GBS

Email DLP or how to stop bleeding sensitive data through your email

How to use Data Loss Prevention against malicious or accidental data leaks in your outgoing communication

As the most important business communication channel, email serves as the primary platform for exchange of data within and outside the company, a large portion of which contains sensitive information. Consequently, email is one of the main targets of hackers and the ultimate gateway for malware such as ransomware and phishing. This is why ensuring adequate security of email communications and compliance with data protection regulations should be one of the top priorities of a company's security strategy. The good news is that security vendors are working continuously to improve and enhance the features of email security technology.

Contents

Data Loss Prevention – a rule-based concept for data-driven security

As a large number of companies have already recognized, there is much more that can be done for email security than mere anti-virus scanners, firewalls and spam filters. By upgrading to data protection tools, organizations can monitor their email traffic more closely, identify potential vulnerabilities and control access to sensitive data without compromising productivity. It is now possible to analyse outgoing emails as per internal security policies, detect suspicious email activity and prevent the accidental/ intentional leaking of sensitive information.

The technology behind these functionalities is called Data Loss Prevention (DLP) – a term that has been around for more than 15 years. The concept of DLP is exceptional and has become the foundation for many other cyber security mechanisms and tools. In fact, DLP is one of the first examples of data-driven security.

Data Loss Prevention relates to every technology designed to protect data. Correspondingly, email DLP therefore specializes in preventing data leaks in email traffic, by blocking insider threats, containing human errors and detecting sensitive data and suspicious activities.

Can DLP help against phishing?

Hackers and data thieves resort primarily to phishing mails to gain access to sensitive data. Their highly personalized emails look so convincingly real, that it is often difficult to recognize the fraud before it is too late. By pretending to be a trustworthy sender and by faking a legitimate concern, the recipient is tricked into disclosing confidential information, such as credit card data or passwords, or is misled to opening a file attachment. One click can be enough to start the undetected installation of a Trojan virus, collecting and transmitting data directly to the data thief or giving hackers access to the company network.

To prevent this, outgoing communication should be analyzed and the attempted distribution of sensitive contents (e.g. customer lists in Excel spreadsheets) or behaviour anomalies (e.g. email attachments or massive transmission of company data) should be detected and blocked. Manual solutions not only compromise productivity but are also error-prone, which is why the magic word here is “automation”. Modern DLP solutions are characterized by monitoring functions and dashboards, enhancing transparency and providing insights regarding current threat levels.

DLP prevents both malicious and accidental security vulnerabilities in outgoing email

It can be distinguished between two general categories of data loss via outbound emails – accidental (also non-intentional) and malicious. Here are some examples of both.

- Employee sending by mistake sensitive info to the wrong recipient
    - When they hit "reply all" instead of just "reply"
    - Through a typo in the recipient name
- Employee attaching the wrong file, which contains sensitive data
- Employee unknowingly sending information or replying to
    - an unauthorized person
    - a phishing email
    - an email manipulated by identity/ account theft
    - an email compromised by supply chain attack
- Employee non-maliciously forwarding documents with sensitive information from work to personal email (unsecured devices) to continue working on them at home
- Deliberate or unknowing sending to a blacklisted recipient/domain
- Deliberate sending of sensitive information and attachments

Without a DLP solution in place, detecting any of the above would be quite a difficult job. Just imagine that each employee sends about 10 emails per day, for 100 employees that is 1000 emails per day to check by hand. Not to mention the delays in delivery, errors and access verification.

A solution that monitors and analyses email traffic can easily detect abnormal activities that could indicate there is something unusual happening with outgoing emails. The DLP solution's job is to monitor the following performance indicators, compare them to the average values set by the IT administrator and trigger an alert and a predefined action if there is a significant deviation.

- Number of emails
- Volume of emails
- Number of recipients

Who benefits the most from the use of email DLP technology?

Examining what is considered sensitive data sheds light on the question of who could benefit most from DLP technology.

- Examples of sensitive data include:
- Personal identification data
- Driver's license numbers
- Credit card numbers
- Social security numbers
- Bank account numbers and transactions
- Login IDs and passwords
- Health records
- Intellectual property

- Business financial data
- Trade secrets

If we map this data to the respective functions in the company, it becomes clear which departments in a company handle the most sensitive data that is subject to data protection regulations.

