

Mail2World Email FailSafe Service

always there, always safe

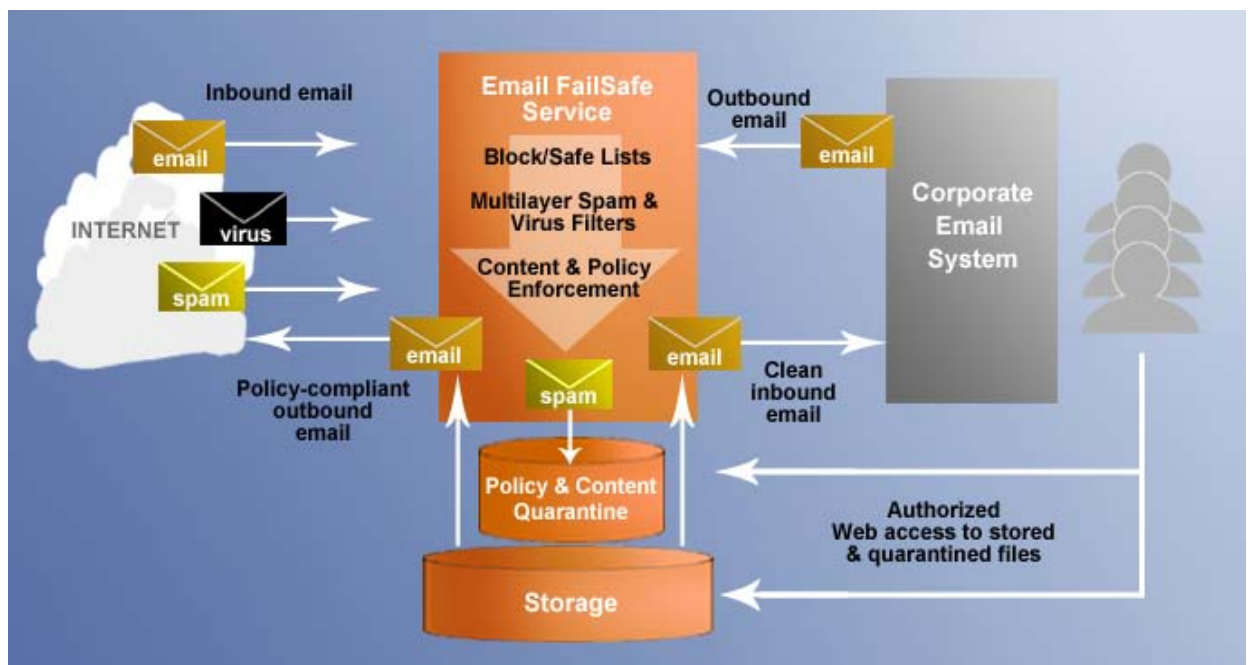
Email is a mission-critical application. Enterprises have found that even a few minutes of email downtime or a single lost message is unacceptable. Yet the reliability and viability of email as the primary conduit for exchanging vital business information is constantly challenged.

Today, companies face an increasing challenge from spam and viruses with a requirement for email to be accessible at all times. In addition, corporations sharing ideas and information as part of a global economy face constant threats of legal liability for communicating that same information via email. For these reasons, it is critical for organizations to have an always on, multipurpose solution that can enforce, control and manage these threats and constant challenges.



Through a sophisticated set of applications, rules and filters operating on a network of custom-engineered servers, Mail2World's Email FailSafe Service simultaneously performs three essential services.

Email FailSafe Service is a global, hosted solution that augments your existing email infrastructure through a seamless interface with Microsoft® Exchange™, Lotus Notes™ or any other email system. The result is comprehensive spam and virus protection with a reliable, affordable alternative to either a costly parallel messaging infrastructure or additional onsite storage servers.



Mail2World Email FailSafe Spam & Virus Protection

always there, always safe

M2W Email FailSafe

Email FailSafe Service

Spam & Virus Protection

The most comprehensive perimeter protection available against spam, viruses and denial-of-service attacks.

Policy Enforcement

Allows you to maintain policy control and management oversight through a single point of control.

Disaster Recovery

Delivers email availability during natural or man-made disasters, power outages, system glitches and virus attacks.

Comprehensive email protection is delivered through a solid perimeter defense; world-class, predictive anti-virus filters; multilayered email filtering; and customizable Sieve scripting. In addition to securing emails coming in, going out and residing on your network, Email FailSafe Service protects information from being compromised during the transmission process from sender to receiver.

Feature & Benefit Highlights

Inbound & Outbound Mail Process Flows

Inbound Mail

As inbound messages flow into the Email FailSafe Service system, they pass through a series of powerful spam, virus and content filters. Clean inbound email is immediately sent on to corporate mail servers, and a copy is stored in our Email FailSafe Service data center. Viruses are sent to trash. Spam is stored in a user-accessible quarantine server.

Outbound Mail

Outbound emails sent by corporate users are filtered for viruses, copied to our Email FailSafe Service archiving servers and instantly delivered to recipients via the Internet.

