Cloud Email Firewall

Maximum email availability and protection against phishing and advanced threats.

If the company email is not protected then the information is not safe

Cloud Email Firewall is a solution **that efficiently protects business** mailboxes and enables organizations to administrate, control and secure their email.

Email is a strategic tool and keeping it safe is critical for today's organizations.. **Phishing attacks** remain as one of greatest threats faced by corporations and 95% of the email that businesses receive on a daily basis is spam or malware.   This situation decreases the productivity of the companies. An email firewall makes possible to reduce the financial impact of receiving spam and malware by optimizing the use of email-related technology

infrastructures.   The constant evolution of the spammers.

techniques   calls for   the use of an email firewall that utilizes advanced filtering technologies that are constantly being updated.

Cloud Email Firewall is based on proprietary detection technologies that analyze billions of emails every day   aiming at identifying Spam patterns   in real time and blocking their   entry.   Malware is   withheld at Spamina's cloud, ensuring consequently that the company mail server receives   only clean email. Suspicious email is quarantined in our data centers for up to 28 days.
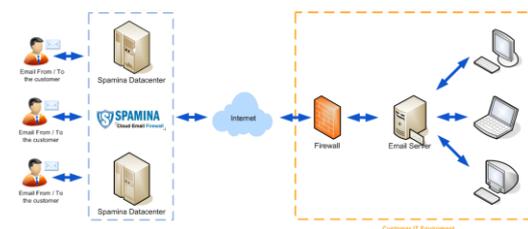
Email filtering is designed to detect spam, phishing, malware and viruses in real time using advanced patterns and classifications techniques. Cloud Email Firewall provides a comprehensive antivirus protection that integrates several layers of AV filters by default while some extra layers can be added optionally.

European developer & provider ensuring data protection

Spamina complies with the most demanding EU regulations in terms of personal & corporate data privacy. Our data centres are located within the limits of the EU therefore there is no *Safe Harbor* data transfer that could wriggle out of the European legislation.

Simile Fingerprint Filter®

This spam detection technique differentiates and separates automatic bulk mailing from the legit corporate email that gets efficiently delivered. The process is further supplemented by adding extra AV filtering layers and some other content filtering techniques ensuring spam, phishing, virus and malware are stopped in real time. The collection of filtering technologies that powers the Spamina service detects and blocks 99 percent of spam, with less than one in one million false positives. Customers may also opt to enable the Spamina Advanced Threat Protection (ATP) module, which adds an extra layer of protection that

performs dynamic analysis of attachments in a sandbox prior to delivery. ATP ensures that emails received by end users are free from zero-day malware and threats beyond the scope of detection of fingerprint-based techniques. Furthermore, it makes sure that URLs embedded in emails are checked for safety at click time.

Administrator and User Consoles

Administrator console: Spamina provides a unified administrator console for the overall management of whitelists, blacklists, security policies, management groups, level of spam filtering and other options. You can easily define white and black lists globally or allow users to manage their own lists. The administrator console has been designed for being extremely user friendly and for enabling you to swiftly implement the company security policies for the email.
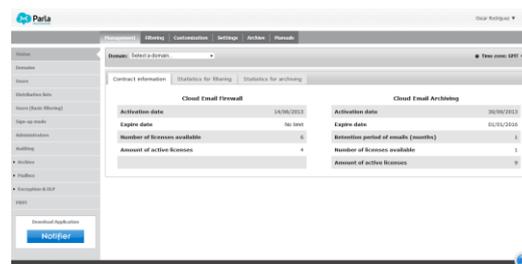
User console: Besides the managing capabilities for the administrator, Cloud Email Firewall incorporates a console that provides a way for users to easily manage their own email and access their preferences. The employees receive daily reports so they can easily check Spam activity on their accounts; add sender's whitelists and blacklists, recover emails and other functionalities without the need for

credentials or the administrator's intervention. Valid email can be classified in the white list

Policies and content filtering rules

Administrators can define rules based on granular policies for the inbound and outbound email. They can also fix a wide range of actions based on message attributes and content. The content filtering engine enables defining corporate policies without disrupting the normal workflow of the employees. New version adds improvements in the rules engine such as the option of selecting MIME-type attachments or the possibility of adding logical operators when applying a rule sequence. Cloud Email Security Suite includes optionally the ability to add our advanced encryption and DLP module for confidential data protection and legal compliance.


Management console with fully customizable reports

The Cloud Email Firewall control panel manager provides email statistics including global email traffic, and enables customized reporting for every domain protected with Cloud Email Firewall.
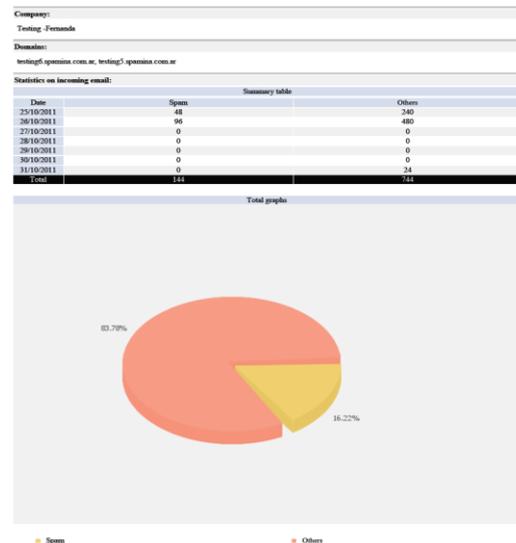

