

E-mail Lifecycle Management



Your path to safe and efficient e-mail.

GROUP Technologies is a world leader in e-mail lifecycle management.



Isolated solutions for e-mail management are inefficient – a virus scanner here, a spam filter there, encryption software somewhere in between, and then, perhaps, a link to an archiving system. Today automated, secure, and efficient business processes for e-mail are requisite. And such processes are provided by e-mail lifecycle management, which effectively increases productivity, reduces costs, and improves competitiveness.

E-mail lifecycle management makes it possible to efficiently implement current and future security and organizational requirements for electronic mail.



Jürgen Wege
Chief Executive Officer
GROUP Technologies AG



The best technology is useless if it doesn't address everyday problems, and reduce workloads. GROUP Technologies has designed e-mail lifecycle management solutions to tackle everyday problems and streamline business processes. And, this is why so many companies, large and small, have been using our cutting-edge technologies for over 10 years.

Only powerful and integrated software such as our iQ.Suite permits the mapping and implementation of effective e-mail business processes. This capability ensures comprehensive e-mail lifecycle management, and guarantees that companies will have safe and efficient e-mail communication.



Frank Kresse
Chief Technology Officer
GROUP Technologies AG

Contents

E-mail Lifecycle Management	6	iQ.Suite at a Glance	13
■ E-mail Pre-processing	8	iQ.Suite – Basic Functions	16
■ E-mail Firewall	9	iQ.Suite – Products	18
■ E-mail Classification	10	■ Accounting & Billing	19
■ E-mail Compliance	11	Budget	19
■ E-mail Archiving, Retrieval, Retention	12	■ E-mail Pre-Processing	21
		Crypt	22
		Trust	23
		Smart	24
		Trailer	25
		■ E-mail Firewall	27
		Watchdog	28
		Wall	29
		■ E-mail Classification	31
		Wall	32
		■ E-mail Compliance	35
		Bridge	36
		Clerk	37
		■ E-mail Archiving, Retrieval, Retention	39
		Safe	40
		Store	40a
		Bridge	41
		■ Technical Requirements	42



Professional Services	44
Partners	48
References	50
Success Stories	52
About GROUP Technologies	56



From the very beginning, dolphins have symbolized the power and sensitivity of GROUP Technologies. Their extraordinary mental and physical capabilities make them uniquely suited to represent our company's corporate culture and our industry expertise. The abstract depiction of leaping dolphins has been incorporated into the GROUP corporate logo as an expressive symbol of these qualities. Dolphins are generally described as socially adept, intelligent, fast, powerful, courageous, and purposeful. The dolphin serves as a perfect metaphor for GROUP Technologies.





We make your e-mail safe and efficient.



E-mail Lifecycle Management

E-mail lifecycle management (ELM) is a set of strategies and methods for processing, storing, and managing e-mail, from creation to deletion, in accordance with business processes and regulations. E-mail lifecycle management ensures effective business processes in every company.

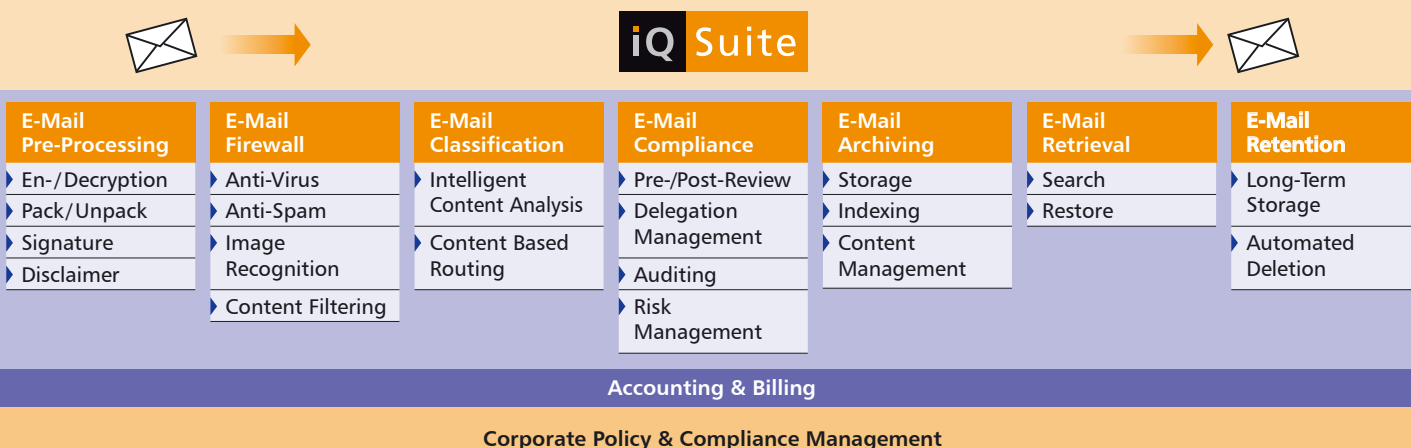
The iQ.Suite from GROUP Technologies is the leading software package for e-mail lifecycle management, and is the ideal solution for implementing safe and efficient business processes. With iQ.Suite, e-mails pass through all the necessary processes on a single platform, from encryption and virus protection, anti-spamming and content-filtering, to classification and long-term archiving.

