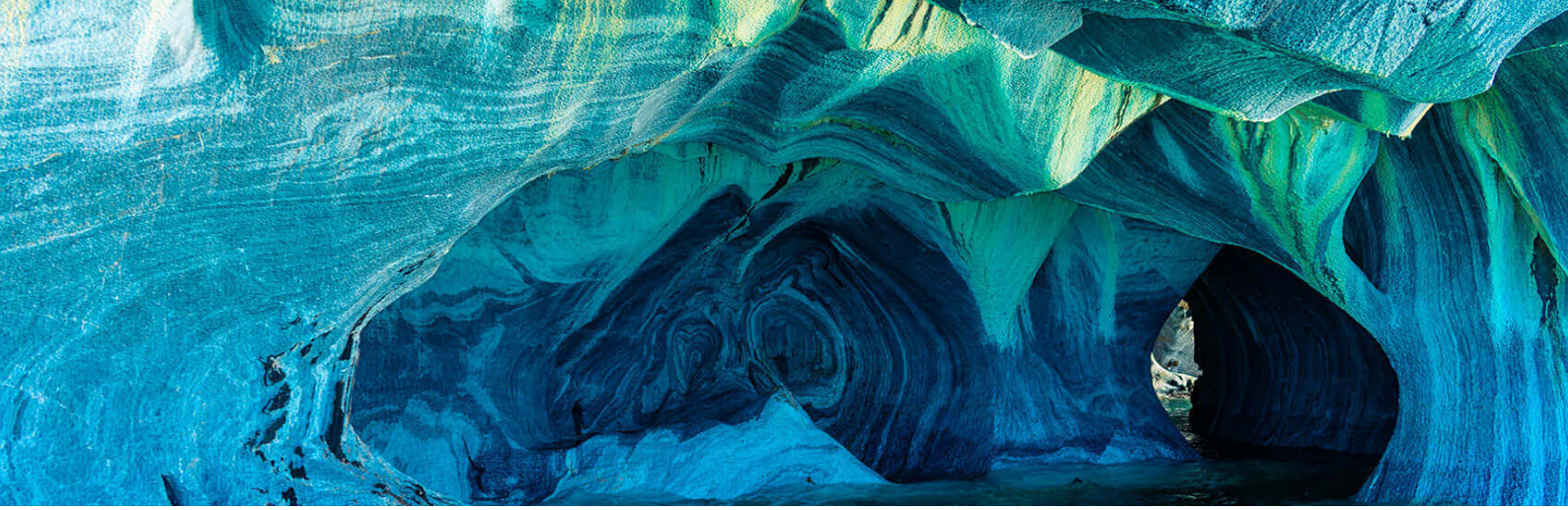

iQ.Suite DLP

Data is one of the most critical assets of a company

Data Loss Prevention protects you from attacks exploiting employee behavior

Protecting sensitive information such as customer data and confidential documents (Data Loss Prevention) is a major challenge for companies. In times when attacks on business-critical content are increasing in number and sophistication, a consistent email security strategy is more important than ever. However, securing incoming communication only with the help of virus and spam protection is no longer sufficient, so outgoing communications must now also be taken into account.

iQ.Suite – Advanced Data Loss Prevention based on the principle “analyze, evaluate, block”

Email data breaches can take different forms, such as accidentally sending sensitive data to the wrong recipient, unauthorized email communication between the development department and external recipients, or dismissed employees sending confidential corporate data shortly before they leave. To prevent these scenarios, organizations must have technology in place to identify sensitive information, guard against data theft and accidental data loss, as well as to comply with GDPR requirements.

Analyze email traffic

- Real-time analysis
- Clear identification of file attachments
- Detailed examination of emails
- Detection of behavior anomalies
- Detection of suspicious text patterns

Evaluate and visualize

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

Block suspicious mails

- Flexible rules and thresholds
- Options for actions

Benefits

- Identification of sensitive information in email texts and attachments
- Detection of behavior anomalies in email transmission
- Blocking of suspicious emails
- Double-check (four-eyes) principle review and release of stopped emails
- Web-based dashboard for visualization of key figures
- Easy export of data for reporting purposes
- Compliance with current data protection guidelines