

YouSendIt Security Policy

The YouSendIt Seven-Layer Security Strategy

YouSendIt employs seven levels of security throughout its infrastructure to deliver the premier secure, reliable digital content delivery platform in the industry, including:

- Secure, Reliable Data Center Facilities
- Network Access Control
- User Authentication and Authorization
- Data Storage
- Data Transmission
- Data Retention
- Auditing

Introduction

Today's ever-growing number and size of digital file formats—such as MP3, JPEG, PowerPoint, Excel and more—quickly exceed the attachment size limitation of commonly used email applications. This has given rise to the popularity of digital content delivery services that enable companies to easily send these files to customers, partners, and vendors so they can collaborate and conduct business fluidly.

YouSendIt provides the leading solution for business-critical and large file deliveries. This on-demand service is used by over ten million people in 220 countries to reliably send, receive and track documents via the YouSendIt website and from popular applications such as Microsoft Outlook, Office, Photoshop, Final Cut Pro and more.

Whether a company is large or small, it must ensure that the file sending solution it deploys offers the highest level of security available. Secure file transfer is not merely a matter of ensuring that no one can intercept data in transit, it requires an all encompassing solution that addresses every possible threat to data confidentiality and integrity. Today, a broad range of solutions exist to meet the needs of companies and individuals that must transfer large files. Most, however, are either inherently insecure or involve cumbersome set up and maintenance issues. Small businesses and enterprise level organizations alike need a solution that offers both highly secure transfer and a low Total Cost of Ownership (TCO).

YouSendIt has implemented a comprehensive, seven-layer security strategy so you can rest assured that your data remains safe and secure at all times. Based on industry-standard security mechanisms and best practices, YouSendIt provides controls at every level of data access, storage, and transfer. In this whitepaper, we will detail each layer of YouSendIt's seven-layer security strategy and explain how YouSendIt provides a low cost, highly secure file sending solution to our customers.



Each YouSendIt secure data center features:

- Dual power feeds
- UPS battery systems, diesel generators, and HVAC systems
- Double-wall construction
- Water suppression technology
- Dry-pipe fire protection
- Environmental monitoring

YouSendIt protects its customers' sensitive information with:

- 128-bit or higher SSL data encryption
- Multi-level, ISP grade hardware- and software-based firewalls
- Intrusion detection technology and regular vulnerability scans
- Continual virus protection scanning
- Ongoing security management and policy enforcement

Secure, Reliable Data Center Facilities

YouSendIt maintains secure, redundant, state-of-the-art data centers in California and London, England. Each YouSendIt data center facility is protected with double-wall construction and secured with biometric and video surveillance security. Physically protected around-the-clock by on-site security guards, each YouSendIt data center includes raised floors, seismically protected equipment, and water suppression and dry-pipe fire protection technologies to prevent damage or loss from fire, earthquakes, flooding, and other natural disasters.

All servers within each data center are secured in a locked room with limited access only by authorized individuals, and every visitor to a YouSendIt data center must possess not only a valid password but also must pass a biometric scan to gain entry. Guests and one-time visitors are always escorted by a data center security guard or another authorized YouSendIt employee. The entry and exit time of each visitor is recorded in a secure audit log.

To guarantee continuous, around-the-clock operations, YouSendIt maintains dual, redundant power supplies for every device and system in each data center, including UPS battery systems and diesel generators. Upon failure of the primary electrical power source, the backup power supply takes over, assuring users of continuous service at all times.

Network Access Control

YouSendIt implements network and ISP grade firewalls to provide IP filtering and intrusion detection protection. Every server in each YouSendIt data center is protected with a constantly updated, industry-leading firewall, which blocks all ports except HTTP and S-HTTP on port 443. Port 443 using HTTP or HTTPS is dynamically opened and closed as required. In contrast, competing solutions using Secure FTP or Secure Shell (SSH) require permanently open ports in a firewall, allowing unfettered inbound network commands and leaving the network vulnerable to attack.

Every server in YouSendIt's data centers is based on the Linux operating system, a secure operating system that is not commonly affected by viruses or malicious attacks. For additional security, YouSendIt conducts regular vulnerability scans of its internal network to proactively detect and prevent security threats.

User Authentication and Authorization

All YouSendIt users must register using a valid email address and password. These credentials are encrypted during transmission and storage using a one-way hash. YouSendIt also requires every registered user to authenticate his or her email address before the user is able to use the YouSendIt service, ensuring that the user has registered a valid email address. Passwords must be more than five and less than 16 characters in length.

