

Test Report November 2007

SpamTitan for
VMware,
Version 4.09

Anti-Spam Technology Report

SpamTitan for VMware, Version 4.09

Vendor Details

Name: Copperfasten Technologies

Address: Storm House, Galway Business Park,
Dangan, Galway, Ireland

Telephone: +353 91 540054

Website: www.spamtitan.com

Product: SpamTitan for VMware, Version 4.09

Test Laboratory Details

Name: West Coast Labs, Unit 9 Oak Tree Court, Mulberry Drive
Cardiff Gate Business Park, Cardiff, CF23 8RS, UK

Telephone: +44 (0) 29 2054 8400

Date: November 2007

Issue: 1.0

Author: Rob Tanner

Contact Point

Contact name: Rob Tanner

Contact telephone number: +44 (0) 29 2054 8400

SpamTitan for VMware, Version 4.09

Contents

Introduction	4
Test Network	6
Test Methodology	7
Product Test Reporting	8
Checkmark Certification	9
The Product	10
Test Report	11
Test Results	15
West Coast Labs Conclusion	16
Security Features Buyers Guide	17

SpamTitan for VMware, Version 4.09

Introduction

The ever evolving spam threat

“Two years from now, spam will be solved.” Bill Gates – Jan. 2004

At the beginning of 2004, Bill Gates was addressing the World Economic Forum in Switzerland and confidently predicted that “Two years from now, spam will be solved.” Sadly his prophecy has proved somewhat wide of the mark as reports continue to emerge about the size of the problem.

The latter half of 2006 saw an unprecedented rise in spam volumes with SurfControl reporting a 50% increase in spam over the previous half year, and spam now accounting for almost 90% of all email traffic on the Internet.

The nature of spam has also changed. In 2004 spam content was dominated by pornography, Viagra sales and the infamous “Nigerian scam” advance-fee fraud spam. Those types of spam are very much still with us but have been added to by phishing attacks, “Pump-and-Dump” scams (which involve artificially inflating the price of a stock in order to make a quick profit on stock previously purchased cheaply) and spam that tricks users into following URL links to web sites that download malicious code that will compromise their machines.

The methods used by spammers to launch their attacks have also transformed over time. The vast majority of unsolicited email is now being sent via vast armies of infected PCs known as botnets – often these are the machines of home users who are unaware that they are part of the problem.

This distributed system approach is making it more difficult to separate out spam emails based upon simple network-based criteria, and so companies providing anti-spam technologies are having to provide more intelligent filtering solutions.

SpamTitan for VMware, Version 4.09

In a recent interview, Dr Richard Cullen, distinguished engineer at SurfControl said, "The threat landscape has changed dramatically over the past couple of years. Malware attacks are now commercial ventures, with well organized cybercrime gangs harnessing the power of vast botnet armies to launch spam, phishing, DDOS and malware attacks."

The spammers are also always trying to find new ways of bypassing anti-spam defenses. One such technique that is on the increase is image spam – emails with images containing the spammer's messages within random text designed to foil less sophisticated spam filters. Peter Firstbrook, security research director for Gartner, has reported that image spam went from 6 percent of all spam in Q3 of 2006 to 30 percent by Q4, and it is now thought to make up almost 40% of all spam.

Apart from being harder to block, image spam also causes knock-on problems because the spam messages are actually larger than simple text messages. According to some reports, the average size of a spam message has increased by 77% since September last year, from 6.62Kbytes to 11.76K) and continues steadily to grow. This adds to the cost of managing email, it wastes bandwidth and also consumes storage if a company needs to archive all incoming mail.

And according to the New York Times security columnist John Markoff, one recent botnet outbreak managed to consume 15% of Yahoo's resources while searching for random pieces of text to pad out such image-based messages.

As a result, anti-spam vendors are now having to adapt to this new threat by both enhancing existing techniques such as heuristics rules to analyze the characteristics of image-based spam, and by adding new technology layers, such as optical character recognition technologies. Where will it all end?

SpamTitan for VMware, Version 4.09

Test Network

WCL has a number of domains that collect genuine spam. These domains receive varying levels of spam and are consistent with different email environments.

