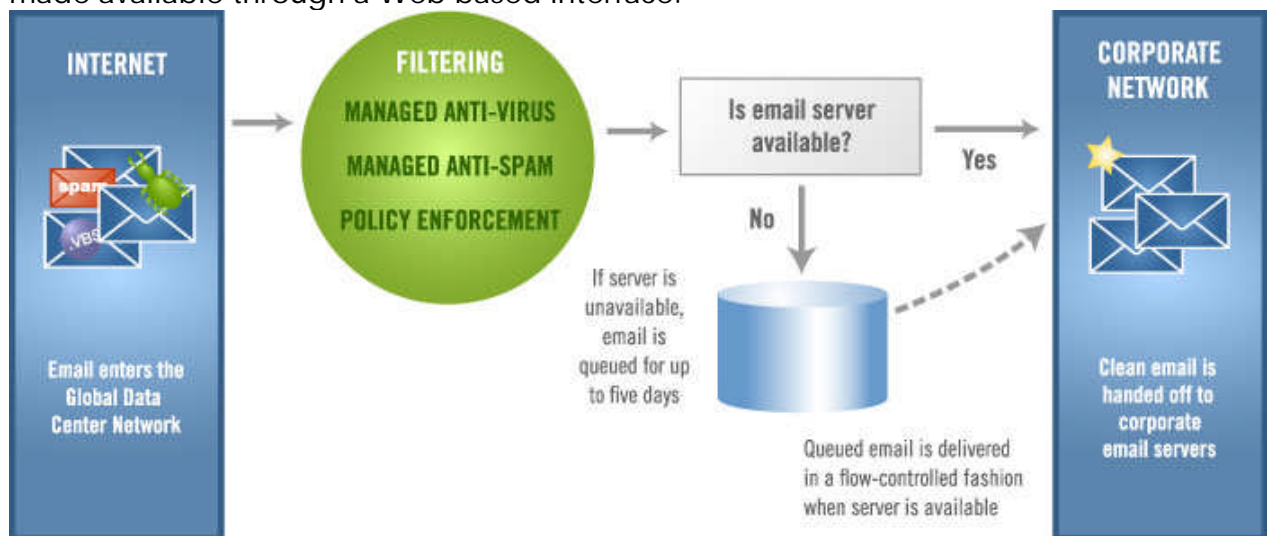


Disaster Recovery/Mail Relay

Enterprises increasingly rely on email as a conduit for exchanging data, contracts, orders, legal documents, and other mission-critical communications. Because companies rely on email to sustain and improve their business, their email infrastructure must offer the highest level of security and reliability. Ensuring the availability of this infrastructure is a sizeable task that presents a real challenge to many IT departments.

Because our network is always available, if our customer's email servers or Internet connection become unavailable for any reason, we ensure no email is lost or bounced. We securely spool and queue inbound email for up to five days. Once the customer's email servers recover, all queued email is automatically forwarded in a "flow-controlled" fashion. In cases of extended downtime, email can be rerouted to another server, or made available through a Web-based interface.



