

## The Anti Spam Solution for your Business

### SpamTitan

SpamTitan is a complete solution to email security offering protection from Spam, Viruses, Trojans, Phishing and unwanted content.



### Feature Set

- ✓ Two Anti Virus engines including ClamAV and Kaspersky Labs
- ✓ Multi layered Anti Spam analyses resulting in 98% plus Spam detection
- ✓ Less than 0.03% False Positive Rate
- ✓ Content Filtering
- ✓ Inward and outward email scanning
- ✓ Email Disclaimer capability
- ✓ Simple download and installation process
- ✓ Plug and Play Solution
- ✓ End user Spam management using email quarantine reports
- ✓ Web based administrative GUI
- ✓ Multiple automated reports
- ✓ Automated updating including anti virus, anti spam, version releases and system backup
- ✓ LDAP, Dynamic and aliases file recipient verification

SpamTitan is available in two flavours, **SpamTitan ISO** and **SpamTitan for VMware®**, both of which can be downloaded and installed for free.

### Which is for me?

**SpamTitan ISO** and **SpamTitan for VMware®** have identical functionality, operating systems and support costs. Both can be downloaded, installed and configured quickly and simply. Which you choose to install is entirely dependant on your own requirements.

**SpamTitan ISO** is a complete operating system and software suite image. When installed on a PC or server, it will clear any existing operating system, replacing it with its own and the SpamTitan software suite resulting in a dedicated SpamTitan email appliance for your gateway.

**SpamTitan for VMware®** is a complete operating system and software suite designed to run on VMware®. This will enable you to run SpamTitan on any server running VMware® irrespective of the operating system, allowing you to run multiple applications on a single server. For more information and to download a copy of VMware® see: [www.vmware.com/appliance](http://www.vmware.com/appliance)



The Anti Spam Solution for your Business

SpamTitan VMware® – Technical Specifications

SpamTitan provides feature rich functionality to allow you manage and protect your email. Below are details as well as technical information to allow you to download and install SpamTitan.

|   |   |
|---|---|
| <b>Double Anti Virus Protection</b>                     | SpamTitan includes both the award winning ClamAV and Kaspersky Labs Antivirus engines offering double scanning of all incoming and outgoing email. Both anti virus engines are auto updating thus ensuring the least management and utmost protection.  |
| <b>Multi Layered Spam Analyses</b>                      | To ensure the highest continuous levels of spam accuracy SpamTitan uses a comprehensive layered approach to separate genuine email from spam. These include Sender Policy Framework, Recipient verification, SURBL's, RBL's Bayesian analyses, keyword, header and body text analyses, customised scoring algorithms as well as many other customised rules. These combine to give email an over all score which defines it as spam or not. |
| <b>Content filtering</b>                                | SpamTitan can block unwanted attachments including file types, mime types and renamed files. This can be enabled at both the domain and user level allowing administrators to block unwanted content in line with the organisations email policy.   |
| <b>End User Spam Management</b>                         | SpamTitan allows you to push the daily management of spam to the end user. Using the spam digest feature end users have full visibility of all email blocked by SpamTitan. Using hyperlinks included in the digest, from their inbox the end user has the ability to release any required email without having to resort to the company helpdesk.   |
| <b>Full Reporting Suite</b>                             | SpamTitan contains a comprehensive reporting suite providing automated graphical reports including top spam recipients, top email recipients and many more. There is also a "live report" of all email as it passes through SpamTitan with full search capabilities.  |
| <b>Outbound disclaimers</b>                             | In line with your email policy framework disclaimers can be attached to outgoing email. You decide the text of this disclaimer.   |
| <b>Multiple Domains Supported</b>                       | SpamTitan can be configured to accept email for an unlimited amount of domains which in turn can be relayed to an unlimited amount of email servers.  |
| <b>Configurable on both a domain and user level</b>     | All rules can be set at both the domain and user level. This allows detailed configuration for all requirements across the business.  |
| <b>Fully Automated updating, backup and reporting</b>   | All updates, including anti virus, anti spam, new version releases, configuration back up, Bayesian back up and management reports are automated, thus requiring the minimal management overhead possible.  |
| <b>Whitelists and Blacklists</b>                        | Whitelists and blacklists can be configured for the user or at a domain level and to allow/block by full email address or by domain   |
| <b>Administrator and end user Quarantine management</b> | SpamTitan provides both the administrator and end user with a search and retrieval functionality for their email quarantine management.   |
| <b>Full Diagnostics Reporting</b>                       | SpamTitan contains a comprehensive suite of diagnostic tests and reports providing both the administrator and SpamTitan support with all the information required to fully investigate any support issues. This includes the ability to send a canned diagnostic report to SpamTitan support and remote ssh authenticated log on from SpamTitan support   |
| <b>Web Bases GUI</b>                                    | All SpamTitan features are accessed using an intuitive web based interface. This allows controlled access from the network and removes the need for client based management software. Restrictions can also be put in place to limit who and where this interface can be accessed from.   |

Operating System

SpamTitan for VMware® is specifically designed to run on VMware®. The download contains both the SpamTitan application and its own operating system, a hardened Linux platform, including scripts for self installation. There is no operating system requirement. You will require a copy of VMware® running on your server or workstation. SpamTitan for VMware has been tested on the following versions:

- VMware ESX Server®
- VMware Workstation®
- VMware Server®
- VMware Player®

Minimum Hardware Requirements

| <1000 Users   | <2000 Users   | <5000 Users   | >5000 Users   | >20,000 Users                            |
|---|---|---|---|--|
| Intel Pentium® 4 (or equivalent)<br>2.5Ghz Processor<br>512MB RAM, 40 GB Disk,<br>1 Ethernet Port | Intel Pentium® 4 (or equivalent)<br>2.5Ghz Processor<br>512MB RAM, 80 GB Disk,<br>1 Ethernet Port | Intel Pentium® 4 (or equivalent)<br>3Ghz Processor<br>512MB RAM, 80 GB Disk,<br>1 Ethernet Port | Intel Pentium® 4 (or equivalent)<br>3Ghz Processor<br>1GB RAM,80 GB Disk,<br>2 Ethernet Ports | Please Contact<br>helpdesk@spamtitan.com |