windows
Both the SureDrop Admin Console and the SureDrop client for syncing and sharing files run on Microsoft Windows.

Available on the App Store

iOS
SureDrop for iOS is now available. All groups and files may now be viewed on iPhone and iPad.

Android and Mac OS X
SureDrop is also available for Android and Mac OS X, bringing secure file sharing to the full range of mobile devices.

SUREDROP® IN ACTION: A TECHNICAL EXAMPLE

IT departments face the same challenges around secure file sync and share collaboration solutions:

> File control

> Privacy

> Information security

> Efficient collaboration

> Mobile workforce productivity

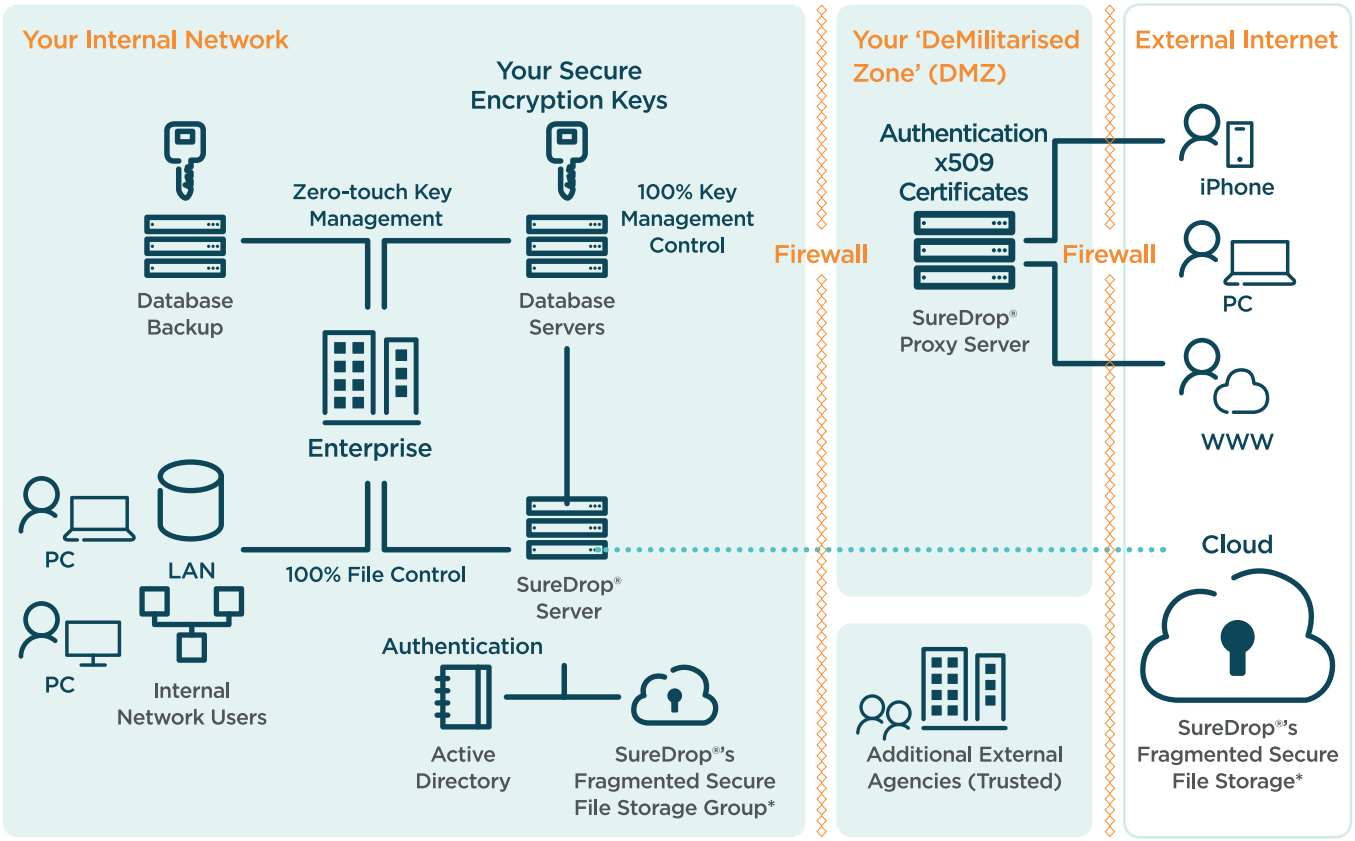
> Secure Cloud

Architecture Example and Illustration

The illustration shows an architecture overview of a broad implementation design, recently completed at a major bank. 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.