E-mail can be controlled and automatically processed throughout its entire lifecycle based on specific rules. Third-party archiving systems can be seamlessly incorporated into the iQ.Suite and used for audit-proof e-mail archiving.

Take advantage of e-mail lifecycle management:

- Integrated e-mail business processes
- Legal compliance
- Higher productivity
- Lower Cost of Ownership (TCO)
- High Return on Investment (ROI)

E-Mail Lifecycle Management



E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature Disclaimer	Image Recognition		Auditing	Content Management		
	Content Filtering		Risk Management			



E-mail Pre-processing

E-mail preparation for processing and transmission.

Packed files frequently contain viruses, some of which are encrypted. These files often evade virus scanners and go undetected.

E-mail pre-processing ensures that all incoming e-mails are first decrypted and unpacked by the server. Subsequent spam and virus filtering identifies unwanted e-mails and places them in quarantine. Checked e-mails can then be automatically re-encrypted and forwarded.

Outgoing e-mails can be signed, furnished with a legal disclaimer, packed, automatically encrypted, and sent.

E-mails are centrally and automatically encrypted on the mail server, based upon address. The mail server uses PGP, GnuPG, or S/MIME, all of which can also be used in parallel operation. Keys can be managed on the server without a cumbersome public-key infrastructure (PKI), and digital certificates can be easily created and updated.

iQ Suite	Crypt	_____	Page 22
iQ Suite	Trust	_____	Page 23
iQ Suite	Smart	_____	Page 24
iQ Suite	Trailer	_____	Page 25

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



E-mail Firewall

Protection against dangerous or unsolicited e-mail and accidental transmission of confidential information.

Almost daily we hear news reports about viruses and the increasing volume of spam on the Internet. Effective protection against these dangers is essential. The iQ.Suite gives companies a rule-based filtering method to check incoming e-mail for viruses, spam, and unwanted images, files, and content.

Integrated virus filters check the entire e-mail for malicious code. Critical file types are filtered based upon unique file pattern information, known as “fingerprints.” Companies can use any combination of the leading virus scanners in parallel operation.

Before delivering an e-mail, the iQ.Suite checks for spam based upon company policy, inspecting every part of the message: address data, subject line, text, file attachments, and image files. With outgoing e-mail, the iQ.Suite can block the transmission of sensitive information.

The integrated CORE technology (Content Recognition Engine) classifies and filters e-mail automatically based upon individual specifications. CORE guarantees the highest detection rates for anti-spam, and prevents *false-positives* (e-mail incorrectly identified as spam).

iQ Suite **Watchdog** _____ Page 28

iQ Suite **Wall** _____ Page 29

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



E-mail Classification

Detection and classification of content, and additional content-based e-mail processing.

Rule sets are an integral feature of the iQ.Suite, permitting companies to individualize their business processes based upon internal policies. Using e-mail classification, a company can automatically categorize, forward, or further process e-mail based upon predefined contents or recipient addresses.

The rule sets are implemented in the CORE technology, which is integrated into iQ.Suite. CORE is a statistical method for automatic e-mail verification and classification. As a self-learning filter, CORE can also detect complex content based upon individual criteria.

Using the classification function, incoming e-mail can be forwarded to the appropriate recipient automatically. For example, a customer support request sent to a general e-mail address can be forwarded directly to the employee who is best-suited to address the problem.

This address- and content-based routing guarantees that critical messages go to the right mailbox, and that any actions needed for further processing are initiated immediately.

