DropSecure

Encrypt. Protect. Prevent

Enabling True File Transfer Security

How **DropSecure** safeguards your confidential data

DropSecure
Encrypt. Protect. Prevent

Table of Contents

Executive Summary

People transfer trillions of bytes of data to and from locations all around the world every day—often at the expense of privacy and security, because it is far too easy to forget the sensitivity of our data and its vulnerability to interception or other compromise.

DropSecure exists to protect your privacy and safeguard your data by encrypting all files sent through our system using military-grade algorithms before they leave your device. These files are decrypted only after they have been downloaded by the recipient. Unlike some of the most widely used file-transfer services, this end-to-end encryption means that DropSecure cannot read your files at any point, even while they are residing on our servers. Further, we never store the keys required to decrypt your data on our servers. This means that DropSecure cannot read your data even if we wanted to—which we don't.

This real-time encryption shares both a private link and a one-time code with you and your recipient(s) using our patent-pending technology.

While in transit, your data resides in our highly-secured datacenters that meet a broad range of compliance requirements, such as SOC1, HIPAA, and FIPS. This residency can be either transient (for unregistered users) or permanent (for Premium users, who can delete their files at any time.) DropSecure never shares your email address or any other available information with our affiliates or any third party. All file transfers enjoy the highest levels of privacy and security available today.

For even greater security, DropSecure offers a "zero-knowledge" transfer option where your encryption keys never pass through our systems. Using this premium feature requires senders and receivers to register using an email address. This allows you to fully leverage proven public key cryptography in order to securely transfer files without the need to exchange passwords. All standard and premium features are accessible using a simple, intuitive interface that takes only seconds to use.

Key Features

DropSecure offers the following key features and benefits to our customers:

- **End-to-end encryption:** DropSecure is the only file transfer service to provide encrypted downloads as the sole option for using our service. Your data is encrypted using military-grade algorithms before it leaves your device and is never decrypted until the intended recipient(s) have downloaded the file(s) to their system(s).
- **Two-factor authentication:** All unregistered users must enter a one-time verification code in order to download the file(s) being sent to them. For enhanced security, they can choose to receive this code on their phones via SMS. This prevents unauthorized parties from being able to access your data even if your email account becomes compromised. For Premium users, the download link itself is protected using their public key, which cannot be decrypted until they log into DropSecure. Additional Premium authentication factors are currently in development.
- **Protected links:** DropSecure protects all download links for registered and unregistered users alike. An unauthorized entity compromising your download link would not be able to access or decrypt your data because they would lack the decryption key and/or one-time verification code.
- **Zero-knowledge transfers (Premium feature):** The strong end-to-end encryption offered by DropSecure is secure enough for most transfers; however, if required by law, DropSecure could intercept the keys during transit. Zero-knowledge transfers avoid this by not sending keys through the DropSecure system, making it impossible for us to read or encrypt your data regardless of any legal requirement. The zero-knowledge option requires both parties to register with DropSecure using their email addresses.
- **File vault protection (Premium feature):** DropSecure uses public key cryptography to protect assets for registered users. Each registered user receives a pair of public and private keys. Data sent to a registered user is always encrypted using their public key. The private key is encrypted using a strong BCrypt password hash with an AES-256 symmetric key before being stored on our servers. This private key can only be decrypted with the original password. DropSecure never sends user passwords through our system, rendering us unable to decrypt your files at any time.

The Need for Encryption

Cybersecurity is a growing priority for individuals and organizations because data breaches and other attacks are fast becoming an inevitable part of doing business. IT departments have responded to these threats by developing and installing increasingly sophisticated firewalls around the edges of their networks; however, most leaks and breaches originate inside those networks, rendering traditional peripheral defenses ineffective.

Meanwhile, individuals and organizations alike are increasingly relying on cloud service providers (CSPs) to store and transfer data because of the convenience, affordability, and versatility they offer… but not all CSPs encrypt the data they are entrusted with from origination to destination. Those CSPs that do encrypt data normally provide "server side" encryption that only encrypts data after it has arrived on their servers—an approach that leaves the data vulnerable to interception during transit. Users are literally at the mercy of these CSPs and their willingness and ability to encrypt and protect their data, and they know it. Worse, their sensitive files are at risk of unauthorized access, leak, and/or other compromise.