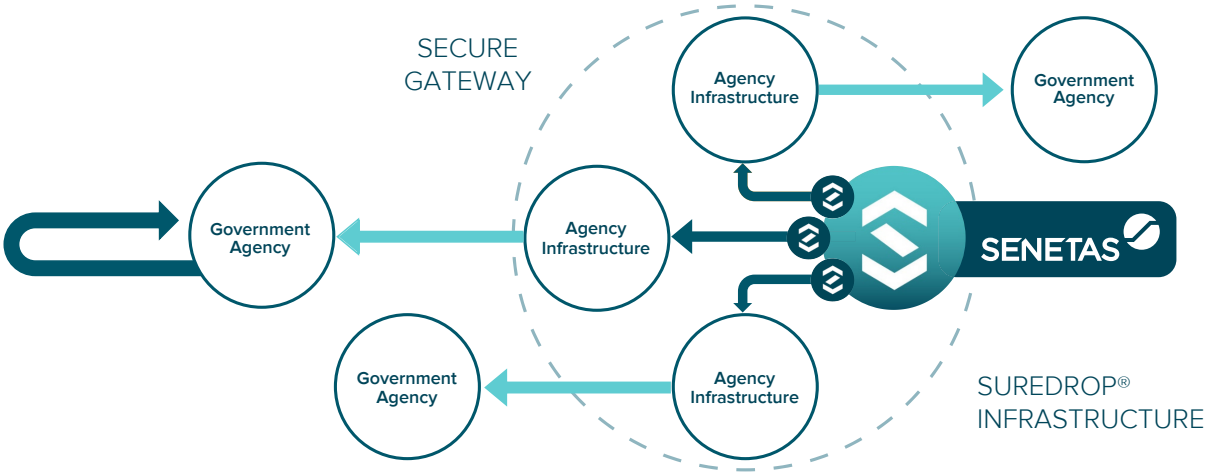
The illustration outlines the infrastructure architecture used in this example as well as the alternative storage solutions supported by SureDrop without compromising zero-touch data security.