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



E-mail Compliance

Full observance of and adherence to legal and regulatory provisions.

With the iQ.Suite, companies can send and receive e-mail in compliance with government regulations and internal company policies. Using company-specific rule sets as a basis, e-mails can be automatically intercepted and checked in accordance with the *four-eyes* security principle. After released from this process, e-mails are then sent, placed in quarantine, forwarded to third parties, or deleted.

This verification process ensures that the recipient receives only e-mail that is in full compliance with company policies. Outgoing e-mail cannot be abused through the unauthorized transmission of sensitive documents.

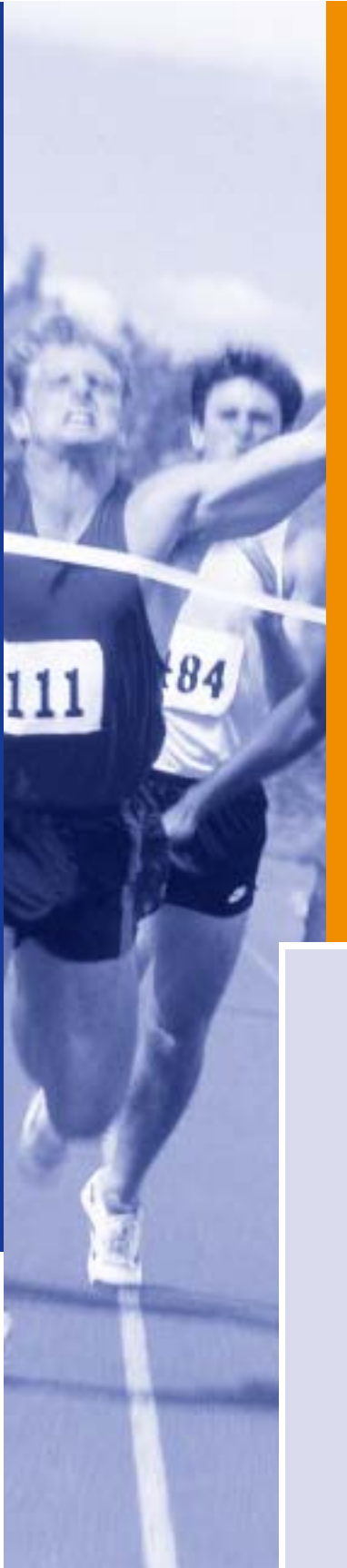
E-mail correspondence can be seamlessly traced and retrieved when needed for internal or external audits.

Rule-based, uniform e-mail forwarding ensures that all important messages are forwarded to authorized delegates when the e-mail recipient is absent. At the same time, the system also makes sure that confidential messages are not forwarded.

iQ Suite **Bridge** _____ Page 36

iQ Suite **Clerk** _____ Page 37

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature Disclaimer	Image Recognition		Auditing	Content Management		
	Content Filtering		Risk Management			



E-mail Archiving, Retrieval, Retention

E-mail Archiving, administration, search, retrieval, and deletion.

Companies are obligated by law to archive their e-mail for specific time periods. The integrated iQ.Suite archiving module can be used for this purpose, and leading archiving solutions by third-party vendors can also be seamlessly incorporated into the system.

Archiving takes place prior to delivery in order to prevent manipulation by users.

iQ.Suite automatically forwards important metadata such as e-mail headers, processing details, and categories to the archiving system for automatic index generation.

E-mail correspondence can be retrieved at a later date based upon keywords (e.g. for a tax audit). This guarantees that e-mail is audit-proof as required by law.

iQ Suite	Safe	Page 40
iQ Suite	Store	Page 40a
iQ Suite	Bridge	Page 41

iQ.Suite

The leading e-mail lifecycle management solution.

With the iQ.Suite, companies can optimize the performance of their e-mail environment, increase productivity, reduce costs, and ensure legal compliance. E-mail can be a safe and efficient business process. The iQ.Suite can be used with the leading e-mail platforms Lotus Domino, Microsoft Exchange, and SMTP Gateways.

The iQ.Suite is modular, fully scalable, and offers a high degree of investment security. Because of its completely server-based architecture, this powerful software package can be administered from a central location for further cost savings.



iQ Suite

Flexible policies for optimized business processes

Well-planned integration into existing business processes is a vital prerequisite for the safe and efficient use of e-mail. Company-specific, freely user-definable policies form the basis for the management and control of effective e-mail communication. The iQ.Suite guarantees completely rule-based policy management for maximum security and optimized business processes.