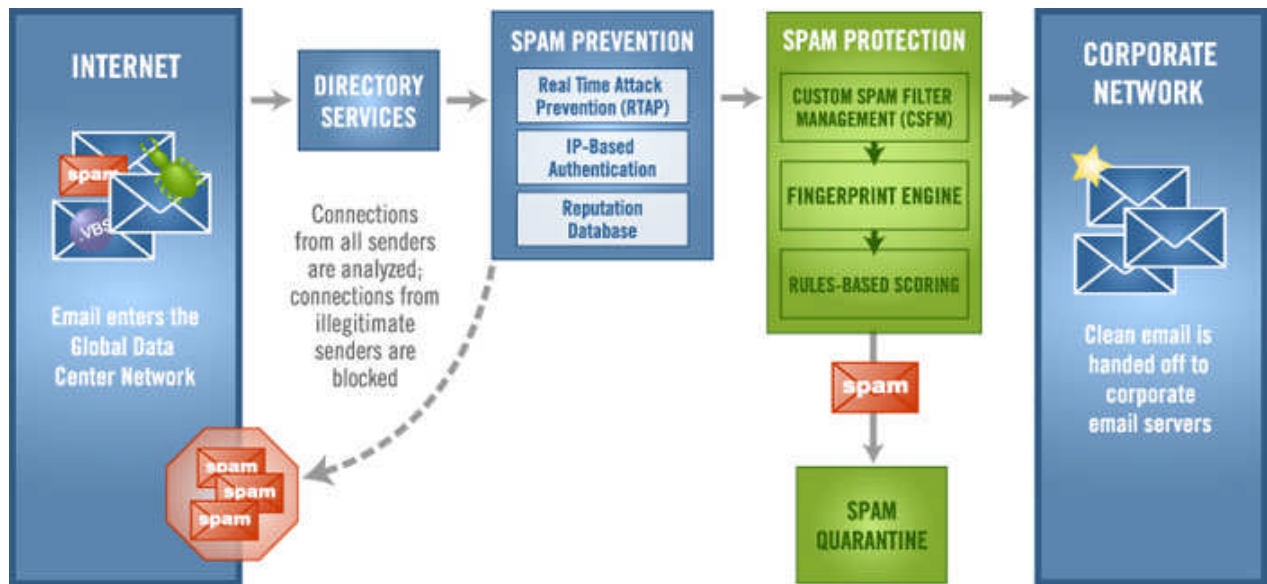
Your privacy is protected. We do not permanently store customer's email at any point during the Disaster Recovery process.

DISASTER RECOVERY/MAIL RELAY BENEFITS

- ◆ No bounced email - Email will not bounce, even if your network and email servers are unavailable.
- ◆ Always on - No need to "flip a switch" to declare disaster mode.
- ◆ High availability and reliability - The advanced architecture of our network ensures that our customers' email will always be delivered. Our network is guaranteed to have 99.999 percent availability, and historically has offered 100 percent uptime.
- ◆ Privacy protected - Customer email is not permanently stored at any time.

Anti-Spam

Anti-Spam is a managed service that deploys multiple layers of technology to protect businesses from receiving unsolicited email. Left unchecked, the scourge of spam can overwhelm businesses, destroying the productivity and benefits of this vital business communication tool. The sheer volume coupled with spammer creativity leaves businesses with no option but to turn to technology to combat this ever-present threat.



HOW IT WORKS

Anti-Spam provides preventative and protective spam defense, keeping spam from reaching corporate email servers. A simple re-redirect of a business' MX record routes all of an organization's messages to a data center in our Global Network, where we process messages using a multi-layered approach.

Spam Prevention

At the edge of the network, we deploy several pieces of technology to prevent spam from entering the network. RTAP, our unique and proprietary email traffic analysis technology, quickly detects, in real-time, anomalies in email traffic in order to block incoming connections from spammers. In addition, we use IP-based authentication, including SPF lookups, to ensure email is coming from a known sender as well as who it claims to be from. Finally, we employ our own reputation database with lists of the most flagrant spammers to prevent unwanted message delivery.

Spam Protection

We use several methods of message analysis to protect corporate networks from spam, including Fingerprinting, Rules-Based Scoring, and Custom Spam Filter Management (CSFM). Our unique fingerprinting technology takes a "digital picture" of each message and matches it against known profiles of spam messages to detect unwanted email and

flag it as spam. In addition, messages are scored against our proprietary database of spam rules, assigning scores to messages based on more than 20,000 unique characteristics of spam and legitimate email. When a message's score reaches a defined threshold, it is flagged as spam. For additional message scrutiny, customers can enable Custom Spam Filter Management (CSFM), providing an additional layer of protection from messages with defined characteristics such as Web bugs and embedded HTML and JavaScript tags.

Spam Handling

Once detected, multiple options are offered for spam handling, including holding spam in the offsite Spam Quarantine for up to 15 days, re-routing spam to a designated mailbox, or flagging spam in the X-header or message subject line. The Spam Quarantine allows email administrators or end users to review quarantined messages to review messages flagged as spam. HTML notification messages can be sent to end users, making Spam Quarantine review simple and effective. The Spam Quarantine and HTML notifications are localized in seven languages.

