



SEND WORD NOW SECURITY AND TECHNOLOGY

Overview

Send Word Now's goal is to provide a completely secure, flexible, scalable, and reliable system that customers can trust. Our infrastructure is based on a strong foundation, which is maintained through systematic updates, monitoring, auditing, and reporting. The security of our system is based on a defense-in-depth approach, and provides comprehensive protection against attacks. In order to protect the system, we have secured all equipment in hardened parts of the network that are not externally accessible, and use both carrier-grade Session Border Controllers (SBCs) and firewalls. Send Word Now's SBCs are configured to only accept traffic from white-listed IPs, while all other traffic is ignored so as to not incur any overhead to the gateway.

In 2009, Send Word Now successfully completed a SAS 70 Type II audit as a part of its commitment to security, dependability, and customer support. An independent audit firm tested Send Word Now's platform, validating the full operating effectiveness and integrity of Send Word Now's infrastructure. Based in multiple datacenters throughout the United States and in the United Kingdom, the system is configured to prevent attacks, and has a proven track record of reliability. We will continue to have our systems and operations certified annually.

Foundation

Send Word Now's infrastructure was built from the ground up, using technology from recognized industry leaders. All aspects of the foundation are based on industry best practices and solid designs that guarantee security and reliability.

Data Centers

Currently, Send Word Now has colocation space in top-tier colocation facilities from Equinix, TWTC, 365 Main and TaTa. Each hosting location provides extensive physical security, with on-site security guards present 24/7 supplementing both indoor and outdoor security monitoring. Access to any given facility requires a valid photo ID and a name on the list of pre-authorized personnel. Biometric hand scans are also required for entry, and they limit hosting customers from moving from one co-location area to another within the facility. Closed circuit cameras monitor and record all areas within the facilities, and customer equipment is kept in either a locked cage or a locked cabinet. The hosting provider keeps the keys to all cages and cabinets; customers do not have copies of the keys. As a result, only Send Word Now personnel have physical and logical access to Send Word Now resources.

Power is provided by dual municipal power feeds entering the buildings at different points. The facilities' UPS is comprised of parallel strings of batteries or flywheel technology that are in-line with the main power for instantaneous power in the event of municipal power failure. Additionally, facilities have N+1 or greater diesel generators capable of handling full power load. The generators are supplied by tanks capable of keeping the generators running for 48 hours with active refuel contracts in place.

Cooling at all facilities is also N+1 or greater for all equipment necessary to maintain normal temperatures.

All of our facilities are designed to maintain 100% uptime and, in some cases, to provide 100% uptime SLAs. Data centers are also located very far apart from each other, eliminating the possibility of a "regional" disaster crippling the service.



Network

The Send Word Now network is built on Cisco technology and complies with the highest industry standards. The network has a demilitarized design, and compartmentalizes Internet-facing devices in a restricted area. Any devices communicating to or from the Internet reside in the demilitarized zone (DMZ) and have tightly controlled Access Control Lists (ACLs) to limit communications with other parts of the network. ACLs are written following a well-defined firewall configuration policy to ensure that the strictest possible ACLs are always in place. The perimeter and DMZ firewalls are Cisco Adaptive Security Appliances.

All communication with the Send Word Now application is performed via secure means. Send Word Now supports secure protocols (including HTTPS, FTPs and SFTP) and encrypted email using PGP.

Servers

Send Word Now uses Dell servers for its core computing platform. Servers are specified with scalability and reliability in mind, eliminating single points of failure wherever possible. All servers have dual power supplies and, where applicable, redundant network connectivity.

Operating Systems

Send Word Now's software is based primarily on the Microsoft Windows operating system. All systems are built with the latest service packs and hardened based on Microsoft best practices for installations. Our builds follow detailed configuration procedures to ensure that all servers are hardened to the same level of security.

Application

The Send Word Now alerting application has been developed with security in mind. It provides a rich set of security-oriented features that include communication via secure means, role-based permissions, and detailed logging, reporting and auditing capabilities.