Clear competitive advantage

Optimized external and internal e-mail communication within a company means a clearer market focus and significantly higher levels of customer satisfaction. Increased flexibility and targeted, rapid response to customer and market needs translate into increased revenues and profits. The iQ.Suite is a critical element for increasing your overall competitiveness.

Reduced costs and increased efficiency

Secure external and internal e-mail communication protects companies against direct and indirect damages, and eliminates the need for cost-intensive damage control efforts. More efficient use of e-mail saves time and money. With the iQ.Suite, you can immediately realize enormous cost-savings potential in your e-mail use. The iQ.Suite can also be centrally managed, which significantly reduces administrative overhead. Common protocols, reports, and statistics provide cost transparency and clearly show ways to further optimize your e-mail rule sets.

Secure investment for the future

The iQ.Suite has a rich portfolio of applications aimed at optimized security and efficient e-mail organization. iQ.Suite products can be combined and scaled as needed with applications used standalone or as a complete solution, depending upon a company's specific needs. Its modular structure enables the iQ.Suite to be expanded at any time. This ensures optimal functionality and stability, and also guarantees that your investment will continue paying dividends well into the future.



Risk management and legal compliance

Failure to comply with mandated regulations on audit-proof e-mail archiving can lead to significant penalties in the event of a government audit. There is also a risk of direct, personal liability by company officers vis-à-vis shareholders/owners or government agencies. The iQ.Suite guarantees that your e-mail communication is in compliance with all applicable laws, and uses active risk management to avoid possible dangers.

Complete security, designed by experts

GROUP Technologies is a specialist in e-mail lifecycle management. Our many years of experience translate into well-tested and robust solutions – yesterday, today, and tomorrow. You can rely on the iQ.Suite, the leading solution for e-mail lifecycle management.



iQ.Suite – Basic Functions

The iQ.Suite's modular architecture allows it to be deployed as a standalone solution for a specific problem, or as a completely integrated strategic solution for e-mail lifecycle management. Regardless of which iQ.Suite module you choose, the basic functions are always included.

The basic functions include professional policy management, reporting and statistics, comprehensive quarantine management, centralized administration, and the iQ.Suite Portal.

Powerful basic functions mean efficient e-mail management, always a given with GROUP Technologies.



Policy management

Policies for e-mail communication within your company can be comprehensively depicted in the iQ.Suite rule sets. This is a major step toward compliance with legal requirements such as Basel II, GDPdU, SOX, and HIPAA.

The flexibility of the iQ.Suite rule sets allows policies to be implemented for users, user groups, user ranges, and domains. Using objects from the user directories is as easy as adapting to modified company policies. The iQ.Suite's flexible import/export functions ensure efficient implementation. In addition to using customized white and black lists, companies can also selectively send messages to administrators, senders, recipients, and any other individuals or groups. The standard functions of the iQ.Suite can also be enhanced as needed with user-defined scripts for extremely complex policies.

Reporting and statistics

The reporting and statistics functions contained in the iQ.Suite form the basis for a number of different analyses, e.g. tracking the course of a specific virus attack. The preconfigured or customized analyses can be shown in overviews and diagrams. Statistics on the proportion of sender groups can also be displayed as a diagram and generated as a file. With this function, users can create easy and fast analyses for inclusion in reports to management.

Quarantine management

Regardless of whether a message is spam, a virus, or an incorrectly encrypted e-mail, the system administrator can manage all blocked e-mails centrally and efficiently in the iQ.Suite quarantine. Each user can also define a user-specific quarantine to classify and manage suspect e-mail. Access remains restricted to the individual e-mail mailboxes, which reduces the administrator's workload. The progressive iQ.Suite quarantine management system means that critical e-mails are never lost.

Centralized administration

All of the iQ.Suite modules can be centrally administered through a uniform user interface.

iQ.Suite Portal

The iQ.Suite Portal is the user interface, available as a browser or client application. Each user gains access through the iQ.Suite Portal to the e-mails that have been placed into quarantine for him, and to his own individual white and black lists.

Personal absence management settings can also be easily administered using the iQ.Suite Portal. Automated absence notification to deputies or other individuals can be freely defined. The administrator can specify and easily configure the options available to each user.

