Spam Filtering

Powered By TitanHQ

Email represents the single critical utility of today's companies driving productivity, efficiency and cost savings. Unfortunately, bundled within its many advantages are significant threats which have the capacity to destroy your network and incur serious legal and financial repercussions for you and your business.

The simple act of opening an email or clicking a link can release payloads of viruses which, apart from demolishing your network's internal structures, can also unleash devastating consequences for your clients by fulfilling their basic viral nature; that of spreading secretly from one computer to another with malicious intent.

Benefits

- Cloud-based solutions allows for easy set up and maintenance
- Guarantees 99.97% spam detection
- Protects against viruses and malware
- External authentication means users won't have to remember multiple passwords
- Scans outbound email to prevent IP blacklisting

Protect Your Business

What is Spam Filtering

A part of the ProCloud Security suite of products, Spam Filtering Powered by TitanHQ is a full-service, cloud-based email security solution which protects your business, your employees and your clients. The cloud solution is extraordinarily simple to set up and manage, requires no software installation and provides among its many features, 99.70% spam detection, virus and malware blocking, authentication control, outbound scanning, as well as robust reporting structures.

Email Content Control and Protection for Business

Spam Filtering protects the organization from threats by managing the organization's email traffic and regulating the email that employees receive by blocking spam email, viruses and malware.

Spam Filtering requires no software installation and can be set up and operational in a matter of minutes, making it an ideal solution for any organization.

Why Use Spam Filtering

Spam Filtering has been purpose-built to enable businesses to easily protect their users and network from spam email, viruses and malware. The cloud solution is designed to easily integrate into the existing infrastructure and deployment is very straightforward.

The solution enables businesses to filter the organization's email traffic without any expensive or time consuming overheads.

According to a 2016 report by Kaspersky, the percentage of spam within global email traffic has increased over the past couple years to the point that 59 percent of email received is spam. And the majority of malicious spam included ransomware, greatly compromising businesses.

Spam Filtering
Spam Filtering Powered by TitanHQ filters your organization's email traffic to stop email spam from reaching your users. The solution guarantees 99.97% spam detection through multi-layered spam analysis, including: real time blacklists (RBLs), lists of websites that were detected in unsolicited emails (SURBLs), sender policy frameworks and Bayesian analysis. This coupled with a low false positive rate of 0.03% allows you to rest easy knowing your users never lose genuine email but are protected from unsolicited email.

Virus and Malware Blocking
The multi award-winning solution contains double antivirus, including: Kaspersky Lab and Clam AV, which serve to block viruses and malware trying to infiltrate your network through email.

White Listing/Black Listing
The solution allows you to whitelist/blacklist sender email addresses, meaning you can choose to always allow/always block mail from a particular email address. Keys can be created instantly and allow the user to bypass a policy rule. Each Cloud Key can be created for single or multiple users, controlled by time or date.

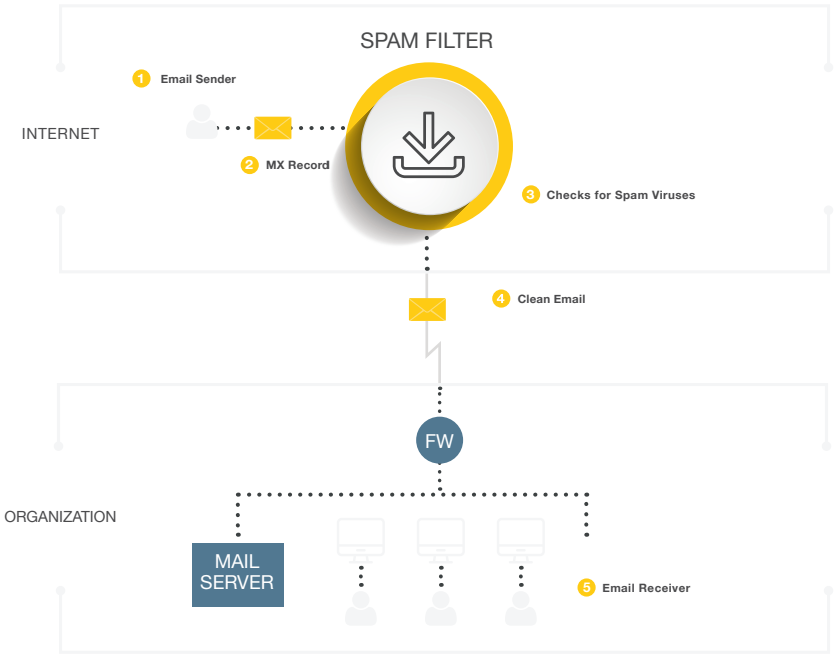
Reporting
Spam Filtering can send quarantine reports to users at specified times and intervals. The quarantine report contains a list of emails which have not been sent to the user because they potentially contain spam or viruses. The end user can decide to deliver, whitelist or delete the emails in the quarantine report.