Figure 1 shows how a typical CSP works and why your data is at risk:

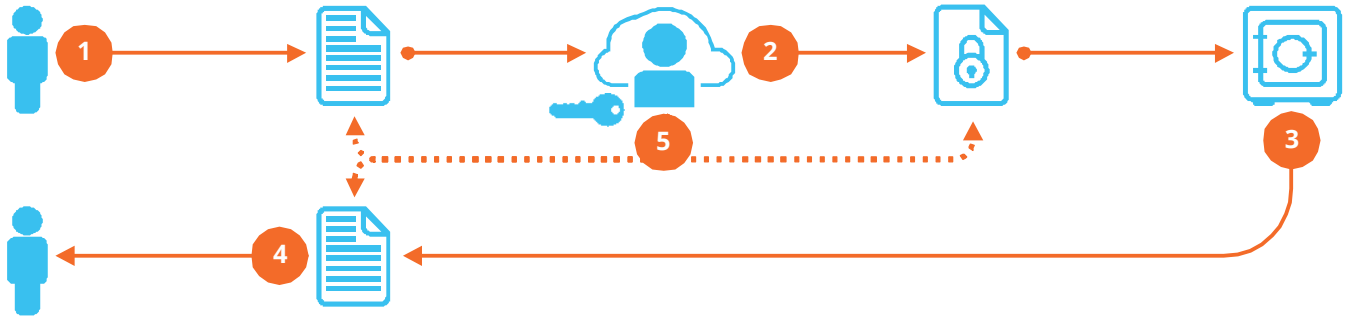

Figure 1: Typical file-transfer process

A typical file transfer process works something like this:

1. The sender sends a file to the receiver in plain text via a CSP.
2. The CSP uses their own encryption key to encrypt the data, which is then stored on their file server.
3. When the recipient clicks the download link, the CSP server uses the encryption key to decrypt the file.
4. The file travels to the receiver as plain text.
5. The CSP owns the encryption keys and can therefore read incoming data, decrypt and read data stored on their servers, and/or read outgoing data.

The connection used to transfer your data from your device to the CSP is usually protected by an HTTPS connection, but the CSP sees it as plain text. Your CSP does have the option to encrypt your documents at rest; however, they can still read your files at any time because they alone have the keys needed to decrypt your data. Further, any compromise of the CSP or your organization could allow unauthorized access to your data.

Passwords are no defense because they can only keep honest people honest. Hackers can bypass passwords, and people inside the CSP are also inside the peripheral defenses mentioned above.

From email providers to social media, file storage, data transfer, and beyond, CSPs have an unprecedented level of access to your sensitive data. They can access and read that data any time they want and can grant that access to others.

Some CSP terms of service even go so far as to explicitly grant them this access... but the lack of such terms does not mean they can't do it anyway. True data security limits the CSP to serving as a medium for transferring data, with no ability to access that data or to make any claims of ownership or control over that data. The only way to achieve this is by using end-to-end encryption and by carefully controlling how encryption keys are handled.

~*~

Enter DropSecure

DropSecure is entirely built around end-to-end encryption, where all communications are always protected by keys that are never stored on our servers. We believe that you deserve the ability to protect all of your data, regardless of whether you share it with a registered DropSecure user or someone else. Premium users can go one step further using "zero knowledge" transfers that prevent DropSecure from being able to read your data under any circumstances.

Becoming a Premium user is as easy as signing up with your email address. DropSecure is pleased to work with business entities to configure their SMTP servers to handle all email/key exchanges. By default, all communications between registered users is zero knowledge; however, a Premium sender with a properly configured SMTP server can leverage zero-knowledge transfers to any recipient, whether or not the recipient is registered with DropSecure.

Free Users

End-to-end encryption encrypts your data before it ever leaves your system. DropSecure stores your encrypted files and emails download instructions to your designated recipient(s), who must then verify themselves. Only then can they decrypt and view the data. You and your receiver(s) are the only parties who possess the keys required to decrypt the files stored at DropSecure. Your data can never be stored or viewed in plain text.

Figure 2 (see next page) displays the free DropSecure end-to-end encryption system in action. The free DropSecure file transfer process works as follows:

1. The sender sends a file to the receiver in plain text via the DropSecure free service.
2. DropSecure uses a one-time encryption key to encrypt the file before it leaves the sender's device. The file then travels to DropSecure. The encryption key used to protect the data is then encrypted with another AES-256 key (encryption protection key), meaning that the encryption key is itself encrypted and that both keys are required to decrypt the file. The encrypted key is sent to the receiver(s) in the email download link, and the encryption protection key is sent to the DropSecure key servers.
3. DropSecure stores the encrypted file on a secure server that meets multiple compliance requirements, such as SOC1, HPIAA, and FIPS. The encryption key and the encrypted key are never sent through or stored on this server; it only contains the encryption protection key, which is useless without the encrypted key.
4. When the recipient clicks the download link, the DropSecure server first verifies the identity of the receiver.
5. Once the receiver identity is verified, the DropSecure key server sends the encryption protection key, which allows the encryption key (previously retried by the receiver via the email link) to be decrypted.
6. The encrypted file sent to the receiver can now be decrypted on the receiver's device.

