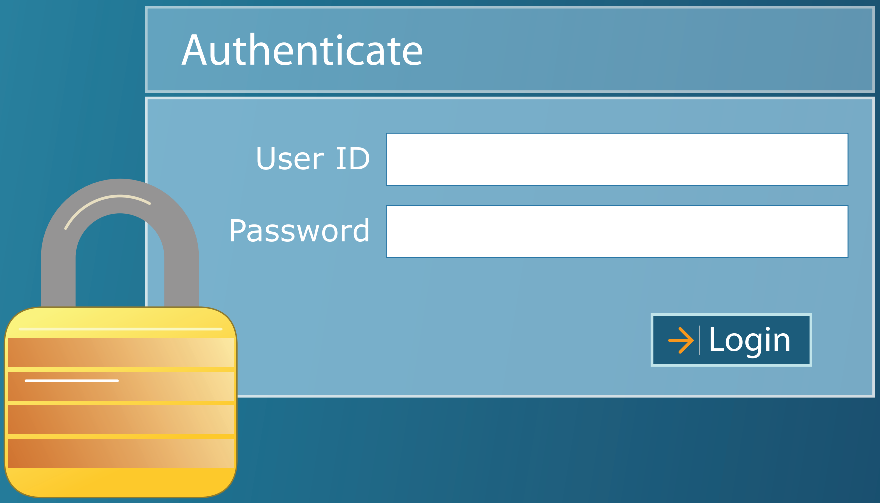
Sendside®

The leading platform for customer communication and interaction

Security Overview



Sendside Networks, Inc.

1590 W. Park Circle, Suite 100
Ogden, UT 84404
801.285.6125
www.sendside.net

Sendside – Security and Technology Overview
Best Practices for When it Matters®

What do we mean when we say "When it Matters?" More than a tagline or a positioning statement, it refers to our DNA- core tenets upon which our organization was founded- to provide solutions for organizations looking to securely, yet easily, disseminate and manage important, personal or confidential information. In contrast to secure email providers that build encryption solutions on top of SMTP email, Sendside has designed a complete communication platform from the ground up with security, next-generation functionality, interactivity and control in mind – not as an after-thought.

Security today goes beyond simply encrypting the body of a message or an attachment. Social engineering, phishing and other email-based attacks seek to compromise a user's private information and have undermined trust in the public email system. Care must be taken to ensure the identities of both the sender and recipient to prevent information from being viewed or accessed without authorization.

In today's fast-paced, global-access environment, organizations are asking for more. They want to control WHERE data resides, HOW it is displayed, WHO can view it or forward it on to others, and exercise control in ways never before contemplated. Sendside's technology allows organizations to do just that, and much more.

Sendside takes security to another level by taking a comprehensive approach to data security – beyond what most web-based services or applications rely on today. In nearly all cases, our approach is far beyond what companies are able to design and implement themselves. Using the latest in active and passive firewall systems, intrusion detection systems, industry-standard transport encryption such as 256-Bit Secure Sockets Layer (SSL) technology and/or Transport Layer Security (TLS), authentication and password security policies, key management and proprietary security protocols, Sendside delivers a world-class communication platform designed to protect information in motion, and at rest.

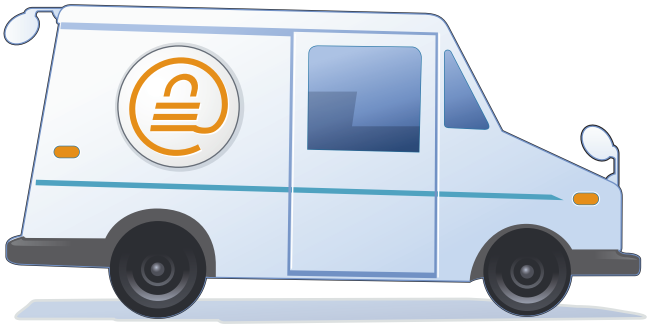
Best Practices

Security is a multidimensional imperative that demands consideration at every level – not just the application level – which includes data management and storage, network infrastructure, and physical facilities. Sendside adheres to the best practices and policies to offer world-class security at each of these levels. Plus, Sendside employs industry experts and partners to attempt to find exploits or vulnerabilities on a constant basis. This keeps us one step ahead so we can offer a level of commercial service unmatched in the marketplace today.