- Company departments that benefit from DLP:
- Human Resources (personal data, social security numbers, etc.)
- Finance and accounting (credit cards, bank transfers, IBANs, passwords, etc)
- Sales and Customer service (customer data)
- Research & Development (intellectual property)

As data is the new gold of the business world, industries that typically generate and process large amounts of data are the first to be targeted by hackers. Given this fact and their critical importance to the economy, they are subject to strict regulatory control by the government and the EU.

- Industries that benefit the most from DLP:
- Utilities (Energy, water, etc.)
- Telecommunications
- Health and Pharma
- Finance and Insurance
- Public administration
- Legal bodies
- Digital service providers

To configure your Email DLP solution, you need definitions first

The most important thing to remember about DLP technology is that it relies on rules to work properly. DLP gives companies the flexibility to define these rules in full accordance with their internal policies and to set key indicators and thresholds that best meet their needs.

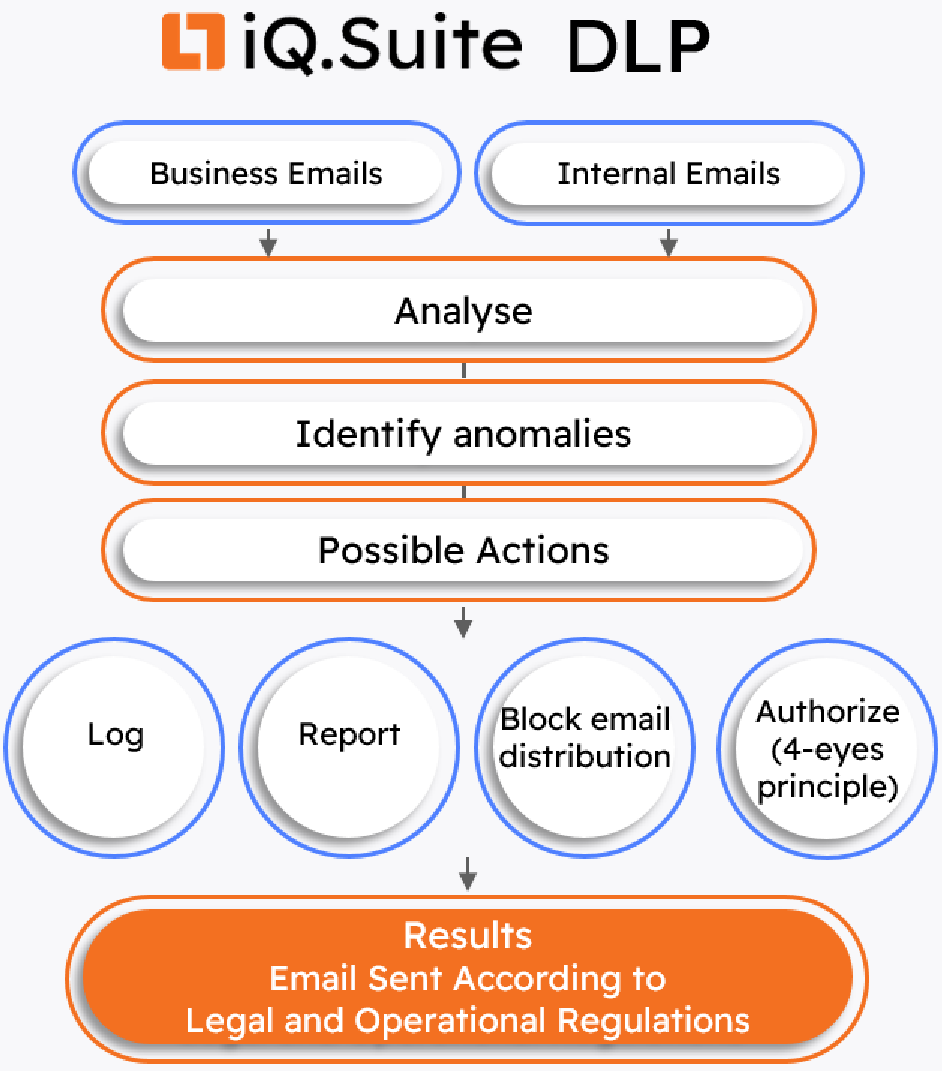
To ensure optimal performance of DLP technology, companies need to identify the following key definitions for their rules.