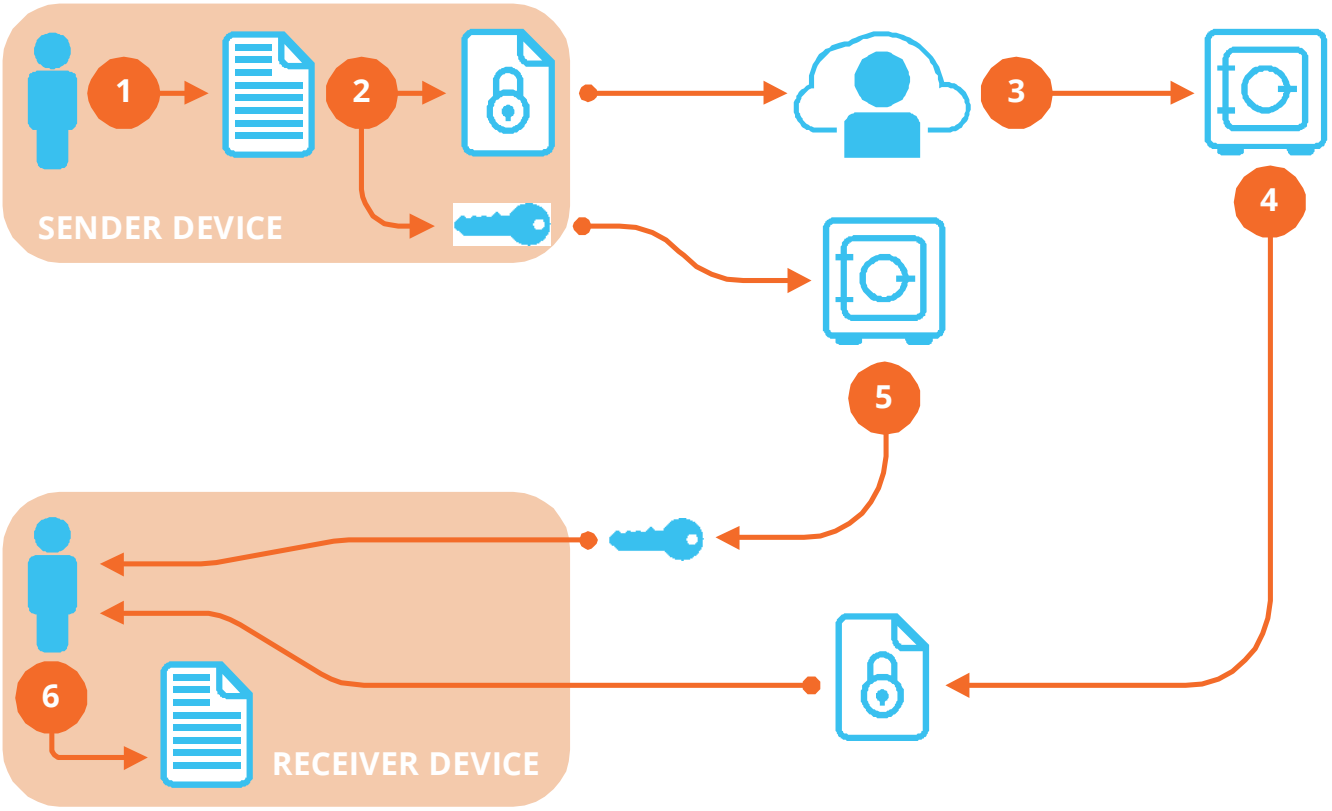

Figure 2: DropSecure file transfer with end-to-end encryption for free users

Free users do not need to register or share passwords in order to benefit from end-to-end encryption while sending files. They only need an email address to send up to ten (10) files with a total size of 2GB or less to anywhere from one (1) to ten (10) recipients. A patent-pending algorithm delivers both a private download link and a one-time verification code to each recipient. Both components are required in order to download the files, which are only decrypted upon receipt. As a further safeguard, the sender receives an immediate notification when the recipient(s) access the data.

As shown in Figure 2, DropSecure never stores your data as clear text. Further, all encryption keys are distributed using servers that are completely isolated from the data storage servers. Unauthorized parties who manage to compromise the data storage servers cannot decrypt your data without the keys, and unauthorized users who compromise the key servers have no access to the data. DropSecure servers reside in highly-secured datacenters that meet a broad range of compliance requirements, such as SOC1, HIPAA, and FIPS.

