Nest Mail Security Powered By SpamTitan+
Real-time AI Protection Against Zero-Hour Phishing Attacks

SpamTitan email securityfor business.

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 networi<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.

What is SpamTitan ?

SpamTitan is a full-service, cloud based email security solution which protects your business, your employees and your clients. The solutionn operates as a hosted multi-tenant Software-as-a-Service deployment from Nashua Nest's datacenter and is extraordinarily simple to manage, and provides 99.97% spam detection, virus and malware blocking, authentication control, outbound scanning as well as robust reporting structures.

Central to everything we do is our service commitment to our client base, which is many companies trust us with their business.

Email content control and protection for business.

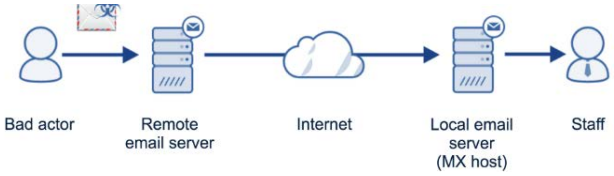
SpamTitan protects the organisation from threats by managing the organisation's email traffic and regulating the email that employees receive by blocking spam email, viruses and malware.

SpamTitan is ideal for both small and larger organizations as it provides all of the benefits of a gateway solution with virtually none of the technical overheads. Your SpamTitan service can generally be deployed by one of our engineers within 24 hours of your request.

Why use SpamTitan?

SpamTitan has been purpose-built for business of all sizes to enable easily protect their users and network from spam email, viruses and malware.

No Email Security Solution



With Nest's Email Security Solution

Product features

MANAGEMENT FEATURES:

Extensive API

SpamTitan has an extensive API which enables you to integrate with third party management products.

Scalable

SpamTitan is easily scalable and can grow as your business expands. It has the capacity to facilitate unlimited users and unlimited domains and allows multilevel administration including user level, domain level and groups of domains etc.

Our Cloud

SpamTitan is deployed as a cloud-based service. This SaaS email security service is hosted in the Nashua Nest Cloud operating within our secure datacenters.

Reporting suite

SpamTita can send a quarantinee 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.

CUSTOMER FEATURES:

Spam filtering

SpamTitan filters your organisation'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.

Sandboxing

Spam Titan sandboxing protects against breaches and data loss from zero-day threats and sophisticated email attacks by providing a powerful environment to run in-depth, sophisticated analysis of unknown or suspicious programs and files.

This advanced email security layer will provide protection against malware, spear-phishing, advanced persistent threats (APTs), offering insight into new threats and helping mitigate risks.

DMARC

Domain-based Message Authentication, Reporting and Confonnance (DMARC) is an email-validation system designed to detect and prevent email spoofing. It is used in conjunction wth SPF and/or DKIM to give domain administrators the ability react to emails when criteria
are not met.

DMARC matches the "From" header to the "Envelope From" of the sending email. It can help prevent spoofing of the "From" headers often used by spammers in phishing campaigns.

Virus and malware blocking

The multi award winning solution contains double antivirus protection; Bitdefender 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.

Recipient verification

SpamTitan offers a number of Recipient Verification types they are: Dynamic Recipient Verification (DAV), LDAP, list based and specify regular expression verification. Once a mail is delivered to the SpamTitan Cloud, 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 organisation, 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 productivity is difficult and time consuming to resolve. SpamTitan 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 appro priate authentication server for that domain.

SpamTitan+ Technical Specifications

Spam filtering	» 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 • Bayesian analysis, » Low false positive rate of 0.03%.
Virus and malware blocking	» SpamTitan contains double anti-virus protection; » Bitdefender and Clam AV which 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.
Recipient verification	» SpamTitan offers a number Recipient Verification types. They are: • Dynamic Recipient Verification (DAV) • LDAP • List based • Regular expression » These all help to keep your license count correct. » Once a mail comes to SpamTitan we will question the mail server.
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 • SOL 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	» SpamTitan can also scan your outbound mail, thus preventing potential IP blacklisting.
Extensive API	» SpamTitan has an extensive API which enables you to integrate with third party management products.
Scalable	» SpamTitan is easily scalable and can grow as your business expands and has the capacity to facilitate unlimited users and unlimited domains and allows mutti- level administration including user level, domain level and groups of domains etc.
Cloud Based	» SpamTitan is deployed as a cloud based service within Nashua Nest's secure Gaborone based datacenter.

Nest Mail Security Powered By SpamTitan+
Real-time AI Protection Against Zero-Hour Phishing Attacks

About Nashua Nest

Nashua Nest is the CSP (Cloud Service Provider) division on Nashua Botswana.

We operate our own independent vendor neutral tier-2 compliant datacenter within Nashua House in Gaborone from where our full range of cloud services operate. We provide a full range of hosted IaaS, SaaS, PaaS, DRaaS, BaaS, FWaaS deployment models, including full-service ICT MSP services for outsourced ICT services utilizing our hosted RMM (remote management and monitoring) solutions. As well as being an approved Microsoft CSP and partners with a range of other relevant vendors, we also provide a full range of hardware design/provision/support from SME to large scale corporate virtualized server infrastructures and storage solutions.

Our goal is to simplify the intricate world of cloud and ICT services for our customers. This goal has driven our business since inception and today we have a range of SME to large corporate clients across Botswana supported by a committed team of professionals who are focused on delivering the best products and services for companies who require solid and proven cloud and ICT services for their business.

Contact details

If you are interested in learning more about Nashua Nest range of services, please reach out to us on by phone or email and one of our experienced professionals will take the time to answer any questions you may have.

Phone
+(267) 399 4041 / 399 2016
+(267) 71729186 / 75431188

Email
nest@nashua.co.bw