- Define what counts as sensitive information and what are the indicators for it
- Define text content items that will be considered critical
- Set benchmark values and thresholds for comparing email traffic
- Define roles and responsibilities for handling critical emails
- Define processes that are triggered after a violation is detected
- Set quarantine rules
- Set automatic blocks
- Set forwarding to review persons
- Set alerts and notifications to users for different actions

iQ.Suite DLP by GBS – advanced Data Loss Protection solution for your email

iQ.Suite DLP by GBS is an advanced solution for protection against malicious and accidental data leaks in outgoing email communication. The solution is available for Domino, Microsoft, On-Premises, Cloud and as a Service.

iQ.Suite analyses every element of the email, its body, subject lines, attachments and HTML code according to predefined policies and values. At the same time, the sender's actions are inspected for deviations from normal activities and thresholds. If a suspicious pattern is detected, an automatic process is initiated depending on the issue. The email can be blocked, quarantined or forwarded to others for review and all relevant notifications are sent.



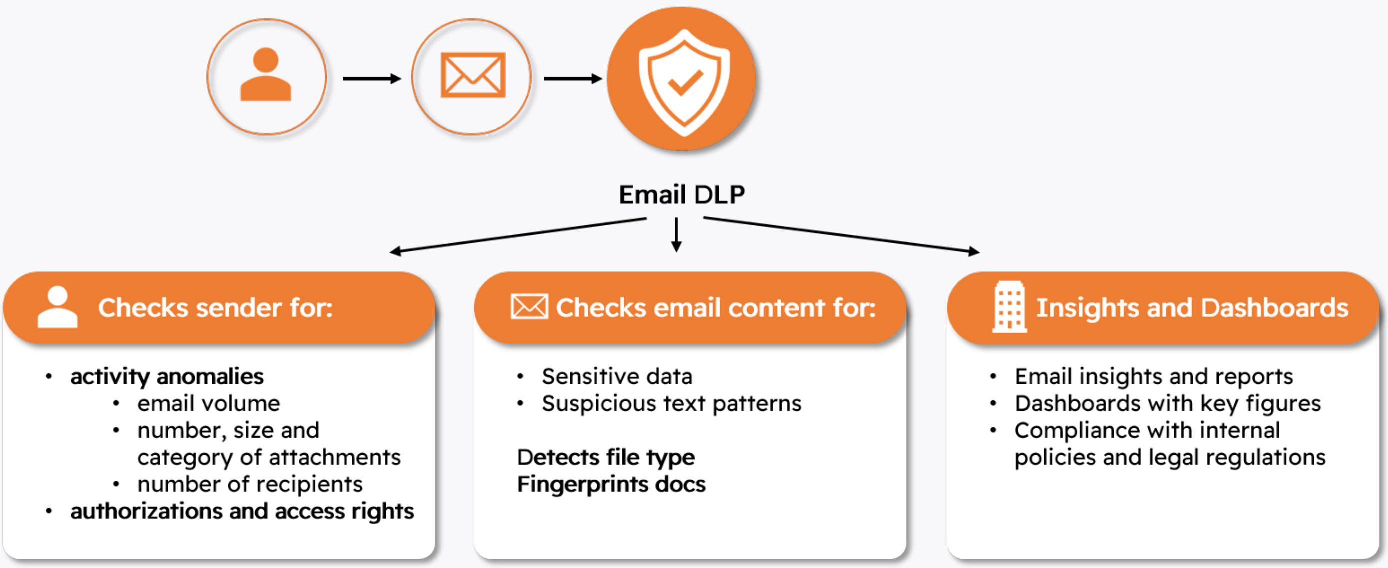
iQ.Suite DLP workflow

How does iQ.Suite DLP ensure advanced security for your sensitive data?

A good email DLP solution identifies sensitive information, prevents data theft and stops data leakage. In accordance with this principle, iQ.Suite DLP provides advanced data security in just 3 steps: it analyzes, evaluates and blocks.

Step 1 - Analyzes email traffic

- Real-time analysis of outbound email communications, company-wide or for selected departments
- Detailed examination of emails before sending
- Detection of suspicious text patterns (credit card data, customer numbers, etc.) in email texts and attachments
- Clear identification of file attachments such as Office formats thanks to the advanced fingerprint technology
- Detection of behavior anomalies in email flow. For this purpose, information such as the number and size of the emails sent in a given period is collected and compared with the current behavior of users. This makes it possible to detect a disproportionate increase in email volume or the sending of large amounts of data, which could indicate a leak of confidential data.