To reflect the email usage within a corporate environment, within each domain are a number of designated user accounts with a variety of email practices and needs including some that are subscribed to a variety of newsgroups and mailing lists. Some user accounts actively contribute to mailing lists.

The multiple domains designated for testing purposes were those that, between them, receive spam at a level consistent with the defined requirements of testing.

Software solutions included in the test program were installed on servers that meet the minimum specifications required by the vendor. Appliance-based solutions were installed on the network according to the vendor's recommended placing.

For hosted services, WCL tests through identified email domains and changed the MX records to divert the mail stream through the hosted service.

SpamTitan for VMware, Version 4.09

Test Methodology

WCL initially performed the testing with an “out-of-the-box” configuration, changing only those settings on the solution needed to ensure correct operation inline with the vendors recommended installation and configuration procedures.

Further testing was then performed following the vendor's advice for the tuning or training of the solution under test. WCL fine-tuned the solution each day of the test, spending no more than half an hour per day undertaking such work.

Throughout the course of testing, a mixture of email was sent to the test domains from other email addresses and domains controlled by WCL to mirror genuine email activity common in business, for example requesting meetings, sending notifications to groups and non-business related social emails.

Emails were also sent from web-based accounts such as Hotmail and Google's Gmail in order to simulate external users sending non-business related social emails, and home workers.

Thus, during the testing period the domains received some spam, some list/newsgroup mailings and “genuine” individual emails.

SpamTitan for VMware, Version 4.09

Product Test Reporting

Product evaluation addresses three specific areas* - Management/Administration, Functionality, Performance plus Additional Feature Testing.

1. Management/Administration

- Ease of setup/installation
- Ease of use
- Logging and reporting function
- Rule creation
- Customization
- Content categories

2. Functionality

- Email processing steps
- Allow/blocking of email
- Quarantine area
- Additional functionality reporting
- Steps to process email
- Block email addresses
- Blacklist/whitelist
- Allow email addresses

3. Performance

- Volume or percentage of spam detected
- False positive rate
- Spam incorrectly passed through
- Legitimate mail blocked
- Legitimate subscription mail blocked

SpamTitan for VMware, Version 4.09

Checkmark Certification

Upon completion of the testing, individual product results are analyzed, resulting in accreditation to one of the two Checkmark Certifications for Anti-Spam subject to achieving the following catch rates:-

- Checkmark Anti-Spam Certification
Premium – 97% and over Catch Rate
- Checkmark Anti-Spam Certification
Standard – 90% and over Catch Rate



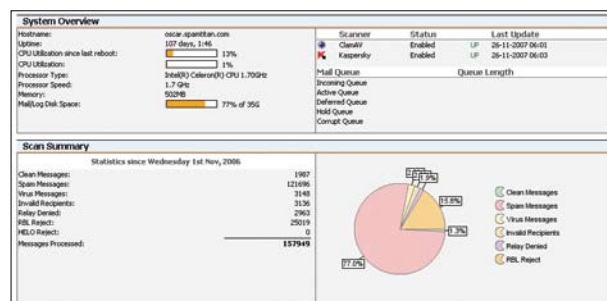
SpamTitan for VMware, Version 4.09

The Product

Introduction

The SpamTitan solution provides end-user organizations with the ability to implement a dedicated email protection solution, as it acts as a multi-purpose email traffic filter between the internet and an internal email server. The solution provides protection from undesirable email-based content, including malware and spam-centric threats, and it is deployed with automatically updated engines as standard, ensuring a low maintenance overhead to deliver potential cost savings.

It is available as either an ISO image or a VMware certified virtual appliance, with both options available via an internet download. West Coast Labs implemented the VMware option for testing the solution, with the prime objective of assessing the anti-spam functionality against the Checkmark Anti-Spam Certification.



