



DMZMessaging

Comprehensive email security.
Designed to protect your mail systems from security threats.



Using industry-leading tools to protect against spam, virus, spyware and fraud attacks, DMZMessaging filters malicious content before it reaches your systems.

The DMZMessaging solution provides industry leading, secure, policy-based mail management. Protecting your systems by removing spam and malicious software before it reaches your network. DMZMessaging eliminates the requirement for on-site infrastructure, decreasing bandwidth requirements and reducing costs.

Service options

DMZGlobal provides a number of highly configurable versions of DMZMessaging to address your requirements:

Standard

This solution eliminates significant amounts of spam and includes reputation filtering, black listing and multiple anti-virus engines (this solution is currently only available as part of the DMZInternet service).

Advanced

The full mail security solution including additional virus scanners, security mechanisms and the world's leading anti-spam solution.

Policy

This includes all the features of the advanced version with the added ability to manage mail content including profanity filtering and apply policies with associated actions.

Compliance

This version is focused on meeting business requirements around independent management, storage and retrieval of mail to meet corporate policy, legal and compliance needs including PCI.

Encryption

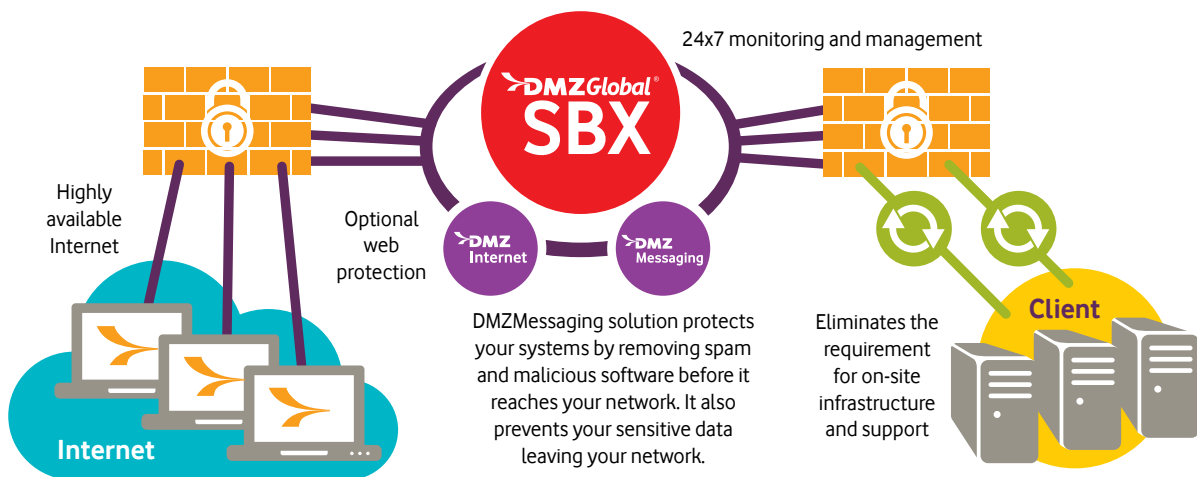
Industry leading encryption technology including SEEMail and PKE support.

Continued over...

Key attributes

The key attributes of DMZMessaging include:

- **Data loss prevention:** DMZMessaging monitors outgoing traffic to enforce your security policy on data types and specific files, ensuring protected information does not leave your organisation via email
- **Reputation filtering:** By utilising the IronPort SenderBase Network, the world's most accurate reputation system, DMZMessaging blocks and filters email from known trouble sources
- **Flexibility:** DMZMessaging has a wide range of configurable options that provide tailored solutions
- **Spam filtering:** DMZMessaging utilises 17 different filtering technologies including IronPort Anti Spam (IPAS) to maximise detection (over 95%) and minimise false positives (99.9999% accuracy rate). The spam filters are updated every five to ten minutes for rapid response to new spam threats
- **Multiple virus/malware engines:** DMZMessaging utilises multiple virus engines when inspecting messages, including solutions from Clam, Trend Micro, McAfee and Sophos. At any given time, at least three engines are used to scan messages
- **Malicious attachment protection and image classification:** DMZMessaging allows you to strip and/or quarantine all suspect attachment types known to carry malicious material and filter images for their content
- **Zero day protection:** DMZMessaging utilises IronPort's Virus Outbreak Filters (VOF's) to assist with protection from day-zero attacks (when malware is spreading but virus patterns are not yet available)
- **Availability protection:** With relay protection, recipient verification, directory harvest attack protection and spam backscatter protection using Bounce Address Tag Verification (BATV)
- **Client white lists and black lists:** Allows you to maintain unique safe lists and block lists in order to allow mail to be passed by spam and MAP controls for specific senders and receivers
- **Message digests & quarantine tool:** DMZMessaging provides an optional digest facility to notify users of quarantined emails, while the quarantine tool allows administrators to control the release of email
- **Best practice enforcement:** DMZMessaging checks for bad practice such as relaying and address spoofing for outbound as well as incoming messages



Benefits

The DMZMessaging service delivers leading edge email security protection that provides:

Reduced costs

- A reduction in costs associated with a dedicated email security infrastructure
- Reduced bandwidth as unwanted email is removed before it traverses the client's internet connection
- The impact of spam on email gateways, mail stores and mailbox virus scanning systems is vastly reduced

Increased productivity

- Ensuring clients are not black listed as a sender
- Reducing the manual effort associated with users and IT staff managing spam

- Eliminating downtime due to virus outbreaks
- Allowing users or administrators to self-release mail

Improved security

- DMZMessaging's multi-layered solution provides defence against spam, viruses, malware and spyware. Using multiple best-of-breed products to maximise protection, DMZMessaging allows you to benefit from a carrier grade infrastructure that would typically be too complex or costly to implement and maintain in-house

High availability and "Disaster Recovery"

- DMZMessaging is virtualised and load-balanced across DMZGlobal's geographically diverse points of presence. In the event of your email infrastructure being unavailable, DMZMessaging will either queue your email until service is restored or redirect the mail to an alternative mail server

Why DMZGlobal?

DMZGlobal Security Solutions from Vodafone provide your business with:

- Trusted 24x7 protection for your organisation including network infrastructure, applications, confidential data, users and ultimately, your reputation
- Experienced security services professionals and one of New Zealand's largest dedicated IT security teams
- A cost effective 'in cloud' alternative to significant in-house capital investment with true scalability and flexibility
- Industry leading solutions built on strength-in-depth design, best practice process and best-of-breed technology
- DMZGlobal services future-proof your business, with continual development to stay ahead of emerging security threats, as well as meet regulatory standards and compliance requirements.

How to contact us

New Zealand

0508 400 300

Email

info@dmzglobal.com

www.dmzglobal.com

All brands and products referenced in this document are acknowledged to be trademarks or registered trademarks of their respective owners.