Email DLP

Checks sender for:

- **activity anomalies**
  - email volume
  - number, size and category of attachments
  - number of recipients
- **authorizations and access rights**

Checks email content for:

- Sensitive data
- Suspicious text patterns

Detects file type
Fingerprints docs

Insights and Dashboards

- Email insights and reports
- Dashboards with key figures
- Compliance with internal policies and legal regulations

iQ.Suite DLP features

Step 2 - Evaluates indicators and visualizes key values

- Web-based dashboard for visualization of key figures
- Detailed insights into outbound email communications regarding email volume, number, size and category of attachments, number of recipients per email, etc.
- Easy export and use of data for reporting purposes
- Integrated rights and roles concept: Users can access relevant to them information only if they are authorized.
- Configurable data deletion after a specified time period according to current data protection guidelines

Step 3 - Blocks suspicious emails

- Flexible rules and thresholds - defining how to handle emails containing confidential content
- Options for actions
- Place emails in quarantine until further examination
- Additional notification of sender and third party
- Double-check (four-eyes) principle review performed by a pre-determined person who takes the final decision if the email is to be released or blocked.
- Any combination of actions is possible, in accordance with the company guidelines

4-eyes (double-check) principle for review of stopped emails

If an email with critical content is detected and it is not entirely clear whether it is safe to send, iQ.Suite DLP allows the 4-eyes principle to be applied. The four-eyes principle (also known as double-check, dual control and two-man rule) is simply an internal control mechanism stipulating that a certain critical activity, process or decision must be approved by two predetermined competent persons to ensure that the best possible decision is made. This principle is applicable in a broad variety of areas – for instance, many legal documents require two signatures to be authenticated or to authorize document revisions in certain data management systems before the changes to the data are accepted. In other words, iQ.Suite DLP forwards questionable emails to pre-determined people who can decide whether the email is safe enough to be sent on to the final recipient.

Notifications that educate and rise security awareness

If an email is classified as critical, iQ.Suite offers the option to send a notification about it to the sender, the recipients or any other person or group. These notifications can contain any text, links or graphics, which gives companies the opportunity to educate their employees about security vulnerabilities and the company's internal security policies. It is easy to prepare ready-made texts explaining why the email has been blocked/quarantined/reviewed and how the data it contains could be compromised. A simple quote from the internal security policy or a link can be added to support the explanation. This helps the employee understand the risk and increases their security awareness, making them more vigilant and enabling them to correct the email and avoid disclosing data in the future.

Features of iQ.Suite DLP:

- Detection of anomalies in email transmission
- 4-eyes principle review and release of stopped emails
- Stops transmission of suspicious emails
- Monitoring functions and dashboards, enhancing transparency and providing insights into current threat levels
- Enforcing email-encryption by tagging an email containing sensitive information

Benefits of iQ.Suite DLP:

- Automated and managed from a central point
- Eliminates human error and reduces workload
- Allows implementation of internal policies
- Compliance with legal regulations due to high data security
- Easy export of data for reporting purposes

Every year, the renowned ISG Provider Lens™ Quadrant Reports evaluate and rank the best solutions in the category “Data Leakage/Loss Prevention (DLP) and Data Security”. In 2022, GBS ranked for the fourth time among the leading companies on the German market in the area of "Cybersecurity - Solutions and Services" with its security solution iQ.Suite DLP. The repeated ranking in the same category as the strongest players in the IT and security market proves that the GBS solution, with its outstanding innovative features, makes no compromises when it comes to data security.

About GBS

GBS is a distinguished provider of e-mail and collaboration security solutions in Germany with almost 30 years of experience in data protection, productivity and compliance. The company is recognized as a leader in cyber security solutions, particularly in the areas of Data Loss Prevention and Collaboration Security by top market researchers in Germany and by our partners.

GBS offers one of the most comprehensive next-generation solutions for e-mail productivity, compliance and multi-level protection of e-mail communication and data exchange across different collaboration platforms against all types of security threats. Our solutions for Microsoft 365, Office 365, Exchange and HCL Domino are easy to use and flexible, covering key areas such as malware protection, encryption, e-mail productivity, data leakage, workflow and compliance.

GBS solutions protect more than 2 million end users worldwide. The company has built long-standing relationships with over 2,000 customers.