When a user requests a password reset, YouSendIt verifies that the correct, authorized user is making the request by sending a notification to the requesting email address that requires a response. In addition, a second notification is sent to the same email address after the password has been reset to verify the password.

Data Storage

All files stored on YouSendIt servers are encoded and stored using a scrambled name, which makes it impossible for a network intruder to identify the file by its original name or read the contents of the file. In order to access and download a file from YouSendIt's servers, either the full download link or complete user credentials are required.

Data Transmission

In the YouSendIt digital content delivery model, a sender uploads a file to a server in the YouSendIt data center. Once uploaded, an email is automatically generated to the recipient or recipients, who then download the file to their computer or computers. To ensure that data is not compromised in either the upload or the download of a file, YouSendIt employs the Secure Socket Layer (SSL) protocol. In order to protect data integrity during file transfer, online payments, and user registration, YouSendIt implements industry-standard, 128-bit SSL encryption deployed using Class 3 certificates and Server-Gated Cryptography (SGC).

For additional security, a customer may require that a recipient use another password to ensure that only a specific person can receive a file. This is common if the file recipient works on a shared computer or email account, or in an insecure environment. In this scenario, the customer specifies a password during file upload. This password is not transmitted by YouSendIt to the recipient. Instead, the customer must communicate the password to the recipient offline. To download the file, the recipient must use the password.

Finally, users can ensure that files are only downloaded by authorized individuals using authenticated delivery. This service requires that the file recipient have a YouSendIt account. The user must login with his or her username and password prior to being allowed to download a file.

Data Retention

YouSendIt automatically stores all files uploaded by a customer for 14 days, at which time the file automatically expires and is deleted. Customers also have the ability to customize the data retention policy to meet their specific requirements, setting file expiration time as short as 30 minutes or as long as 'never expire'. In the event a user notices an unexpected or unauthorized download of a file, he or she can delete the file from YouSendIt's servers.

All user files uploaded to YouSendIt servers are replicated on a second server within the same data center and stored on both servers for the life of the file. In the event of a server failure, the file will be retrieved from other server within the same data center. Server replication to ensure total redundancy is conducted on a daily basis.

Auditing

With YouSendIt's comprehensive tracking tools, customers can monitor how many times a file has been downloaded, by whom, and at what time. This complete audit trail enables customers to ensure compliance with government regulations regarding the traceability of information privacy and accidental disclosure.

To further ensure the security of its customers' information, YouSendIt undergoes quarterly perimeter security audits by third-party auditors. In addition, third-party auditors conduct regular vulnerability scans of the YouSendIt service, alerting YouSendIt to potential new vulnerabilities and ensuring the remediation of these vulnerabilities before they cause a security breach.

YouSendIt is PCI compliant and already complies with the privacy provisions of the Gramm-Leach-Bliley (GLB) Act, which governs certain activities of the financial services industry. YouSendIt qualifies as a service provider under GLBA. For more information, please see www.ftc.gov/privacy/privacyinitiatives/gblact.html

YouSendIt ensures secure data transfer:

- 128-bit or higher SSL data encryption
- Password protected secure file transfer
- Certified delivery option requires user authentication

Customize your data retention policies:

- Data retention can be configured at the user level, group level or company level
- Easily set file expiration options
- Server replication ensures total data redundancy

YouSendIt provides a complete audit-trail for governance and compliance:

- Report on who sent a file, how many times it was downloaded and by whom
- HIPPA and PCI compliant. Graham-Leach-Bliley Act (GLBA) qualified service provider



Conclusion

From physical and network access control to user authentication and authorization to data storage, transfer, and retention to monitoring and auditing, YouSendIt secures your information at every level of data access, storage, and transfer. With its comprehensive, seven-layer security strategy, YouSendIt delivers the only secure, reliable digital content delivery service on the market, giving you peace of mind that your company's confidential and private information always remains safe and secure. When you use the YouSendIt secure digital content delivery service, you can better comply with government regulatory requirements, protect your corporate brand and customer loyalty, and ensure the privacy of your intellectual property and other sensitive data.

For more information about YouSendIt

Visit: www.yousendit.com

E-mail: sales@yousendit.com

Call: 408.879.9118

YouSendIt, Inc.

1919 S.Bascom Ave., 3rd Floor
Campbell, CA 95008

866.55U.SEND

sales@yousendit.com

www.yousendit.com