- > **Pre-Protection Filtering:** Email FailSafe Service's first layer of defense includes a protocol filter, SMTP security, reverse DNS lookup, block scan attack, real-time blacklists, connection limits, mail relay and block connections.
- > **Industry-Leading Virus Protection:** Email FailSafe Service anti-virus protection is powered by Norman Data Defense, an award-winning developer of tools for the detection and removal of viruses.
- > **Sequential Content Analyzer:** This filter automatically refreshes itself as often as every 15 minutes, allowing Email FailSafe Service to easily identify and block the latest forms of disguised spam and malware as well as forecast and prevent new attacks.
- > **Impenetrable Channel Encryption:** Before an email is sent, Email FailSafe Service queries the receiving mail server to confirm support for encryption. Fully encrypted channels ensure that emails are sent via an impenetrable connection to the intended recipients, so email content is invulnerable to unauthorized access during transmission.
- > **Flexible Access Parameters:** Management is an integral part of Mail2World's holistic approach to protecting and enhancing the value of your email communications. Email FailSafe Service includes customizable controls that include domain-level quarantine access for users and administrators through a Web interface.

Mail2World Email FailSafe Policy Enforcement

always there, always safe

M2W Email FailSafe

Email FailSafe Service

Spam & Virus Protection

The most comprehensive perimeter protection available against spam, viruses and denial-of-service attacks.

Policy Enforcement

Allows you to maintain policy control and management oversight through a single point of control.

Disaster Recovery

Delivers email availability during natural or man-made disasters, power outages, system glitches and virus attacks.

Content Policy Filters: Outbound emails sent by corporate users pass through a set of customizable content filters that are controlled by policy managers from an easy-to-use Web control panel. When the content filters detect a suspicious outgoing message or attachment, those items are immediately delivered to a quarantine server, where policy managers may inspect them more closely for policy violations.

Web-based Message Monitoring & Retrieval: Any authorized user wishing to monitor or retrieve archived or quarantined messages may simply login to the password-protected Email FailSafe Web interface. Messages can be quickly and easily searched by Subject, Date, From, To, Cc, Message Size, Attachment and Priority. Users may also conduct a full text search of the Message Body and popular attachment formats, including Word, Excel, Powerpoint and Adobe PDF.

Feature & Benefit Highlights

Performance Reliability

- > 100 percent historic uptime over 5 years
- > 99.995 percent service-level availability
- > Lightweight POPs in multiple data centers globally crossing network boundaries
- > Individual POPs act as a distributed, load-balanced application via redundant top-tier registry services; each POP is a self-sustaining, NS/DNS registry.
- > Global redundancy provided by root NS/DNS round-robin to all data centers.
- > Each POP installation consists of multiple, independent gateway servers.

- > Sophisticated, customizable rules allow you to set message characteristics, including words and phrases in the subject line, message size, sender and recipient addresses, specific domains and attachments.
- > Full block list and safe list features give users and administrators domain-level control.
- > Forbidden attachment feature fingerprints offensive attachments.
- > Powerful, multilayered spam and virus filters detect and quarantine unwanted messages.
- > Message quarantine server with user and administrator access allows easy inspection of suspicious messages.
- > External message archive safely stores all inbound and outbound email for seven (7) days to guarantee no message is lost and assist with regulatory and legal compliance.
- > Online access to quarantined and archived messages allows you to quickly sort messages, locate specific messages through advanced search tools and delete or redirect any confidential company information.

Mail2World Email FailSafe Disaster Recovery

always there, always safe

M2W Email FailSafe

Email FailSafe Service

Spam & Virus Protection

The most comprehensive perimeter protection available against spam, viruses and denial-of-service attacks.

Policy Enforcement

Allows you to maintain policy control and management oversight through a single point of control.

Disaster Recovery

Delivers email availability during natural or man-made disasters, power outages, system glitches and virus attacks.

Mail2World's Email FailSafe Disaster Recovery
is an affordable, always-on, hosted backup solution that guarantees your company will never again experience email downtime or lost messages.

Threats to your email infrastructure can hit anytime from many directions: power outages, system glitches, virus attacks and natural or man-made disasters. Since the cost of downtime from any one of these threats can be millions of dollars in lost revenue and productivity, companies must find a way to deliver uninterrupted, fully operational email service.

The architecture of Email FailSafe Service is functionally equivalent to, but structurally different from, Microsoft® Exchange™, Lotus Notes™ and other email systems. That's why Email FailSafe is impervious to the cause of your system's failure, serving as an ever-present, invisible shield against the often devastating effects of system crashes. The result is uninterrupted, fully operational email service to your users from the moment your existing system fails.

Feature & Benefit Highlights

Email Outage Risk Statistics

Industry studies reveal some startling numbers about the risk of email downtime.

- > Seventy-five percent of companies will experience a major email outage annually. Another 14 percent will experience a major planned outage due to testing or upgrades.
- > Email outages last an average of more than 30 hours.
- > The amount of business-critical data stored in email is as high as 60 percent. (Source: Gartner)
- > A recent Osterman Research survey found that when email is down, 60 percent of employees use personal accounts for business transactions, increasing the company's risk of legal liability.

- > Guaranteed 24/7/365 off-site redundancy means zero downtime for users and customers during any cause of system failure.
- > Incoming emails are never rejected, so customers and vendors are unaware of your system outage.
- > Storage servers retain all incoming messages received during downtime, so no communications are lost.
- > Full-featured Web email interface lets users retrieve, write and send messages while your in-house system is down.
- > Queued messages are immediately restored to your system when it's back online, eliminating 4- to 48-hour delays or retries.
- > "Pause button" holds messages during scheduled downtime for system maintenance without incurring email rejections.
- > System monitoring, reporting and 24/7 technical support ensure email continuity.