ANTI-SPAM SERVICE BENEFITS

- ◆ Multiple layers of technology to prevent and protect against unwanted email traffic from reaching corporate networks.
- ◆ Block more than 95 percent of unwanted email, reducing message traffic and improving the efficiency of messaging infrastructure.
- ◆ Delivers the lowest false positive rate of any vendor (1 in 250,000) ensuring delivery of all business email; in addition, the lowest false critical rate (false positive for mission critical message) of any vendor (1 in 1,000,000).
- ◆ "Set it and forget it" philosophy offloads management and maintenance of email protection; No white lists to upload or maintain.
- ◆ The team of spam analysts has broad exposure to millions of messages daily; the team constantly updates spam rules, reputation database, and fingerprint to stay ahead of spammers' ever-changing tactics.
- ◆ Service delivery eliminates the need for capital investment and offloads all maintenance and upgrades to the IT experts.
- ◆ Fully scalable solution matches the size of any enterprise.

Anti-Virus

Anti-Virus is a managed service that protects businesses from receiving email-borne viruses and other malicious code. The widespread acceptance of email as an efficient means of business communication has left corporate networks vulnerable to fast-moving viruses attached to messages as a dangerous payload. Email-borne viruses replicate at lightning speed and can overwhelm even the best equipped IT departments that are tasked with keeping viruses at bay.

Anti-Virus significantly reduces the IT burden by capturing viruses before they enter the corporate network. Using multiple strategies to protect against this malicious code, we are the front line of defense to keep enterprises virus free and assure a clean message stream. In addition to guarding against viruses harbored by inbound email, we also protect businesses in their outbound email communications. A company's reputation is critical, and being the source of a damaging virus that infects the systems of customers, partners and suppliers can do irreparable harm to that reputation.

HOW IT WORKS

Functioning as a pre-emptive anti-virus security service, Anti-Virus works between the Internet and the Corporate Network preventing viruses and malicious code from reaching corporate email servers. Before a message reaches its final destination, it enters the the Global Data Center Network where we process the message using a multipronged strategy to protect against viruses.

Multiple Anti-Virus Engines

At the core of our virus fighting strategy are multiple, commercial-grade anti-virus engines, integrated at the API level. At all times, we use at least two different anti-virus engines with the ability to immediately engage additional engines when acute threats warrant additional coverage.

Leveraging its partnerships with leading anti-virus vendors such as Kaspersky, Sophos and Symantec, we provide timely and critical updates with virus definitions updated every 10 minutes, 24/7. Our anti-virus partnerships provide updates to our network before new virus antidotes are available to the general public.

Outbound Virus and Content Scanning

In addition to scanning inbound email, our service protects outbound communications from propagating viruses and deviant code. Our service intercepts outbound messages, scanning and cleaning messages before they are delivered to intended recipients, to ensure all outbound email is reliable, secure and of the utmost integrity.

ANTI-VIRUS BENEFITS

- ◆ "Set it and forget it" offloads management and maintenance of email protection; no anti-virus engines to update.



SlingStone Information Technology

TOTAL E-mail Protection Service White Paper



- ◆ Prevents viruses from reaching the corporate network via email.
- ◆ Multiple anti-virus engines ensure complete, up-to-date coverage against known viruses and the broadest coverage available; engines integrated at the API level for early and quick updates from vendors.
- ◆ Technology partnerships with anti-virus vendors ensure rapid anti-virus definition updates, often before definitions are publicly available.
- ◆ Reduces virus risk without affecting productivity; grouping allows an organization to eliminate risk for 98% of its users.
- ◆ Multi-pronged strategy at a significantly lower cost than most companies would pay to purchase, deploy and manage their own multi-engine solution.

Policy Enforcement/Content Filtering

As email has become the dominant business communication tool, many rules and regulations have been created to govern email content and usage. Specific laws govern email communications in several industries including financial services and healthcare. The Gramm-Leach-Bliley Act, SEC Rule 17a-4, NASD Rules 3010 and 3110, and the Health Insurance Portability and Accountability Act (HIPAA) all contain provisions for maintaining security, privacy and non-disclosure in email communications. Even when there is no regulatory concern, policy enforcement of inbound and outbound communication makes good business sense, as a corporation's most important asset is its intellectual property.