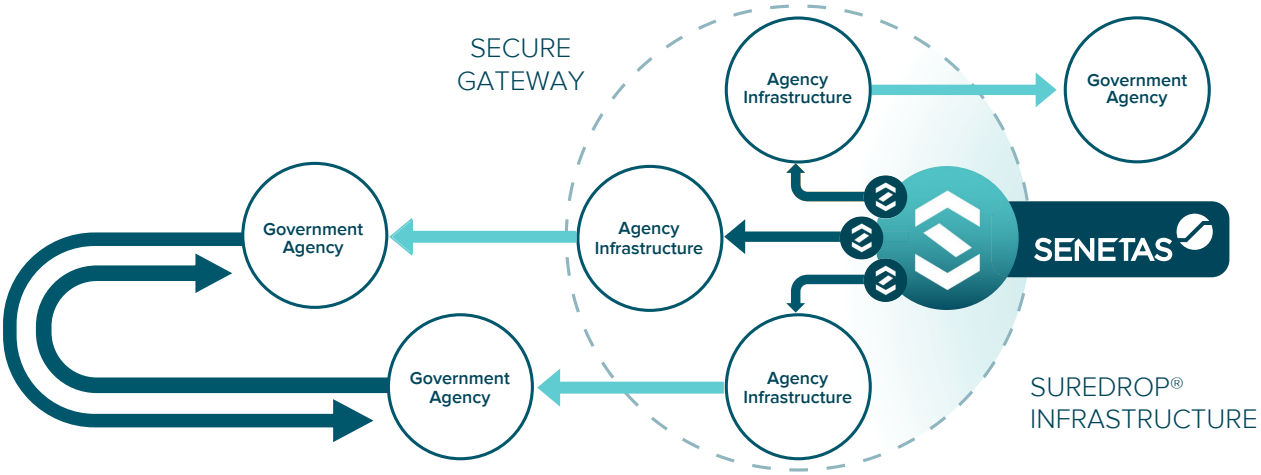


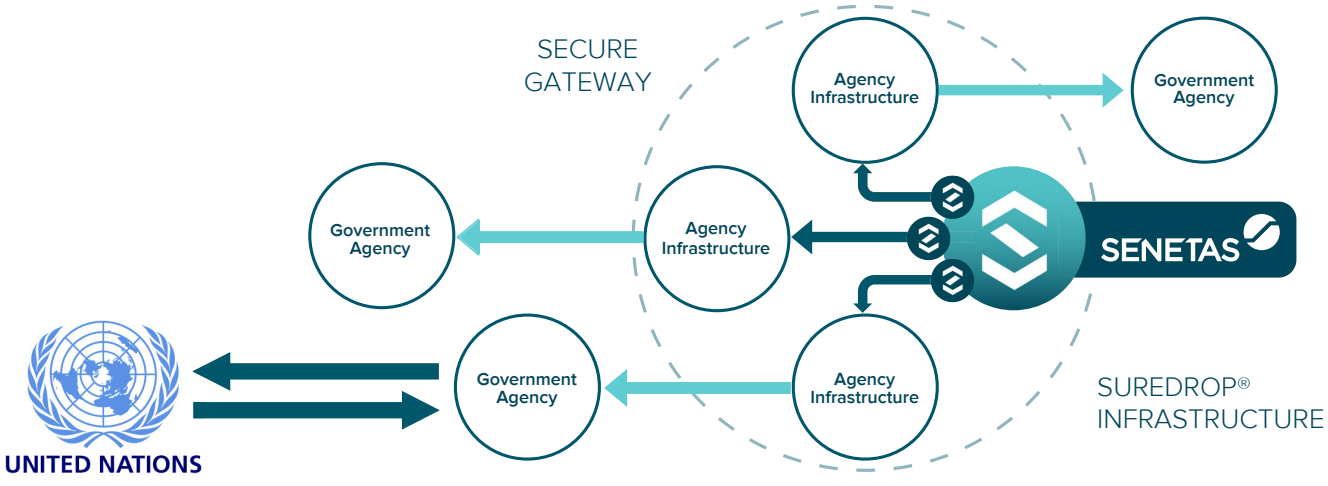
* Optional external storage service.

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

TELECOMMUNICATIONS
DEPLOYMENT OPTIONS







SUREDROP® FEATURES AND PRICING MODELS.

FULLY FEATURED SECURE FILE SYNC AND SHARE

SureDrop's 'unbreakable' encryption and key management do not compromise its performance, ease of use or the features you expect from your file sync and share solution. Compare it to Dropbox or Box and you'll see that SureDrop is fully featured.

Feature	*SureDrop**	*Dropbox*	*Box*
Developed from a security-first principle	✔	✘	✘
Additional file fragmentation and key security	✔	✘	✘
Synch and share anytime, anywhere	✔	✔	✔
Compatible with desktop and mobile devices	✔	✔	✔
100% client-side file location control and data sovereignty	✔	✘	✘
Secure, client-side encryption key management	✔	✘	✘
Intuitive, automatic synchronisation	✔	✔	✔
Support for all file types, sizes and formats	✔	✔	✔
AES 256 encryption standards	✔	✔	✔
Unlimited file copying for backup and recovery	✔	✘	✘
Full integration compatibility with Gemalto's SafeNet 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	✔	✘	✘