Options

iQ.Clustering

- iQ.Clustering is an additional option for iQ.Suite and supplements clustering at the operating system level or between e-mail servers. iQ.Clustering guarantees high availability, failure safety, load distribution, and distributed computing for the iQ.Suite.
- iQ.Clustering ensures full capacity utilization when multiple e-mail servers are used.

iQ.Mastering

- The iQ.Mastering option makes it possible to deploy the iQ.Suite in parallel operation with other leading security products. Products already in use, e.g. antivirus programs, can also continue to be used together with various iQ.Suite modules.

iQ.Suite – Products



E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

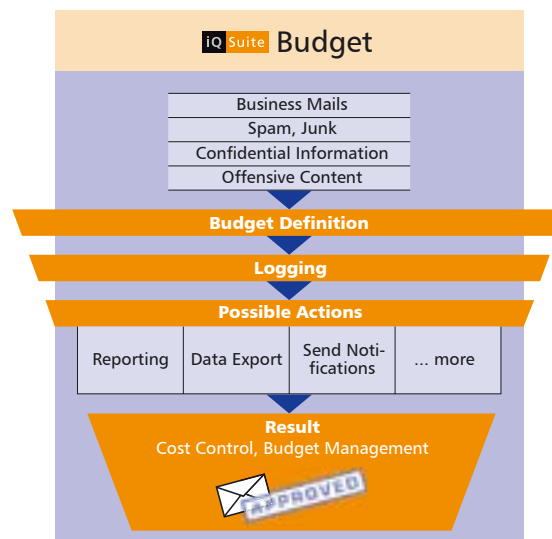


Accounting & Billing

iQ Suite Budget

More than just controlling e-mail costs.

- Analyzes all e-mail processed by the iQ.Suite.
- Evaluates e-mail volume according to defined cost centers, such as measuring memory usage and network load.
- Defines and structures e-mail budgets for users and user groups.
- Creates e-mail traffic log.
- Reporting based upon the drill-down principle.
- Reporting based upon type and size of file attachments, e.g. .pdf, .doc, or .xls.
- Creates individualized reporting templates and reports.
- Reports on e-mail volume, e.g. by user groups or user ranges, separately based upon internal and external addresses.
- Exports data into databases or files for use in other reporting tools.
- Reports e-mail costs with definition of different cost rates.
- Defines budgets for e-mail.
- Graphic display of reports in diagrams and overviews for management.





iQ Suite

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

E-mail Pre-processing

E-mail lifecycle management starts here. E-mail is prepared for transmission or for additional processing. Before delivery to the user's mailbox or sent outside the company, the e-mail undergoes a number of different verification and processing steps based on various criteria.

► **Problem:** You want to send critical information over the Internet by e-mail, while maintaining confidentiality.

Solution with Crypt: Centralized encryption makes it possible to set up safe e-mail communication from server to server, from endpoint to server, and from server to endpoint with minimal administrative effort. Crypt is transparent and meets requirements for end-to-end encryption.

► **Problem:** You are spending a lot of time and money to manage keys and/or certificates on the client servers.

Solution with Crypt: Centralized, automated key administration on the server or gateway significantly reduces administrative costs. Software and keys are not distributed to the clients. You can easily incorporate existing public-key infrastructures (PKIs) via LDAP.

► **Problem:** Encrypted or signed e-mails are potential risks, because they may contain viruses and undesirable contents.

Solution with Crypt: By checking file contents and attachments, even in encrypted and signed e-mails, Crypt works in combination with the Watchdog and Wall modules to guarantee comprehensive content security at all times.

► **Problem:** You need automatic, user-transparent support for the leading encryption standards.

Solution with Crypt: PGP and S/MIME are supported in parallel operation without any effort required on the part of the user. The encryption method is automatically selected based upon your company policies.

► **Problem:** You have no PKI, but want to use S/MIME for encryption.

Solution with Trust: To use S/MIME for encryption and signatures, you must have the corresponding X.509 certificates. You can purchase these from trust centers. It's easier with Trust: All the necessary certificates are easily generated and managed. Simply import the generated certificates into the Crypt module, and you can use S/MIME immediately.

► **Problem:** Transmission of e-mails with large file attachments regularly clogs your data transmission lines during peak business hours.