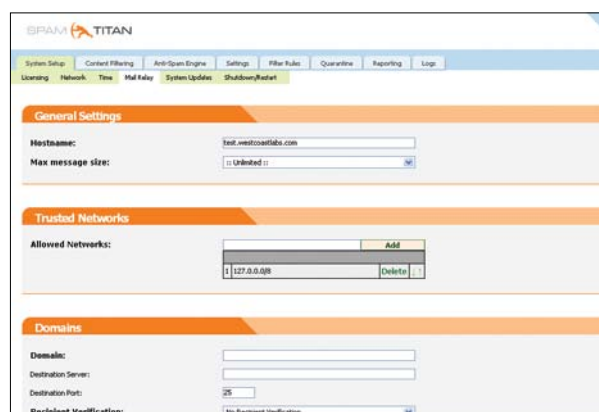
SpamTitan for VMware, Version 4.09

Installation and Configuration

West Coast Labs downloaded and installed the virtual appliance to a relatively low specification computer running VMware Workstation. Upon completion of the virtual machine boot sequence, a simple installation wizard is invoked to guide the end-user through the remainder of the configuration process; the server IP address and domain names are examples of the information entered during the initial installation phase.

By deploying the technology as a VMware virtual appliance – as opposed to a physical appliance or a traditional software based solution – West Coast Labs benefited from improved ease of use in the evaluation and testing process, while also noting real advantages to business users, in terms of potential redundancy, backup, scalability, and mobility gains.

The solution was subsequently configured to forward received email from a live internet domain feed – incorporating spam, ham (genuine), and gray email – to an internal email server. This task was carried out using a web browser to access the management console and enter the corresponding IP address of the internal email server.

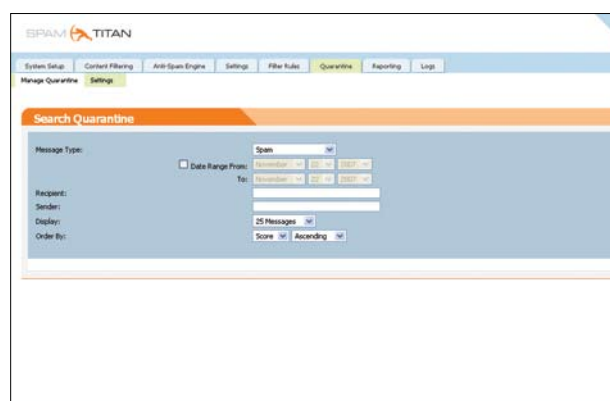


SpamTitan for VMware, Version 4.09

Operations and Features

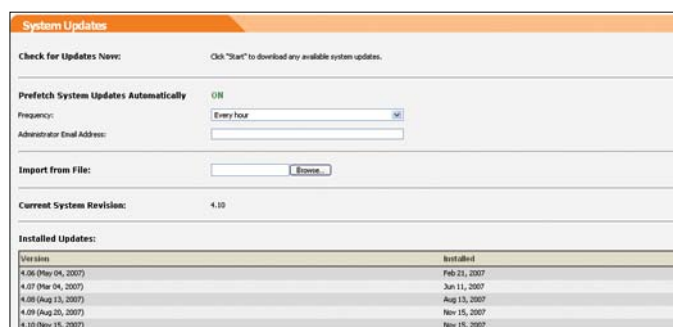
West Coast Labs identified and confirmed key operational functionality and features while testing the product, including support for multiple domains, end user quarantines, white and black lists, and a comprehensive automated reporting suite.

Additional features that may benefit business users include LDAP integration, the ability to scan both inbound and outbound email, support for appending legal disclaimers to messages, and the ability to potentially detect botnet sources.



Throughout the test process, West Coast Labs used the accompanying SpamTitan documentation and found it to be well-written, containing accurate, step-by-step configuration instructions, as well as useful help and support guides.

The solution is deployed with Kaspersky and Clam malware detection engines that compliment and enhance the core anti-spam technologies.



It is also worth noting that the SpamTitan solution focuses on a 'security by default' paradigm, exemplified by the use of FreeBSD as the base

SpamTitan for VMware, Version 4.09

operating system and the requirement to configure trusted networks for mail relay purposes.

Potentially, the most significant supplementary feature is derived from the product delivery method; deployed as a software package, the SpamTitan solution is one of a relatively small number of currently available VMware Certified Virtual Appliances.

A virtual machine infrastructure combines beneficial elements from both software and physical appliances to form a flexible, immediately available solution. For example, the SpamTitan solution was available to be instantly tested, with the added benefit that West Coast Labs were not required to build and configure a separate base operating system for deployment and evaluation purposes.