Premium Users

Used encryption keys are never retained, and DropSecure cannot decrypt historical data. Even so, end-to-end encryption carries the small risk that keys can be compromised during distribution. The fact that the initial key exchange happens through our systems means that we could intercept those keys if

required by law. (We cannot retrieve the keys once they have been exchanged, making it impossible to decrypt historical data.)

For Premium users, DropSecure offers a "zero knowledge" transfer option that uses proven Public Key Infrastructure (PKI) technology to ensure that only the intended recipient(s) can decrypt data. With this option, keys exchanged between Premium users never pass through DropSecure, nor are they stored by us. We therefore have nothing to intercept and are thus unable to comply with any interception or retrieval order. Figure 3 displays the premium DropSecure zero knowledge end-to-end encryption system in action.

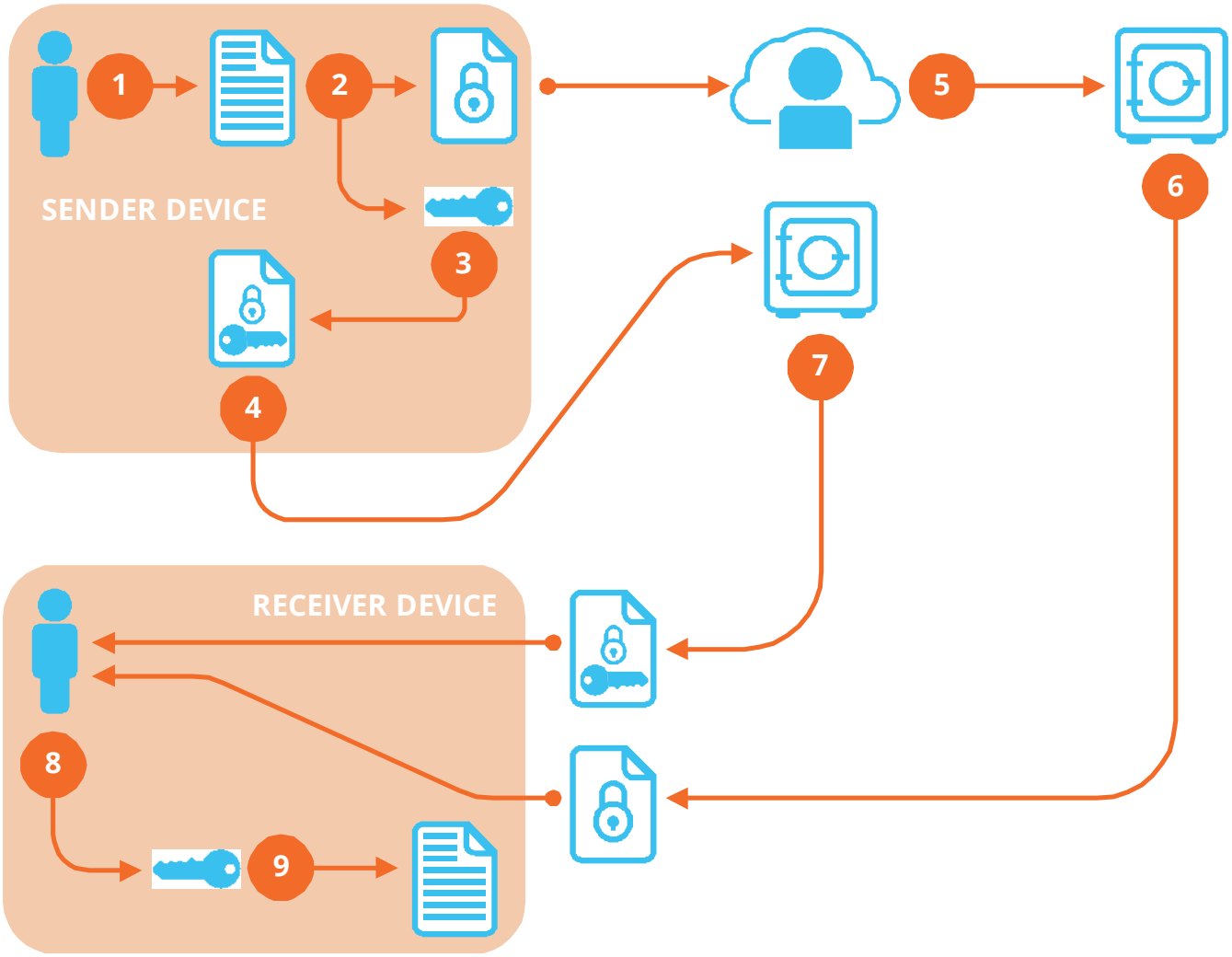

Figure 3: Zero knowledge DropSecure file transfer with end-to-end encryption for Premium users