Solution with Smart: Scheduled transmission of e-mails with large file attachments as well as (de-)compression of file attachments reduces the load on your servers and networks. Smart effectively frees up your network resources, keeping available for other necessary tasks.

► **Problem:** Some of your e-mails contain legally binding information. You want to avoid making statements that could result in legal liability.

Solution with Trailer: The automatic integration of a recipient- and country-specific legal disclaimer into every outgoing e-mail reduces liability risks for employees and company officers at all levels.

► **Problem:** You want to keep your employees' e-mail signature lines in compliance with company rules and present a uniform appearance.

Solution with Trailer: The automatic integration of general and personalized e-mail signatures ensures that sender information will always be in accordance with your business conventions. You can easily configure personalization as desired by using directory information.

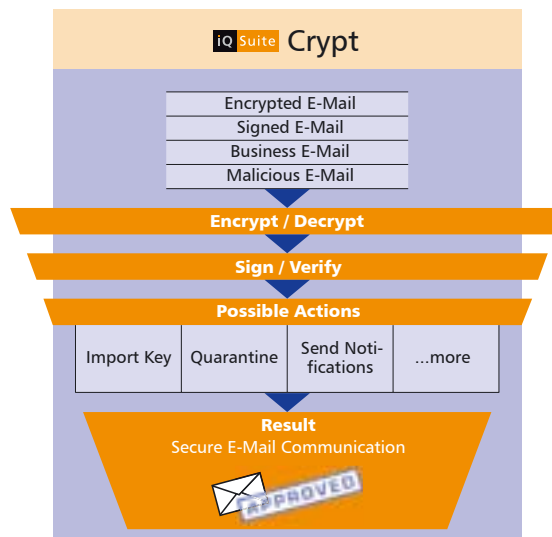
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



iQ Suite Crypt

More than just e-mail encryption.

- **Secure e-mail communication without the need to create your own PKI infrastructure.**
- **Minimal administrative expense.**
- **Simple and fast e-mail encryption – no user interaction necessary.**
- **Compatible with existing PKI structures.**
- **Checks encrypted e-mail for viruses and content when used together with Watchdog or Wall.**
- Server-based, centralized e-mail encryption.
- No software installation on client necessary.
- No training required for end-users.
- Parallel support of PGP, GnuPG and S/MIME.
- Centralized archiving of keys and certificates.
- Uses existing LDAP directories.
- Automatic import of new keys or certificates.
- Separate certificate management in a separate key database.
- Server-to-server encryption for setting up secure communication channels.
- Client-to-server encryption, e.g. for external end-users with client-based encryption from third-party vendors.
- Fully compatible with end-to-end encryption.



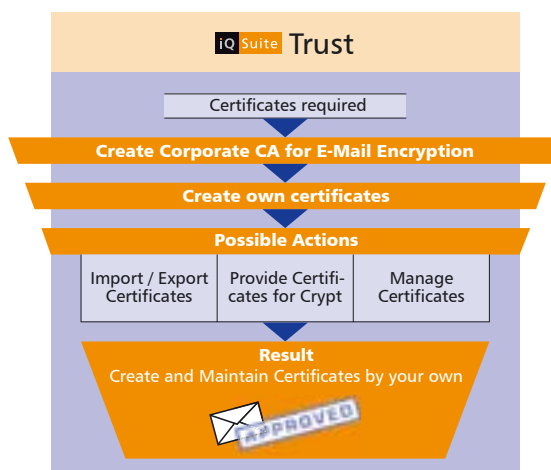


E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

iQ Suite Trust

More than just e-mail certificates.

- **Easy creation and maintenance of digital certificates.**
- **Professional key management to ensure confidential e-mail communication.**
- **Reliable validity monitoring for all certificates.**
- **Ideal supplement to Crypt: Centralized encryption and easy key management without an expensive PKI.**
- Trust serves as the basis for handling the tasks of a trust center and generating certificates.
- Creates X.509 certificates according to internal company policies.
- Monitors the validity of X.509 certificates.
- Creates separate public and private keys.
- Offline administration tool is independent of mail platform.
- RSA support up to 4096 bits.
- ECC support up to 256 bits.
- Supports the use of smartcard devices.
- Effective in combination with Crypt.