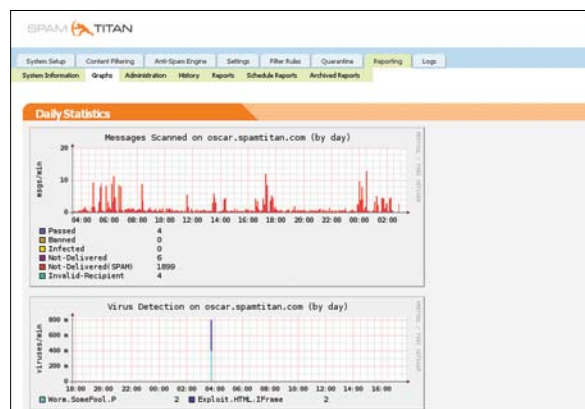
Additional VMware advantages noted in this instance include the easy deployment and re-use of a single virtual machine across multiple locations, backup and redundancy options that essentially provide the equivalent of multiple physical appliances, and scalability gains that allow the fast and simple allocation of additional memory and CPU resources as required by potentially fluid business demands.

SpamTitan for VMware, Version 4.09

Reporting

West Coast Labs made extensive use of the in-built management and reporting functionality that is provided via an SSL-secured web-based console.

A comprehensive dashboard page includes a system overview of current resource utilization, cumulative scan statistics for inbound and outbound spam emails, recent malware activity, and details of the current mail queue. The dashboard data is supplemented by an extensive, easy-to-use reporting capability that provides an audit trail of all historic system activities and email throughput. The solution produces reports in both tabular and chart-based formats. In a multiple domain environment, reports may be produced on a per domain basis for added flexibility.



West Coast Labs found the reporting engine to be feature-rich, containing numerous management and configuration options, beneficial to any business deployment.

SpamTitan for VMware, Version 4.09

Results

<u>Type of Mail</u>	<u>Detected as Genuine</u>	<u>Detected as Spam</u>
GENUINE	100%	0%
SPAM	1%	99%

Performance levels throughout testing proved consistently high, with the solution correctly identifying 99% of Spam email, while correctly delivering genuine email.

West Coast Labs found that the solution identifies spam email using a combination of rule based analysis and advanced Bayesian filtering. The SpamTitan solution also used optical character recognition software to identify image-based spam.

West Coast Labs is pleased to award SpamTitan for VMware the Anti-Spam Premium Checkmark.

SpamTitan for VMware, Version 4.09

Conclusion

The SpamTitan solution successfully fuses impressive spam detection capabilities with ease-of-use to provide a powerful, potentially cost-effective, and flexible email threat detection and protection platform. The flexibility combined with scalability is designed to allow benefits to organizations of all sizes.

Delivered as a VMware virtual appliance, the solution proved incredibly easy to install, manage, test, and backup. In some cases this offers advantages over the more traditional physical appliance or software installation model as it allows for flexibility in the base system used and rapid disaster recovery.

The concise documentation, combined with advanced configuration options and comprehensive reporting ensure that the solution is not only easy to set up for both new users and those more comfortable with the VMware approach, but also that it can be adapted to provide a specialised fit for every company in which it is installed.

SpamTitan for VMware, Version 4.09

Security Features Buyers Guide

SpamTitan for VMware is a virtual email gateway appliance protecting email against spam, phishing, viruses, and unwanted content. It is delivered as a virtual appliance and certified to run with the VMware suite of products.

[url : www.spamtitan.com](http://www.spamtitan.com)

SpamTitan for VMware, Version 4.09

Security Features Buyers Guide

Business Benefits... as stated by CopperFasten

The SpamTitan product focuses on 3 elements of business efficacy and saving.

1. Procurement.

SpamTitan's competitive pricing combined with virtual appliance delivery offers excellent costs savings from product purchase through to product deployment.

Pricing ranges from a 100 user license costing US\$500(UK£244) to a 500 user license costing US\$1250(UK£612). Use of the virtual appliance further drives efficiencies through maximum usage and return on existing hardware resources.

2. Low Product Maintenance

SpamTitan has been designed to operate with the lowest management overhead possible. Automated updating, backup, reporting and notification ensure that management intervention is kept to a very minimum, thus keeping cost to a minimum

3. Solution Saving

SpamTitan spam detection accuracy and end user management tools ensure lost productivity associated with email use is almost eliminated.