As part of our integrated approach to message security, customers use our Policy Enforcement service to automatically monitor outbound and inbound email, stopping sensitive and inappropriate messages from leaving and entering the corporate network. This service allows Administrators to define custom policy rules that flag messages for one or more of the following attributes:

- ◆ Words and phrases in the subject and body
- ◆ Message size
- ◆ Attachment types
- ◆ Sender and recipient addresses

Administrators define and edit attribute and policy rules using an easy-to-use, Web-based Rule Writer in the Admin Center, where they specify the type of rule and message rule parameters. They can also indicate when a rule is to expire, if at all.

Policy Enforcement can also be an important and effective weapon against viruses by filtering specific kinds of attachments and email based on known virus characteristics. For example, by allowing select access to executable content by small user populations, a company can eliminate risk for 98 percent of its users.

Message Handling

Administrators have multiple options for handling email that is flagged by a policy rule. Should a message be flagged by a rule, options for handling that message include:

- ◆ Reject or Allow message
- ◆ Quarantine message for review
- ◆ Redirect message to an alternate recipient or mailbox
- ◆ Deliver message with BCC
- ◆ Encrypt message (requires Secure Email service)

Once policy rules have been put into effect, rejected email is returned to the sender and tallied in the Rejection Report. If Administrators choose to quarantine messages for review, we provide the option to let either users or Administrators review and release quarantined items at their discretion. Further, Administrators can use the Admin Center Policy Rule Writer to set up separate custom bounce messages for the sender, recipient, and Administrator.



SlingStone Information Technology

TOTAL E-mail Protection Service White Paper



POLICY ENFORCEMENT BENEFITS

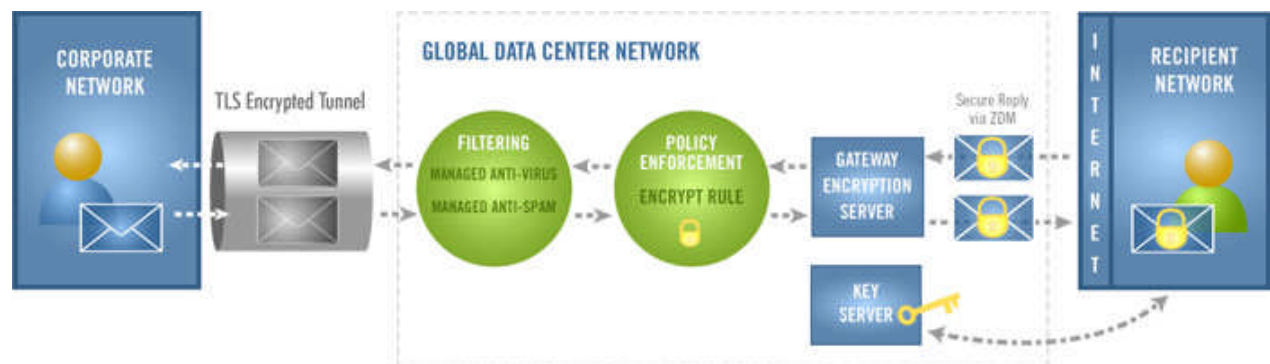
- ◆ Policy adherence - Ensures compliance with written corporate policies regarding sensitive information.
- ◆ Regulatory compliance - Outbound policy enforcement helps companies comply with specific laws and regulations such as HIPAA and The Gramm-Leach-Bliley Act.
- ◆ Content control - Allow companies to monitor and enforce what type of content is appropriate.
- ◆ Liability reduction - Corporate liability is reduced as policy filters help guard against the distribution of information that can result in legal liability.

Optional: Secure E-mail

Secure Email is a convenient, easy-to-use email encryption service that safely delivers your confidential business communications. Experts estimate that 75% of the total knowledge exchange occurring via email contains proprietary, intellectual property, and must be protected as a valuable corporate asset. But the need for increased confidentiality is only one of the many reasons corporations must add protection to existing email communications. Government and industry regulations, such as those posed by HIPAA and Gramm-Leach-Bliley, offer even more compelling reasons for corporations to secure messages.

