Cloud Email Encryption & DLP

Ensure email privacy and prevent data leakage

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

Most of the corporate intellectual property is located in email repositories. Organizations should take a preventive approach and acknowledge the importance of adopting encryption strategies to protect email communications.

Leakage of strategic company's information via email communication is often underestimated. As a result, in most cases the emails are transmitted insecurely then stored and forwarded several times. Mail can be intercepted anytime, making its content an easy target for malicious users.

Cloud Email
Encryption & DLP

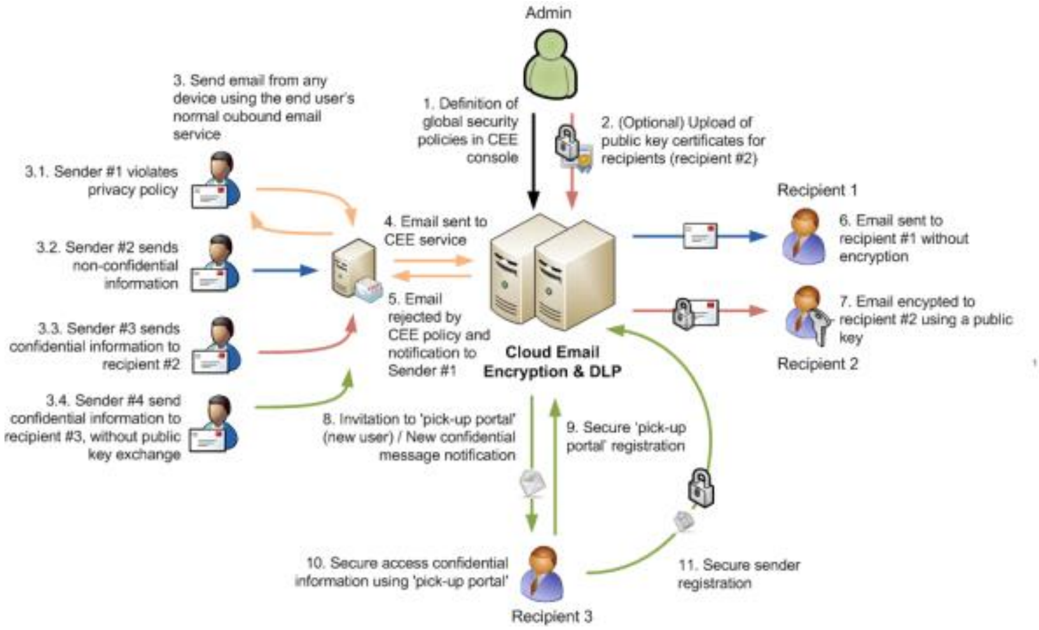
Cloud Email Encryption & DLP is a policy-based managed encryption solution that provides organizations with an easy way to enforce email encryption without disrupting the day-to-day workflow of their employees.

It puts the IT department back in control by enabling it to manage the organization's entire email infrastructure. At the same time it enables users to read their encrypted email from their desktop or mobile device. This policy-based encryption 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.

Automatic email encryption

Automatic encryption of the emails containing sensitive information by the action of a powerful outbound mail policy engine: automatically and securely applies the organization encryption policies while enabling regulatory compliance.

.

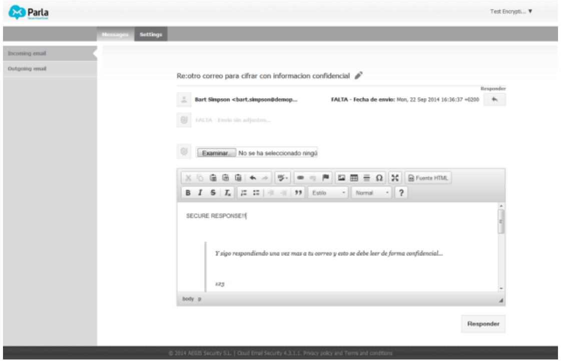

Admin
3. Send email from any device using the end user's normal cubound email service
1. Definition of global security policies in CEE console
2. (Optional) Upload of public key certificates for recipients (recipient #2)
3.1. Sender #1 violates privacy policy
Recipient 1
4. Email sent to CEE service
6. Email sent to recipient #1 without encryption
3.2. Sender #2 sends non-confidential information
5. Email rejected by CEE policy and notification to Sender #1
7. Email encrypted to recipient #2 using a public key
3.3. Sender #3 sends confidential information to recipient #2
Cloud Email Encryption & DLP
Recipient 2
3.4. Sender #4 send confidential information to recipient #3, without public key exchange
8. Invitation to 'pick-up portal' (new user) / New confidential message notification
9. Secure 'pick-up portal' registration
10. Secure access confidential information using 'pick-up portal'
11. Secure sender registration
Recipient 3

Automatic key management

The previous exchange of information between the recipient and the sender is not required in order to ensure that information remains confidential.

Safe email pick up portal

Enables recipients to easily access the encrypted emails while ensuring messages can be read regardless of the device used by the recipient.