The Premium DropSecure file transfer process works as follows:

1. The sender sends a file to the recipient via the DropSecure Premium service.
2. DropSecure uses a one-time encryption key to encrypt the file before it leaves the sender's device.
3. The encryption key used to encrypt the file is then encrypted using the receiver's public key. DropSecure does not have the corresponding private key.
4. The protected encryption key is stored on the DropSecure key server, which is isolated from the file storage server.
5. DropSecure stores the encrypted file on a secure server that meets multiple compliance requirements, such as SOC1, HIPAA, and FIPS. The encryption key is not stored on this server.
6. When the recipient clicks the download link, the DropSecure server forwards the encrypted file to the receiver's device.
7. The DropSecure key server forwards the protected encryption key to the receiver's device. Again, the key server is completely isolated from the file storage server.
8. The recipient uses their own private key to extract the one-time DropSecure encryption key.
9. The recipient uses the extracted one-time DropSecure encryption key to decrypt the file.

In this example, the sender (let's call her Alice) and receiver (let's call him Bob) are both Premium users. Alice decides to send a file to Bob via DropSecure. The file is first encrypted using Symmetric AES-256 encryption. The AES-256 encryption key is then wrapped (encrypted) using Bob's public key, which means that only the Bob's private key can unwrap (decrypt) the AES-256 encryption key. Bob's DropSecure password in turn protects his private key.

Bob successfully logs in to his Premium DropSecure account, and the system forwards his encrypted private key to the browser for decryption. Once that is done, DropSecure forwards both the encrypted data and wrapped key to the browser, where Bob's private key unwraps the AES-256 data encryption key. This in turn allows the data sent by Alice to be decrypted.

At no point in this process does DropSecure have any knowledge about the keys or the data. Bob's password is never sent to the server, thus preventing DropSecure from being able to decrypt Bob's private key. Free DropSecure users enjoy one of the most secure file transfer systems available anywhere, with Premium users being able to leverage even greater security for exchanging confidential data.

No data exchange, however well encrypted, can be totally secure unless the sender retains the ability to revoke access to that data. Premium DropSecure users can delete their files at any time, which will prevent further access to that data by all recipients who have not yet downloaded that data. This extra layer of protection can guard against mistakes, such as accidentally sending the wrong file to the wrong recipient. In addition, all files uploaded to DropSecure are automatically purged from our servers after seven (7) days.

Additional Premium Features

DropSecure is currently developing a series of additional Premium features, such as:

- Friendly URL for accessing files, such as dropsecure.com/account, where "account" is the name given to your Premium account. All files sent through this friendly URL will be zero-knowledge by default.
- Storage quotas up to 100GB on our servers.
- Secure file vault that lets you view and download all of the files that you have sent and received. Future enhancements will include the ability to forward files from your vault to additional recipients with no need to upload them again.
- Ability to download a file without waiting for the one-time verification code. You will still need to login in order to download the file.
- Limit how many times a file can be downloaded *(future)*.
- Plug-ins and integrations for various email providers that will allow Premium-level transfers between you and your contacts list *(future)*.
- Password-less login that will make setting, remembering, and resetting passwords a thing of the past *(future)*.

Note: This list is not all-inclusive and is subject to change at any time without notice.

~*~

DropSecure
Encrypt. Protect. Prevent

About DropSecure

Headquartered in Silicon Valley, California, DropSecure employs a global team from New York (USA), Montreal (Canada), and Mumbai (India). Founder and CEO Amish Gandhi has held leadership positions in financial institutions such as Citibank, UBS, and Goldman Sachs, and at tech companies such as IBM, Apple, and Dell.

Gandhi pioneered big data and machine learning systems before they became commonly used, and has architected secure protocols for enterprises using their existing Active Directory and Single Sign On infrastructure.

DropSecure encompasses Gandhi's passion for security and privacy that protects your confidential data using the most advanced cryptography and security technologies available today.

To learn more about DropSecure, visit **https://dropsecure.com/about**

JOIN US ONLINE

@drop_secure

facebook.com/dropsecure

linkedin.com/company/dropsecure

For Additional Information

This white paper presented the need for security when sharing data, why traditional CSPs fail to provide this security, and how DropSecure implements a series of robust measures to protect and secure your data against unauthorized access from all sides. If you would like more information or to schedule a demonstration, please contact us at:

- **Email:** media@dropsecure.com
- **Phone:** 408.620.6972