Protection at Every Level

Sendside provides comprehensive protection at every level to prevent failures so information is secure, protected and always available. We employ cutting-edge safeguards at each of the following levels:

- **Network & Transport Level**
- **Application Level**
- **Data Storage Level**
- **Facilities Level**



Network & Transport Level Security

Sendside utilizes multi-level security solutions and proven security practices to ensure an extremely high level of network security:

- Software and hardware firewalls limit traffic to the minimum ports required for optimal network operation.
- Messages, documents, content and applications are delivered using SSL or TLS to ensure a secure connection from a client application (mail client, web browser, etc.) to the Sendside.
- Switches are leveraged in a multi-tiered network architecture to reduce data available to each host and increase throughput.
- The internal network IP addressing scheme utilizes RFC 1918 space, an established standard for a secure, private network.
- Intrusion Detection System (IDS) sensors protect sensitive network segments and provide a real-time view of legitimate and illegitimate traffic.
- Internal hosts are not reachable directly from outside the protected network.

- Support access is abstracted through a specific DMZ host to limit points of entry/exit to data center assets and to add an additional layer of security.

- Redundant equipment has been provisioned to ensure high availability.

- Black listing is in force to help combat: Denial of Service (DOS); Distributed Denial of Service (DDOS) attacks; and to deal with habitual problematic situations.

- All networks are certified through on-going internal and third-party vulnerability assessment programs.

- Central logging with utilities is employed to help in anomaly detection.

Application Level Security

Sitting atop of the Sendside platform are core applications that allow individuals and organizations to interact and transact in a secure manner. Security from the application viewpoint is comprehensive and includes client use, geolocation (IP address), social networking, pattern analysis, authentication, challenge / response pairing and more. These methods and technologies ensure only the sender and the intended recipient(s) are able to view and/or manage communications or information flowing through the network.

In addition to providing a secure and robust application delivery architecture, Sendside takes an extra step by engaging third party security companies to conduct ongoing vulnerability assessments. These assessments ensure that Sendside is a proactively dealing with threats to application security instead of being reactive (status-quo). Sendside's application security policy sets a new standard with the use of the following:

- **Unique Sendside Member IDs** – The use of unique user IDs (instead of email addresses) prevents brute force login attacks using an email address as the login variable.

- **Client computer enrollment** – Each client computer must "enroll" with the Sendside application to provide two, single-factor authentications.

- **Challenge / Response** – Even in the unlikely event that a member's login credentials are compromised; a correct response to a challenge question would be needed to successfully log in to the application and compromise member data.

- **Login monitoring** – Sendside's Login Sentinel tracks and monitors login attempts and can dynamically restrict access, temporarily suspend accounts or disable them altogether to prevent password guessing and brute-force attacks.

- **Encrypted session cookies** – The use of encrypted session cookies ensures the member's identity and simplifies the end-user experience.

- **Most recently contacted (patent-pending)** – Sendside builds a custom login page showing profile photos of people the member most recently contacted. This social networking component makes it virtually impossible to be misdirected to a bogus login page (phishing attack).

- **Password strength meter and policy** – Sendside works closely with the member to help them select a password that would be impervious to adictionary-style attack. Additionally, policy prevents users from reusing old passwords.

- **Password encryption** – Passwords and challenge response values are encrypted on the system using Salted SHA Hashing Algorithm (SSHA) and Salted Message Digest 5 (SMD5).

- **Behavior-based pattern analysis (patent-pending)** – Application and user behavior are continually monitored for malicious activity to ensure a quality experience for all Sendside members.

Data Storage Level Security

Sendside takes active steps to ensure that data residing on the network is encrypted and cannot be compromised by unauthorized access.

- All data stored on the Sendside platform is encrypted using industry standard cryptography to provide another safeguard against unwanted or unauthorized access. Only users correctly authenticating from within a Sendside application are able to encrypt and decrypt information residing in the secure repository. Sendside and our administrators (even with physical access to the equipment) do not have the ability to view customer communication and information stored within the secure repository.

- Encryption keys, for general content stored in the system, reside on different network resources and cannot be accessed by an individual within the organization. Sendside's key management policy ensures that confidential information remains confidential.

- Password protected content provide individuals and organizations with another level of security for ultra-sensitive information. With password protected content, the password is not stored on the system so the information is impossible to decrypt.

- Message Level Authentication (MLA), similar to password protected information, uses a challenge response value known only to the sender and recipient to encrypt and decrypt the data. The value provided by the recipient is hashed using a salted hashing algorithm and it is compared to the value provided by the sender. If they match, the key is used to decrypt the message and it is sent to the recipient. At no time is the key (response) ever stored on Sendside's system. It is important to note that if the sender or recipient cannot recall the response to the challenge correctly, similar to password protected messages and documents, there will be no way to recover the data.

Facilities Level Security

In addition to constantly evaluating and managing access to Sendside at the network, application and data layers, it is critically important to maintain the strictest controls at the facilities level. This effort begins in our corporate offices and extends to our data centers. Visitors are required to register and be accompanied by a Sendside representative at all times while in a Sendside office. Unauthorized physical access is prevented by the use of a secure badge and key. Physical access to Sendside's data centers is even more restrictive. Following are several examples of the physical security measures we employ:

- Authorized personnel must enter a gated environment with car trap and security guards to arrive at the building.