Cloud-Based
The cloud-based solution requires no software installation making it simple to set up and manage. There is no management or maintenance overhead as updates and support are fully included in the product.

Recipient Verification
Spam Filtering offers a number of Recipient Verification types, including: Dynamic Recipient Verification (DRV), LDAP, list-based and specify regular expression verification. Once a mail is delivered to the Spam Filter, it will validate the email address against the mail server, thus rejecting fake emails and spam.

Outbound Scanning
Outbound scanning of email is vital today. It blocks spam and viruses being sent out from your organization, thus preventing your IPs from being blacklisted as a spammer by one of the many global blacklisting services. IP blacklisting prevents email delivery, interferes with business process and makes productivity difficult and time consuming to resolve. Spam Filtering prevents this.

Authentication
The web authentication settings allows you to control for each domain what authentication method will be used when a user attempts to login. The following authentication methods are supported: Internal (default), LDAP, SQL server, POP3, and IMAP. The support of external authentication modules ensures that, when possible, users won't have to remember multiple passwords. All login attempts will be directed to the appropriate authentication server for that domain.



ADTRAN, Inc.
901 Explorer Boulevard
Huntsville, AL 35806
256 963 8000

General Information
800 9ADTRAN
www.adtran.com/contactus

Canada Headquarters—Toronto, Ontario
+1 877 923 8726
+1 905 625 2515
sales.canada@adtran.com

Canada—Montreal, Quebec
+1 877 923 8726
+1 514 940 2888
sales.canada@adtran.com

Mexico and Central America
+1 256 963 3321
+1 52 55 5280 0265 Mexico
sales.cala@adtran.com

South America
+1 256 963 3185
sales.brazil@adtran.com
sales.latam@adtran.com

Spam Filtering Technical Specifications

Spam Filtering	■ The solution provides a 99.97% spam detection through multi-layered spam analysis including: • Real time blacklists (RBLs) • Lists of websites that were detected in unsolicited emails (SURBLs) • Sender policy frameworks • Bayesian analysis ■ Low false positive rate of 0.03%
Virus and Malware Blocking	■ Spam Filtering Powered by TitanHQ contains double anti-virus protection ■ Kaspersky Lab and Clam AV serve to block viruses and malware trying to infiltrate your network through email
White Listing/Black Listing	■ You can choose to always allow/always block mail from a particular email address
Reporting	■ Quarantine reports to users at specified times and intervals. The quarantine report contains a list of emails which have not been sent to the user because they potentially contain spam or viruses. The end user can decide to deliver, whitelist or delete the emails in the quarantine report
Cloud-based	■ No software installation required, making it simple to set up and manage. There is no management or maintenance overhead as updates and support are fully included in the product
Recipient Verification	■ Spam Filtering offers a number of Recipient Verification types: • Dynamic Recipient Verification (DRV) • LDAP • List based • Regular expression
Authentication	■ The web authentication settings allow you to control for each domain what authentication method will be used when a user attempts to login. The following authentication methods are supported: • Internal (default) • LDAP • SQL server • POP3 • IMAP ■ The support of external authentication modules ensures that, when possible, users won't have to remember multiple passwords. All login attempts will be directed to the appropriate authentication server for that domain.
Outbound Mail Scanning	■ Spam Filtering can also scan your outbound mail, thus preventing potential IP blacklisting.

For more information about Spam Filtering Powered by TitanHQ, please visit ***adtran.com/msp***