However, existing solutions - such as server-to-server level encryption, public key infrastructure (PKI), and password-protected files - are not only ineffective, but expensive and complicated to integrate and to deploy. These solutions do not provide the flexibility, sophistication and ease-of-use that corporate users need to deploy email encryption throughout their enterprise.

Secure Email enables users to send and receive encrypted email directly from their desktops as easily as regular email, to anyone at any time. With a single click, users can encrypt and deliver any business communication without complex hardware and software to purchase, configure and maintain. Leveraging multiple types and layers of encryption, including transport layer security and gateway encryption, our highly scalable solution meets industry standard protocols, and has been validated by industry and government experts.



SECURE EMAIL FEATURES & BENEFITS

- ◆ Encrypted email delivered directly to recipients' inbox and not to a Web service.
- ◆ Zero Download Manager (ZDM) enables secure, Web-based decryption and encrypted replies for any recipient without pre-shared keys or pre-installed software.
- ◆ Managed key server eliminates the need for certificate maintenance.
- ◆ Communication via TLS-enabled network further ensures messages stay secure.
- ◆ Send encrypted emails to anyone, regardless of their system configuration.
- ◆ Decrypt and read emails securely, without installing client software.
- ◆ Strong, automated encryption with a cost-effective infrastructure.



SlingStone Information Technology

TOTAL E-mail Protection Service White Paper

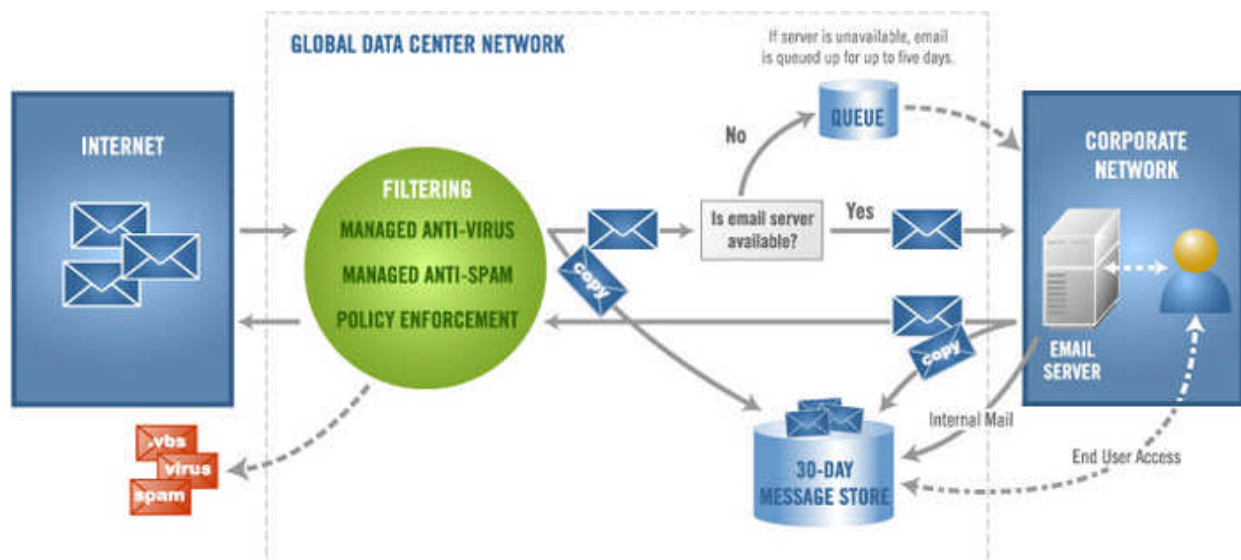


- ◆ Protect sensitive information and data leaving your email gateway, consistently and automatically.
- ◆ Comply with security and privacy requirements such as HIPAA and Gramm-Leach-Bliley.
- ◆ No hassling with key and certificate management, or searching for easy and secure ways to obtain long strings of alphanumeric digits from the people with whom you need to communicate.
- ◆ Generate keys on the fly.
- ◆ Eliminate the need for capital investment, and offload maintenance and upgrades to IT experts.