SpamTitan for VMware, Version 4.09

Security Features Buyers Guide

Technical Benefits... as stated by CopperFasten

SpamTitan is designed as a standalone mail gateway with full SpamTitan's anti spam engine blocks in excess of 98.5% of spam with a less than 0.03% false positive rate. It includes both the award winning Kaspersky and Clam anti virus engines. Functionality includes end user quarantines, a full automated reporting suite, automated updating, per domain reporting and administration, LDAP integration, white/blacklists, in and out bound mail scanning, disclaimers, simple deployment and management, protection from image based spam and botnet detection. These functions coupled with those offered from the virtual appliance provide the management flexibility required for the dynamic aspects of email protection today.

[url : http://www.spamtitan.com/anti-spam/vmware/technical-specifications](http://www.spamtitan.com/anti-spam/vmware/technical-specifications)

SpamTitan for VMware, Version 4.09

Security Features Buyers Guide

Developments over the last 12 months... as stated by CopperFasten

Over the past 12 months we have added greatly to the functionality of SpamTitan and the anti spam rule sets, both of which have increased the products ability to combat new emergent spam techniques and the methods which administrators can manage these outbreaks.

- Added Optical Character Recognition (OCR) plugin to combat increased spread of image only spam. This plugin checks for specific keywords in embedded image files
- On Demand Quarantine Reports - Users now have the ability to request an on-demand quarantine report.
- Added a penpals soft-whitelisting feature. This lowers the spam score of received replies to a message previously sent by a local user to this address. This can be useful in preventing potential false positives from email addresses that users are in frequent contact with.
- Added a 'View Source' tab to the quarantine mail viewer. This allows the user to view the unformatted 'raw' message source.
- Added a spam quarantine cut off level. Administrator can now set a policy to quarantine spam, but to discard messages scoring above a certain level. This is configurable on a per-domain/per-user policy basis.
- Added the ability to import lists of domains during configuration. This is particularly for sites that are handling 100s or even 1000s of domains.
- Added a mail queue management function. This allows users to view, hold, release and delete messages in the event of any mail queue.
- Spam score can be included in the subject of spam messages that are forward when the policy is 'Tag and Pass'.
- Administrator may forward a quarantined message to his/her own

SpamTitan for VMware, Version 4.09

email address for inspection. It is also possible to Release, Delete or Whitelist a message directly from the quarantine mail viewer.

- Botnet detection plug in. This determines if message arrived via a spam botnet which then contributes to the overall anti spam scoring system.

SpamTitan for VMware, Version 4.09

Security Features Buyers Guide

Additional Noteworthy Product Features... as stated by CopperFasten

Of particular note with SpamTitan for VMware is the product delivery method and the benefits accrued from it. Although strictly speaking the product is software it is deployed as a Virtual Appliance. SpamTitan is one of the few VMware Certified Virtual Appliances globally. What virtual appliances offer is the marrying of the advantages of the software delivery with those delivered by physical appliances. It offers the flexibility associated with traditional software delivery combined with the advantages of the “plug and play” elements of physical appliances, no OS build and installation for example. Using the VMware suite of products, SpamTitan can be opened and run as a virtual appliance within a virtual machine on an existing server. On the network it is identified as would any other physical appliance. The customer accesses SpamTitan via the web based GUI, the same way they would a physical appliance. Using VMware they can decide what resources to give this virtual appliance, i.e. memory, CPU, disk space.

This delivery method offers the customer tremendous benefits over traditional software and physical appliances, predominantly associated with flexibility. The product is downloadable so can be tested immediately; test copies can be kept on file. There is no OS configuration or server build required. It can be deployed to global regional offices over the net. Using VMware products it can be backed up (the equivalent of requiring a back up physical appliance) and restored in minutes. The SpamTitan Virtual Appliances can be scaled as required. If our virtual appliance needs more memory or CPU because of increased mail volumes it can be done with a few strokes of the keyboard.

westcoast labs

US SALES

T+1 (717) 243 5575

EUROPE SALES

T+44 2920 548 400

GLOBAL HEADQUARTERS

West Coast Labs
Unit 9 Oak Tree Court
Mulberry Drive
Cardiff Gate Business Park
Cardiff
CF23 8RS, UK