Feature	*Description*	*SureDrop**
State-of-the-Art 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.	✔
X.509 Certificate Authentication	Client authentication is done using X.509 certificates.	✔
Distributed Geographic Storage	Storage of encrypted documents is maintained across multiple geo locations for redundancy and security.	✔
Regional Caches (Option)	Options are provided to create regional data caches distributed globally which are fully encrypted to provide greater performance for larger documents and datasets.	✔
Thick Client	Thick client provided for Windows Desktops.	✔
Web Interface – Thin Client	Thin client web interface provided.	✔
Support For 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.	✔
Data Leakage Protection	Data Leakage Protection (DLP) is considered mandatory in modern document storage and management systems. SureDrop® natively supports the DLP system of your choice or can be provided with a configurable DLP solution.	✔
Support for Client On-Site Data Cache	Options provided to maintain an on-site data cache to improve performance for customers with large data requirements.	✔
Support for Client On-Site Key Management	Support for key management on-site at a client premises allows for greater data security irrelevant as to where the data is ultimately stored.	✔
HSM (Key Management) Support	Support for Open Standards Hardware Security Modules (HSM's) 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.	✔

Feature	*Description*	*SureDrop**
Native Windows File-system Encryption Support	Native 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.	✔
Off-line File Access	SureDrop comes with off-line file access as standard. Providing users with access to content in a secure off-line environment, or where network access is limited.	✔
Mobile Client	iOS client support.	✔
Active Directory (LDAP)	Integration into Active Directory via LDAP.	✔
SAML Integration	Support for SAML and ADFS.	✔
Report Capability	Ability to provide customised and flexible reports.	✔
Storage Management – Quota Support	Ability to limit storage for groups of users.	✔
Flexible Document Ownership	By creating storage groups and allocating files to those groups, the membership of those groups can change dynamically without ownership of files when a user leaves an organisation, and by disabling a group, all files in that group automatically become unavailable.	✔
Expiry of Files by Date	Files may become unavailable after a defined date, an important feature where the Governance requires date ranges for accessibility of legal documents.	✔
Non Destructive Deletes	Being able to recover deleted files is important and a standard feature.	✔
Multi Version File Support	Being able to recover any version of any file is also important and should be considered a standard feature.	✔
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.	✔
Deduplication Support	Support to allow deduplication of duplicate data.	✔
Compression Support	Support for compression. Combined with de-duplication support, this can reduce the client storage requirements to 1/10th of the original size for some document types.	✔

FLEXIBLE PAYMENT OPTIONS†.

Suredrop offers the most flexible payment options in the market. Like all popular file-sharING products, SureDrop is available on a monthly, $ per-user license fee basis. (For SureDrop Premium customers, additional monthly storage fees apply.)

For enterprise or government deployments, payment based solely on a per-user basis may not be suitable; That's why we offer a choice of payment options: $ per-user, $ per MB of data used per-month, or a combination of both.

† Conditions apply. Prices are subject to change without notice.

* Excludes one-time costs that may be applicable.

** Minimum agreement term 1 year. Discounts apply for longer term agreements.

SUREDROP® CASE STUDIES
PROFESSIONAL SERVICES & BANKING.

TWO DIFFERENT BUSINESSES; THE SAME PROBLEM AND SOLUTION.

Banks and architects have one data security issue in common: both need to securely share commercially sensitive documents; collaborate externally and internally; and have access to real-time accurately synchronised files.

