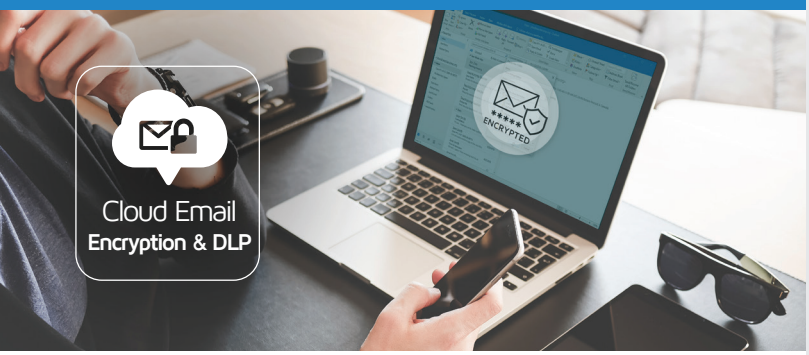
SPAMINA
Securing Digital Communications

CLOUD EMAIL ENCRYPTION & DLP

Proactively protect and control corporate data flow to support governance without user impact



PROTECTED > ENCRYPTED > USER CENTRIC > COMPLIANT

Spamina Email Encryption & DLP is an integrated Data Leak Prevention (DLP) solution for email in the cloud. It identifies, monitors, and protects sensitive data when it's being used, transmitted, or stored. With a comprehensive view into data flow and usage, Spamina Email Encryption & DLP enables you to set and enforce policies that control data exposure. Encrypt or empower users to encrypt customer and business information, personally identifiable information (PII), employee, health and financial data, and intellectual property.

Spamina Email Encryption & DLP also protects against mistakes that can lead to data leaks or misuse and ultimately jeopardize compliance. Even when email is stored securely, it is often forwarded multiple times, making confidential information easier to intercept by malicious actors. Employees also can increase risk unintentionally through instant messaging and emailing documents containing sensitive data. Spamina makes it easy for security teams to align DLP policies with compliance requirements, such as EU GDPR, PCI DSS, and others.

KEY BENEFITS

Accelerate Regulatory Compliance

- Identify and categorize data sent outside the organization
- Support audits and compliance with at-a-glance reports and detailed analysis
- Encrypt communications as needed to comply with industry-specific regulations
- Maintain a record of all encrypted communications

Simplify DLP with Policy-Based Inspection

- Use built-in rule templates and predefined dictionaries to identify confidential content and define policies
- Identify, monitor, and protect data in all incoming and outgoing email messages
- Set policies for the entire organization, specific business units, or individual domains

Empower User Productivity

- Encrypt specific content by default and allow users to decide for other content
- Allow mobile users to simply click to read and respond to encrypted messages
- Deliver encrypted messages in the cloud, and to desktop and mobile devices

Enhance Existing Security Measures

- Alert users when they attempt to send an email that should be encrypted and alert administrators when encrypted emails are sent
- Notify message senders when recipients read their encrypted emails
- Collaborate securely with trusted partners through policy-based auto-encryption

Reduce Costs

- Eliminate CAPEX costs for hardware, software, and on-premises systems through cloud delivery
- Reduce licensing cost and complexity
- Lower OPEX costs with ability to tailor appropriate policies from a single pane of glass

Two-Way Alerts and Reporting

Encrypted emails generate a notification to the security team, which helps organizations meet specific industry security and compliance requirements. User notification alerts end users when an email should be encrypted or when a company policy has not been followed.

A Powerful Policy Engine

Spamina provides rule templates and predefined dictionaries to help identify confidential content and define policies. Powerful inspection capabilities monitor all incoming and outgoing email.

Multiple Access and Management Options

Spamina offers flexible management options. You can determine when to encrypt content by default and when to allow the user to decide. You also can control how messages are delivered—via a "park-and-pull" portal or secured by public-key infrastructure.

Made in Europe

We understand European customers' geographic data requirements. Our data centers operate in areas where your data privacy is legally protected from third parties.

PREVENT DATA LEAK ACCORDING TO POLICY

Set policies based on your organization's requirements. Spamina Email Encryption & DLP identifies confidential content in email messages and attachments, blocks sensitive data from leaving the organization, and keeps detailed logs of encrypted emails for analysis. You can set policies for the entire organization, specific business units, and by domain to prevent data leaks and ensure that emails are confidentially exchanged.

SIMPLIFY DLP FOR MOBILE USERS

Mobile users can easily read encrypted email from their mobile devices. The Spamina mobile app makes DLP completely transparent, allowing users to simply click to read and respond.

ENSURE DELIVERY FLEXIBILITY

Whether your organization uses a third-party public key authentication service or decrypts messages at the user endpoint, Spamina enables you to tailor message delivery to your needs. If you have a service-provided key, Spamina places encrypted messages in a park-and-pull portal. Senders and recipients do not have to exchange private keys prior to sending email, and users can read, write, and reply to messages securely with end-to-end confidentiality.

Spamina also lets you collaborate securely with trusted partners. Policy-based auto-encryption protects data as it moves outside of your organization. When teams collaborate frequently or daily, you can set policy to enable individuals to send and receive emails securely without using the park-and-pull portal.

PROACTIVELY PREVENT DATA MISUSE

Spamina alerts help ensure that data is not misused—whether on or off the corporate network. Encrypted emails can automatically generate a notification when they are sent, supporting compliance with industry-specific regulations and company policies.

Spamina can automatically notify message senders when recipients read their encrypted emails. You can tailor policy to alert users when they attempt to send an email that should be encrypted —notification helps create awareness of potential data leakage and empowers the user to correct the mistake. Administrators have immediate visibility into reports and detailed analysis through the dashboard. You can easily implement new DLP policies on the fly and conduct awareness campaigns that educate users about information protection and compliance.

SUPPORT COMPLIANCE INITIATIVES

Spamina Email Encryption & DLP meets critical data governance requirements for availability, security, usability, and data integrity. It helps identify and categorize data sent outside the organization and greatly simplifies policy creation and enforcement.

Spamina Email Encryption & DLP supports your audit and compliance activities for a wide range of regulatory acts, including EU GDPR. Data protection regulations, such as GDPR, require organizations to keep a record of all data that can contain private information, and organizations must update their policies, messaging inventories, and procedures. Spamina makes it simple. Spamina Email Encryption & DLP also simplifies compliance with PCI DSS, HIPAA, FINRA, PIPED, and other region-specific regulations.

EXTEND THE BENEFITS

Spamina Email Encryption & DLP integrates with Microsoft Outlook in Microsoft Exchange and Office 365, as well as with Google mail. You can further extend email and instant messaging protection with Spamina Cloud Email Firewall, Advanced Threat Protection, and Cloud Email Archiving to integrate communication hard protection, data leak prevention, and threat prevention, and compliance in a single console.

Spamina Trusted Protection for Enterprise Email and Instant Messaging

ASK FOR A FREE TRIAL
spamina.com/en/free-evaluation

SPAMINA
Securing Digital Communications

www.spamina.com
+34 91 368 77 33
info@spamina.com

About Spamina

Spamina provides innovative enterprise solutions in the areas of Threat Prevention, Data Governance and Secure Collaboration. Our cloud services offer customers a safe communication environment where business continuity, service scalability and cost-effectiveness are ensured. Headquartered in Madrid (Spain), Spamina serves customers in more than 50 countries, supported by a network of authorized partners.