Maintenance

Send Word Now strives to keep all aspects of its infrastructure up-to-date in order to maintain the most secure and reliable system on the market. We perform routine maintenance procedures to support our high standards.

Patches

Send Word Now performs regular patching of all systems following manufacturer patch release schedules. Send Word Now follows a documented patch management process to ensure consistent patching every cycle. At a high level, the patch process is as follows: patches are monitored for a week to see if any other organizations or manufacturers report any difficulty. Patches are then tested in multiple quality assurance environments before they are rolled out to the remainder of the environment. This process can be accelerated if a serious risk security patch is available. For manufacturers that do not follow patch cycles, patches are reviewed and deployed as needed.

Send Word Now Application Updates

As operating systems evolve, so too does the Send Word Now application. Send Word Now performs regular updates to continually enhance features as well as address security concerns.



Adapting Methodologies

As with everything else, methodologies need to be adapted from time to time. Send Word Now has built a flexible infrastructure and application that can adapt to evolving practices. This includes the activities necessary to build, maintain, monitor, and manage the infrastructure.

Monitoring, Auditing, and Reporting

In order to ensure the highest possible security and performance, Send Word Now's foundation undergoes routine monitoring, auditing and reporting procedures. We achieve this in a number of ways, and we do everything we can to keep our processes transparent.

Logging

Send Word Now believes that full logging is the key to providing the greatest amount of transparency within all aspects of the system. This includes every aspect of the infrastructure, from the data center to the application itself. To achieve this end, Send Word Now uses a product called splunk to collect and aggregate available logs. Splunk simplifies the collection and manipulation of logs, making searching, reviewing and auditing very easy. Splunk also provides a means of non-repudiation.

Network Intrusion Detection System

Not all activities generate logs, and for this reason, Send Word Now uses Network Intrusion Detection Systems (NIDS) to monitor network traffic for known malicious or suspicious traffic. NIDS are very important not only for detecting malicious attacks, but also for catching activity that may precede an attack. Send Word Now NIDS are placed just behind the firewall in the DMZ and just behind the firewall in the internal network. This provides full coverage of all traffic entering the DMZ from the internet as well as from the DMZ into the internal network.

Anti-Virus

At Send Word Now, malicious network traffic is detected with anti-virus software. All of our Windows-based servers have anti-virus software installed and updated regularly, and we routinely scan all systems for intrusions.

Scans

Send Word Now actively looks for potential security weaknesses by performing regular scans of all devices in the system. Scans are performed using Nessus and are run internally with direct access to all devices in order to provide the clearest security assessment. Send Word Now also contracts annually an independent third party for unbiased review of our security measures. Additionally, many of our customers perform their own penetration testing, and many of the tests are performed using guidelines from the OWASP project.

Performance

In addition to security, Send Word Now closely monitors and profiles the performance of its system. Send Word Now uses both off-the-shelf products like SiteScope and Zenoss as well as a rich suite of custom tools built specifically for monitoring the unique Send Word Now system.



Conclusion

All of the items mentioned above are undertaken in compliance with well defined, documented processes. And to ensure the highest level of security and performance possible, all Send Word Now activities are held to the same standard of integrity.

All additions and changes performed to the Send Word Now system are reviewed and approved prior to being implemented. Reviews are performed by peers and then approved by management. Additionally, change controls limit human error and ensure that standard Send Word Now practices and procedures are adhered to.

The security posture of the organization is governed by the Send Word Now Information Security Policy. The IS policy document provides the guidelines from which all other processes and procedures are based on. This is a comprehensive document covering a range of topics from user training to device configuration guidelines.

Send Word Now has built a system from the ground up that provides a secure world-class solution for our customers' needs. At Send Word Now, we take security and stability very seriously, and we approach all aspects of our infrastructure and services with this in mind. Whether it concerns the location of our equipment, the method of firewall changes, or our process management, we manage every detail in order to properly safeguard our customers' data on a platform that is flexible, scalable and reliable.