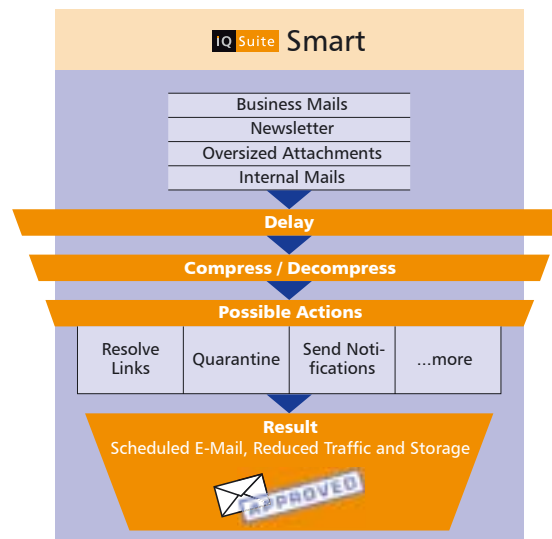
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



iQ Suite Smart

More than just e-mail preparation.

- **Reduces server/network load through scheduled e-mail transmission.**
- **Standardized conversion of e-mail attachments.**
- **Ensures a safe access to attachments by disclosing links.**
- High-volume or large e-mails can be scheduled for later delivery. This makes optimal use of server and network capacities.
- Attachments are decompressed and then compressed again when they arrive on the server (ZIP).
- User can schedule individual e-mail transmission times.
- Automatically converts e-mail attachments into standard formats such as PDF.
- Logical disclosure of links in e-mails for external transmission.



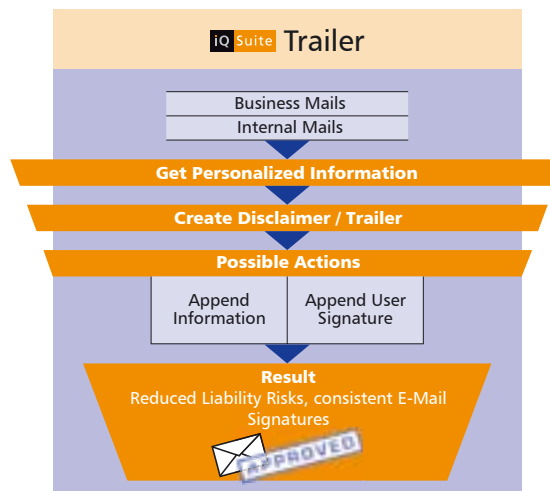
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