Optional: Message Continuity (MC)

Email has evolved from a simple communication tool into a mission critical application that supports all aspects of business. Doing without access to email is not an option, and losing critical information exchanged via email transactions can be disastrous.

Our Message Continuity (MC) ensures that enterprises always have access to email and never lose critical information. MC is an always-on, email continuity and disaster recovery service that protects and guarantees access to email for a business and its employees. As part of our Message Continuity Services, MC protects an enterprise's most critical and valuable communications tool and ensures continual access to email functionality - including reading, composing and replying to messages - even during disaster and emergency situations. MC intercepts and makes copies of inbound, outbound, and internal email and stores those message copies in a 30-day rolling message store. The message store can be accessed 24/7 by email administrators and end users to recover messages that may have been lost or deleted from an enterprise's primary email environment.



MC's Web-based interface includes email tools for composing, reading, and replying to email, ensuring continual access to all email functionality even when the primary email environment is unavailable or a backup email system is needed. Any messages sent via the Web-based tools can be automatically merged into the primary mail system to complete disaster recovery operations.

Finally, if the primary mail environment is down or a business' network is unavailable, preventing normal delivery of email, MC continues to copy messages to the message store and queues the original message for delivery once the primary email environment is restored.



SlingStone Information Technology

TOTAL E-mail Protection Service White Paper



MC BENEFITS

- ◆ Always-on - No need to "flip a switch" to declare disaster mode.
- ◆ Interception-based archiving - Captures messages in transit and works in concert with our Message Security Services to ensure spam, viruses, and other unwanted content are kept out.
- ◆ Easy-to-use Web-based tools - Requires minimal training and allows access to the message store for end users from any location.
- ◆ Continuous access - Even when the primary email system is unavailable.
- ◆ Searchable message store - Easy recovery and restoration of individual and groups of messages.
- ◆ Service delivery - Eliminates the need for capital investment and offloads maintenance and upgrades.

Optional: Message Archive

With electronic messaging as a core component of corporate operations, retaining and having ready access to historical messages is a high priority. When disaster strikes your email infrastructure, interruption to email access can be costly and even pose unique legal liabilities if emails are lost. Regulations such as SEC Rule 17a-4, NASD 3010, Sarbanes-Oxley, and HIPAA impose a variety of message retention and supervisory requirements on businesses. Those regulations plus the potential burden of legal discovery require enterprises to create email and IM retention policies that mitigate risk and meet regulatory compliance standards.

HOW IT WORKS

Message Archive helps enterprises not only preserve the productivity and benefits of electronic communication, but it also complies with the regulatory and legal demands placed upon businesses and their communication systems. The service intercepts and makes copies of inbound, outbound, and internal email, as well as IM and other communications, such as Bloomberg mail, and stores those message copies in a secure, tamperproof archive. Comprehensive message indexing allows users to search stored messages by header, subject line, and body contents, including attachments. If a business' primary mail environment is down, Message Archive continues to copy messages to the archive and queues the original message for delivery once the primary email environment is restored.

The archive can be accessed by email administrators and end users 24/7 whether or not the primary email environment is available. Users access stored messages through an intuitive, Web-based interface. It even provides compliance workflow tools for supervising and monitoring electronic communications.

MESSAGE ARCHIVE BENEFITS

- ◆ Managed service convenience - Complete message archiving is available for the entire enterprise with the lowest total cost of ownership (TCO).
- ◆ Search, retrieve, restore, extract - All messages are fully text-indexed and searchable. Lost messages can be retrieved, restored or extracted.
- ◆ Intuitive web-based user interface - All aspects of the system from end-user to administration is done via a rich, easy-to-use Web interface.
- ◆ Enable email continuity - In the event of primary email system failure, you continue to receive email through Message Archive. Email communication is uninterrupted.
- ◆ Simplified deployment - No additional hardware or software is required, interaction with the archive is done via a Web browser; service is quickly deployed in a few easy steps.
- ◆ Regulatory compliance - All services delivered in compliance with SEC Rule 17a-4, NASD Rules 3010 and 3110, also addresses issues posed by Sarbanes-Oxley, HIPAA, FSA, and other rules regarding communication filtering and retention.
- ◆ Always-on - No need to "flip a switch" to declare disaster mode.