Re:otro correo para cifrar con informacion confidencial

Bart Simpson <bart.simpson@demop... FALTA - Fecha de envío: Mon, 22 Sep 2014 16:36:37 +0200

FALTA - Envío sin adjuntos...

No se ha seleccionado ningú

SECURE RESPONSE!!

Y sigo respondiendo una vez mas a tu correo y esto se debe leer de forma confidencial...

123

© 2014 AEGIS Security S.L. | Cloud Email Security 4.3.1.1. Privacy policy and Terms and conditions

Email reading notification through pickup portal.

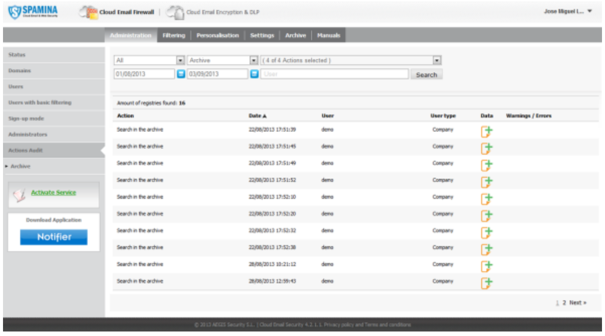
Write and reply messages ensuring end-to-end confidential and safe communications. When an encrypted mail is read by the recipient through the portal pickup, CEE & DLP automatically sends a reading notification to the sender. Sending this email message can be configured (enabled or disabled) at company level, domain, and even user.

Supports standard encryption

Supports encryption with PGP and S/MIME regardless of the emitting device.

Powerful policy engine

Powerful policy engine which includes an extensive number of rule templates and predefined dictionaries, preventing data leakage in your organization: Avoid and locate security breaches according to your leakage prevention policies (DLP).



All | Archive | (4 of 4 Actions selected)

01/08/2013 | 03/09/2013 | User

Amount of registries found: 16

Action	Date ▲	User	User type	Data	Warnings / Errors
Search in the archive	22/08/2013 17:51:39	demo	Company		
Search in the archive	22/08/2013 17:51:45	demo	Company		
Search in the archive	22/08/2013 17:51:49	demo	Company		
Search in the archive	22/08/2013 17:51:52	demo	Company		
Search in the archive	22/08/2013 17:52:10	demo	Company		
Search in the archive	22/08/2013 17:52:20	demo	Company		
Search in the archive	22/08/2013 17:52:32	demo	Company		
Search in the archive	22/08/2013 17:52:38	demo	Company		
Search in the archive	28/08/2013 10:21:12	demo	Company		
Search in the archive	28/08/2013 12:59:43	demo	Company		

1 2 Next »

© 2013 AEGIS Security S.L. | Cloud Email Security 4.2.1.1. Privacy policy and Terms and conditions

Dashboard

Handle all the company's security policies from a single management console. Administrators can create fully detailed statistics of encrypted emails.

Outlook Add-in

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

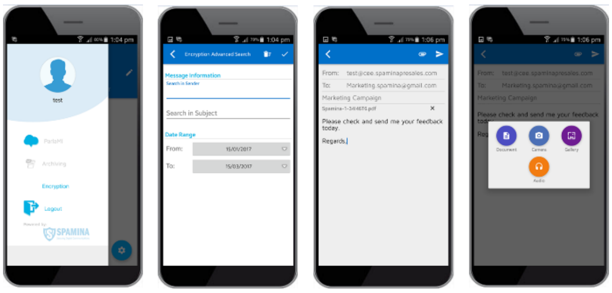
Now integrated in the new Spamina App

An intuitive and friendly interface access to corporate email encryption, through the new App, available for iOS and Android devices

Users of Cloud Email Encryption can now send and received encrypted emails from anywhere.

Functions available from the App:

- Send, received and visualized encrypted email
- Access to content and answer encrypted emails
- Search emails by subject, sender and date



From: 15/01/2017

To: 15/03/2017

From: test@cee.spaminapresales.com

To: Marketing.spamina@gmail.com

Marketing Campaign

Spamina-1-34146T6.pdf

Please check and send me your feedback today.

Regards,

Cloud Email Encryption & DLP

Key Features
New! Integrated in the new Spamina App
Email reading notification through pickup portal
Automatic encryption for the email carrying sensitive information
Encrypted emails can be read from both desktops and mobile devices
Writing and replying to messages ensuring end-to-end protected communications
Automatic key management
Rule templates and predefined dictionaries options
Empower you IT department by enabling the detection of security breaches according to your policies. Prevent data leakage (DLP) and ensure emails are confidentially exchanged.
Supports standard encryption (PGP and S / MIME) regardless of the device used for sending the encrypted email.
Fully detailed statistic dashboard
Integration with Outlook via plugin that enables direct sending of encrypted emails without creating specific policies

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 91368 77 33

sales@spamina.com

www.spamina.com

SPAMINA SOLUTIONS

- Cloud Email Firewall
- ATP Advanced Threat Protection
- Parla Secure Cloud Email
- hi! ParlaMI Secure Instant Messaging
- Cloud Email Archiving
- Cloud Email Encryption & DLP