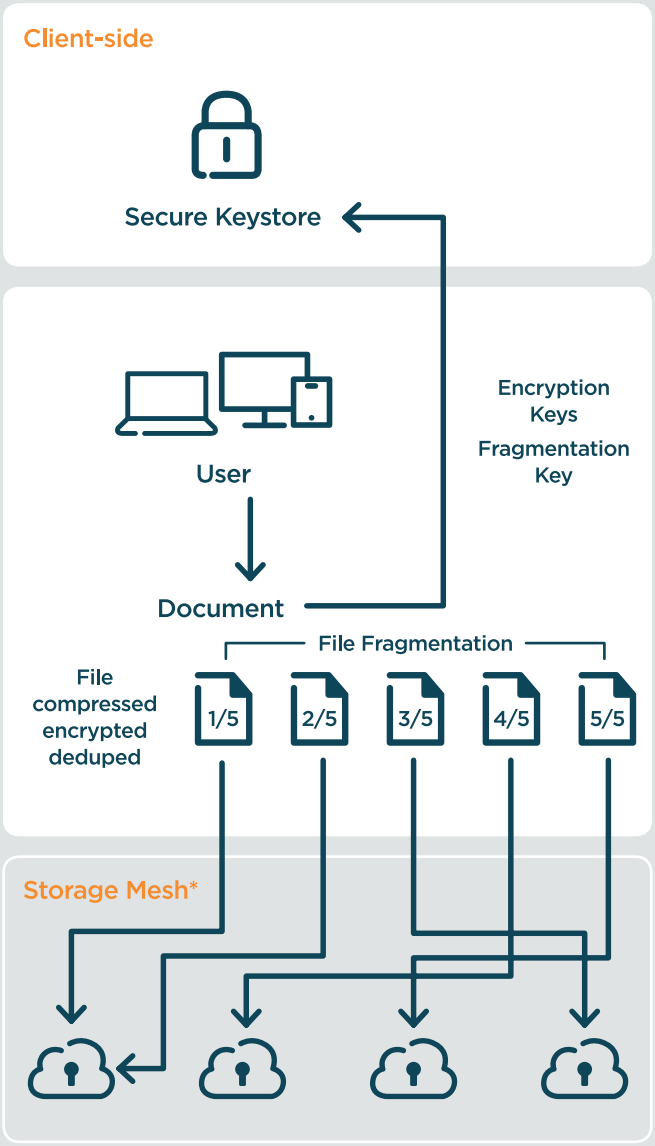
Whether banks' or architects' need for best practice data security is driven by 'commercial in confidence', privacy, or protection of valuable intellectual property; the reality is the regular drop box type file sharing tools are not safe enough.

Before SureDrop, banks and architects mostly emailed or delivered documents to customers, other departments or external parties. 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' collaboration 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 allowed staff access to regular drop box tools...until they found SureDrop.



* Based on chosen storage architecture.

The Challenge

The bank and architecture firm both required a document sharing platform with real-time file syncronisation:

- Specifically developed for secure file collaboration
- Providing state-of-the-art data security
- Enabling internal and external file collaboration 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 collaboration 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.

The Solution

SureDrop enables all the 'file sync and share' collaboration features required; is built around zero-touch standards-based Encryption algorithms and key management; offers an on-premise 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."

The Outcome

"SureDrop allowed us to take 100% control of our files and collaboration 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 currentcrop of file, sync and share 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 the user 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 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.