- Authorized personnel must sign in at a guard station and present two-factor authentication, including biometric scanning and ID presentment to enter the data center floor.

- Man traps control foot traffic coming into and going out of the data center floor to prevent "tag-alongs." Access to Sendside's equipment requires another key before physical access can be granted.

- Cameras monitor all entrances and exits, the building perimeter, and loading dock areas.

- The data center is completely anonymous, with bullet-resistant glass and exterior walls in addition to steel fencing around the perimeter. Inert gas in the data center provides fire protection.

Uptime & Data Availability

An uninterruptible power source with N+1 generators is in place to ensure system uptime in the event of electrical outage. Network connectivity consists of three individual providers all using SONET based services. Multiple conduits provide extra protection against accidental line cutting. In addition, redundant storage arrays ensure very high uptime and availability of data, and all data is routinely archived based on an organization's polices and requirements. Finally, the data center also is resistant to earthquakes measuring up to 7.5 on the Richter scale.

A glossary of key terminology is provided on the following pages.

Glossary

About TLS:

An excerpt from: http://en.wikipedia.org/wiki/Secure_Sockets_Layer

The TLS protocol allows applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications privacy over the Internet using cryptography. Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (whether an individual or an application, such as a Web browser) can be sure with whom it is communicating. The next level of security — in which both ends of the "conversation" are sure with whom they are communicating — is known as mutual authentication. Mutual authentication requires public key infrastructure (PKI) deployment to clients unless TLS-PSK or the Secure Remote Password (SRP) protocol are used, which provide strong mutual authentication without needing to deploy a PKI.

About DMZ:

An excerpt from: http://en.wikipedia.org/wiki/Demilitarized_zone_%28computing%29

In computer security, a demarcation zone (DMZ) or perimeter network, is a physical or logical subnetwork that contains and exposes an organization's external services to a larger, untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network.

About Geolocation:

An excerpt from: http://en.wikipedia.org/wiki/Geolocation

Geolocation refers to identifying the real-world geographic location of an Internet connected computer, mobile device, or website visitor. Geolocation can be used to refer to the practice of assessing the location, or it can be used to refer to the actual assessed location or locational data. Geolocation can be performed by associating a geographic location with: the Internet Protocol address, MAC address, RFID, hardware embedded article/production number, embedded software number (such as UUID, Exif/IPTC/XMP or modern steganography), invoice, Wi-Fi connection location, or device GPS coordinates, or other, perhaps self-disclosed, information.

The term is also used in other contexts to refer to the process of inferring the location of a tracked animal based, for instance, on the time history of sunlight brightness or the water temperature and depth measured by an instrument attached to the animal. Such instruments are commonly called Archival Tags or dataloggers.

About SHA:

An excerpt from: http://en.wikipedia.org/wiki/SHA_hash_functions

The SHA hash functions are five cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length. They are called "secure" when:

- It is computationally infeasible to find a message that corresponds to a given message digest.
- It is computationally infeasible to find two different messages that produce the same message digest.

Any change to a message (including single bit changes) will, with an exceedingly high probability, result in a completely different message digest. The five algorithms are denoted SHA-1, SHA-224, SHA-256, SHA-384, and SHA 512. The latter four variants are sometimes collectively referred to as SHA-2. SHA-1 produces a message digest that is 160 bits long; the number in the other four algorithms' names denote the bit length of the digest they produce.

SHA-1 is employed in several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It was considered to be the successor to MD5, an earlier, widely-used hash function.

About MD5:

An excerpt from: http://en.wikipedia.org/wiki/MD5

As an Internet standard (RFC 1321), MD5 (Message-Digest algorithm 5) has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32 digit hexadecimal number. MD5 is widely used to store passwords. To mitigate the vulnerabilities mentioned above, one can add a salt to the passwords before hashing them. Some implementations may apply the hashing function more than once.

About Salt:

An excerpt from: http://en.wikipedia.org/wiki/Salt_%28cryptography%29

In cryptography, a salt comprises random bits that are used as one of the inputs to a key derivation function. The other input is usually a password or passphrase. The output of the key derivation function is stored as the encrypted version of the password. A salt can also be used as a key in a cipher or other cryptographic algorithm. The key derivation function typically uses a hash function. Sometimes the initialization vector, a previously-generated value, is used as a salt.

Salt data also make dictionary attacks and brute-force attacks for cracking large number of passwords much slower. Without salts, an attacker who is cracking many passwords at the same time only needs to hash each password guess once, and compare it to all the hashes. However, with salts, all the passwords will likely have different salts; so each guess must be hashed separately for each salt, which is much slower since hashing is usually very computationally expensive.