Spamina Notifier

Spamina Notifier is a locally installed management and notification tool that alerts of spam received without having to open either the mailbox, the webmail or the console. It enables users to easily manage their black & white list options without the intervention of the administrator.
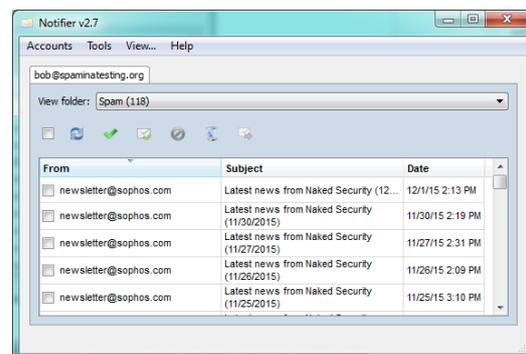
Spamina Outlook Add-in

The Cloud Email Firewall users can access their filtering control panel directly from the Outlook interface via the plugin developed for the 2007, 2010, 2013 and 2016 versions.
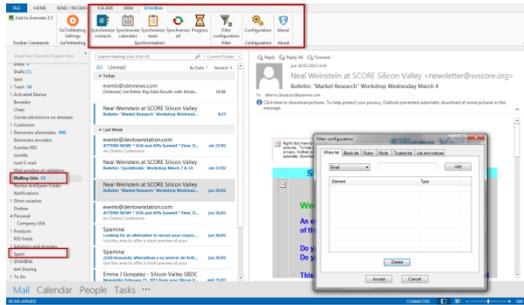
Cloud email continuity

Cloud Email Firewall includes by default Cloud Email Continuity that ensures service continuity even in case of mail server downfalls. It provides with email spooling, backup and webmail access in order to maintain productivity while the service is restored. Anywhere, from any device and with no additional cost.

- **Email spooling**: If your email server suffers an outage, Cloud Email Firewall automatically stores all incoming mail for up to four days, creating a safety net so no email is lost.
- **Automatic email backup:** Cloud Email Firewall automatically keeps safety copies for up to 28 days enabling users to recover false positives or accidentally deleted emails when needed. The administrator can decide to configure this option ad-hoc.
- **Webmail:** Integrated email access via Webmail enabling users to keep working even under email server shutdown.

Corporate image customization

Spamina services are fully customizable with the "white label" option, so you can bring into line the user interface with the company corporate image. Corporate colors or logos may be modified from the Spamina interface in order to match your company branding.

Optional integration with archiving and encryption & DLP solutions

Cloud Email Firewall can be upgraded with solutions designed to prevent data leakage and ensure legal compliance.

- **Cloud Email Archiving**: Archiving, legally compliant solution. Cloud Email Archiving prevents the manipulation of the email content by rendering it immutable. The email gets automatically indexed, stamped for integrity and archived. Storage capacity is virtually unlimited.

- **Cloud Email Encryption & DLP** is a policy-based managed encryption solution. This engine not only encrypts messages based on pre-defined corporate policies, it re-directs and prevents confidential information from being distributed over the Internet to the wrong people.

Cloud Email Firewall

Key Features
Enforce TLS connections on selected destination servers or domains
Improvement alert enhancements when emails cannot be sent
Password recovery mechanisms
Strict validation of mail senders to prevent impersonation
Multi-layer filtering, integrated with advanced technology
Dashboard and report generation engine
Centralized quarantine functions
Available in different provision modes (Public, Private and Hybrid)
A solution based on a scalable and distributed architecture (SDA)
Email policies management
Compatibility with IPv6
Integration with any email platform
Real-time management of users, available for the different profiles
DKIM outbound email signature integrated.
New version adds improvements in the rules engine such as the option of selecting MIME-type attachments or the possibility of adding logical operators when applying a rule sequence.
Full archiving for incoming email
Guaranteed continuity of service through 24x7x365 data center monitoring
Integrated webmail

About Spamina

SPAMINA, is a European-based security company that develops and provides corporations with flexible and Secure Digital Communications. Managing and mitigating cyber-crime related risk is critical. Widely known electronic communications means such as email, as well as the increasingly used instant messaging, are channels where the corporate digital assets can be jeopardized. Simile Fingerprint Filter® proprietary technology protects corporate networks from advanced and zero-day threats. Spamina provides with a safe communication environment where business continuity, service scalability and cost-effectiveness are ensured.

Our cloud services range from enterprise secure email platform, enterprise mobile management, email & IM gateway protection to archiving and encryption & DLP solutions for legal compliance.

A cloud environment involves storage and transfer of digital information. Spamina is subject to the most demanding EU regulations in terms of data protection and is committed to ensuring the highest security standards for digital safeguard.

More information:

Phone: +34 91 368 77 33

www.spamina.com

SPAMINA SOLUTIONS

Cloud Email **Firewall**

Advanced Threat **Protection**

Parla Secure Cloud Email

ParlaMI Secure Instant Messaging

Cloud Email **Archiving**

Cloud Email **Encryption & DLP**

SPAMINA
Securing Digital Communications