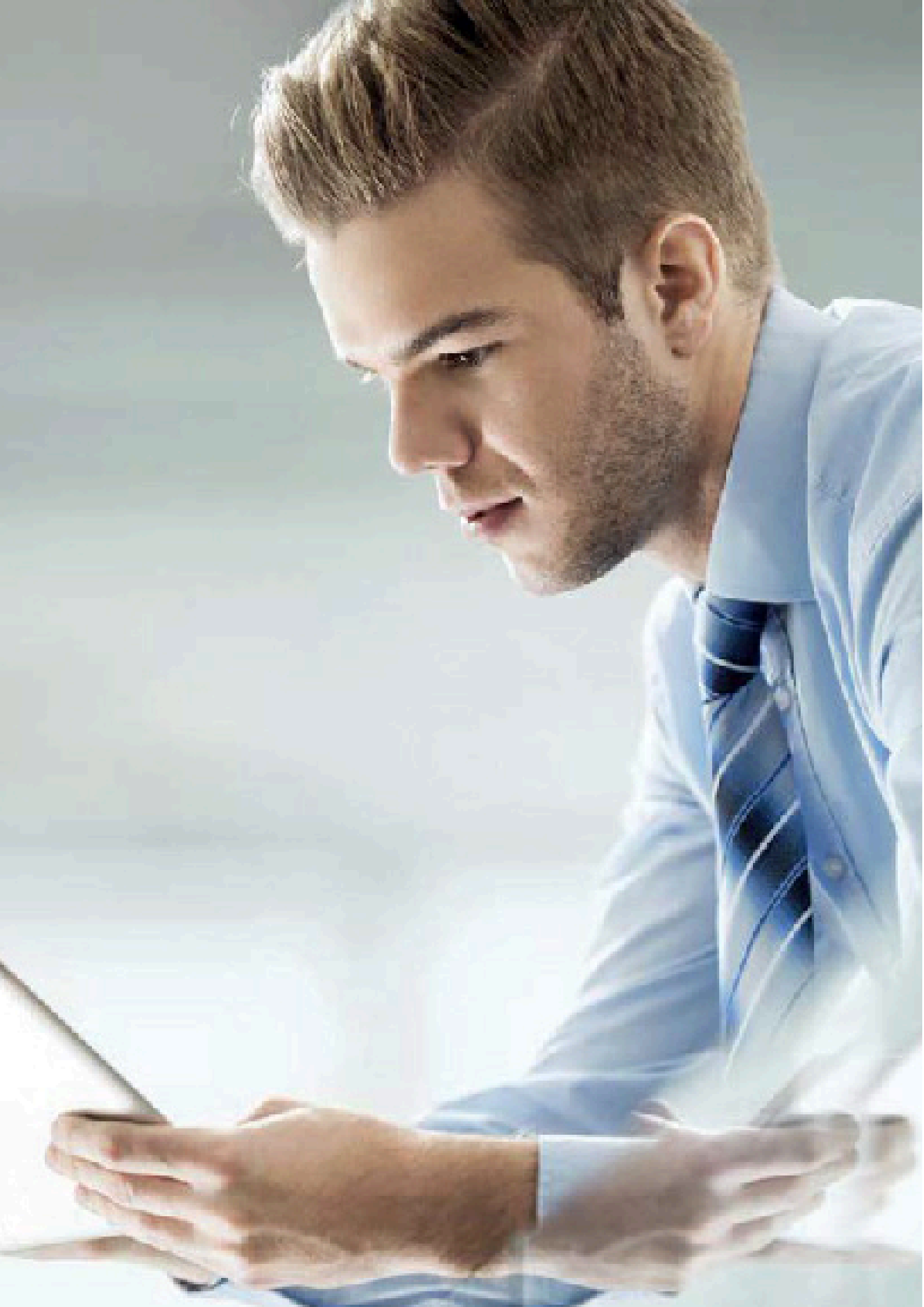
Senetas has used this state-of-the-art encryption key management approach since it first developed its high-speed network data encryptors. This is why Senetas encryptors are used by many of the world's most secure and data sensitive organisations.

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.



ABOUT SENETAS

Senetas Corporation Limited (Senetas) is a global leader in the development of end-to-end encryption technologies. Our solutions protect data in motion for a wide range of commercial, government, industrial and defence applications.

Our CN Series hardware encryptors, CV Series virtual encryptors and SureDrop (our secure file sharing application) all share a common high-performance encryption platform. Thanks to their leading security and performance characteristics, our solutions are used to protect sensitive data and documents in more than 35 countries.

Our encryption solutions leverage state-of-the-art Encryption Key Management and are crypto-agile by design; providing long-term data protection in a post-Quantum computing world. They offer maximum data protection without compromising network or application performance.

Senetas encryption solutions have been trusted to protect much of the world's most sensitive information for more than 20 years. They are used to protect everything from government and defence data to intellectual property, financial transactions to real-time CCTV networks and SCADA control systems.

Senetas solutions are distributed and supported internationally by Gemalto, under its SafeNet brand, within the US Federal Government by SafeNet Assured Technologies and throughout Australia and New Zealand by Senetas and accredited partners.

SENETAS CORPORATION LIMITED

T +61 (03) 9868 4555
F +61 (03) 9821 4899
E suredrop@senetas.com

www.senetas.com
www.sure-drop.com