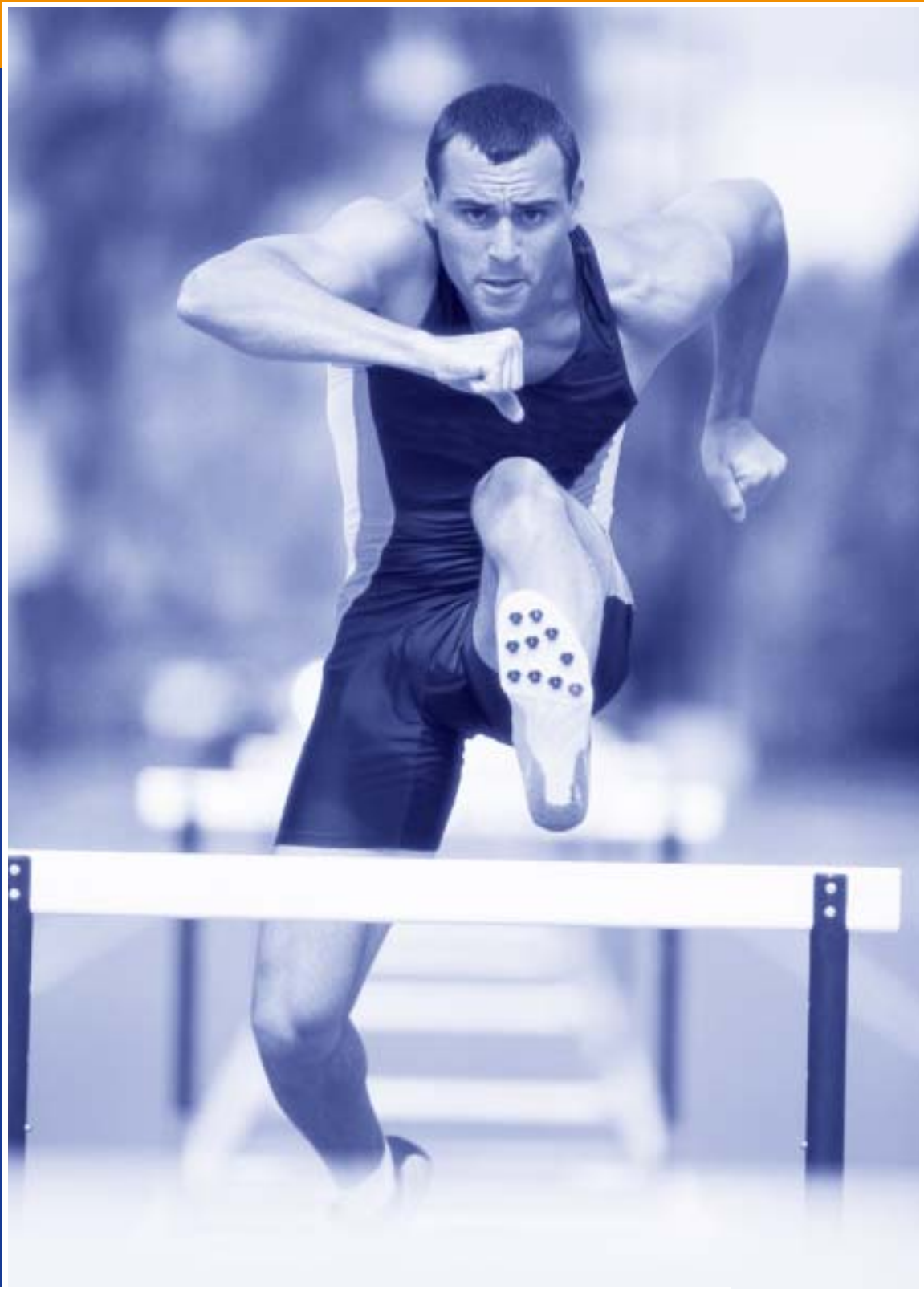


iQ Suite Trailer

More than just a legal disclaimer.

- **Centralized, parameter-driven e-mail signatures.**
- **Automatically adds company information and legal disclaimer to outgoing e-mails.**
- **Reduces company's liability risk.**
- Legal assurance through a standard liability disclaimer.
- Sender-/recipient-specific integration of personalized signatures, (e.g. by department).
- Multilingual trailers for different recipients.
- Integration of dynamic user information from the central e-mail address book.
- Time-based and rule-based use of boilerplate text, e.g. for marketing communications.
- Trailer can work with ready-made text signatures for consistent Corporate Design implementation.
- Supports multiple formats (HTML, text).
- User can select position of boilerplate text within the e-mail (top/bottom).
- Multiple boilerplate texts can be combined in one e-mail.
- Department managers can generate, activate, and update trailers.





iQ Suite

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

E-mail Firewall

E-mail firewall thoroughly examines pre-processed e-mails. All e-mail contents are checked for viruses and spam, and examined based on additional criteria. Dangerous or prohibited e-mails are blocked, and relevant business e-mails are safely delivered.

► **Problem:** New types of viruses and other attacks threaten your infrastructure every day.

Solution with Watchdog: Effective virus protection is absolutely essential for every e-mail system today. Running several of the leading scan engines in parallel operation increases your security.

► **Problem:** Dangerous and undesirable file attachment formats decimate resources and increase costs.

Solution with Watchdog: A graduated security concept for dealing with more than 200 data formats (e.g. .exe, .vbs, .mp3, .jpg, .avi) offers pre-emptive protection. Fingerprint technology is also used to safely detect all file types, even in archives. Your policies determine which e-mails and file types are classified as potentially dangerous and thus to be filtered.

► **Problem:** You want to make sure that you are protected from viruses and are able to filter out file attachments, even in encrypted e-mails.

Solution with Watchdog: A seamless combination with the Crypt module makes sure that even encrypted viruses and file attachments have no chance in your e-mail environment.

► **Problem:** You want to protect your e-mail users and infrastructure against the effects of spam.

Solution with Wall: The combination of different analysis methods permits a detection rate of up to 100 percent. Automated white and black lists ensure that business-relevant e-mails are detected and delivered. You also have optimal protection against "mail flooding attacks."

► **Problem:** You want to verify that your e-mail communication is more closely focused on business requirements.

Solution with Wall: Content analysis combined with sender/recipient lists, as well as automated white and black lists, result in time savings and protect against abuse. Undesirable communications can be proactively excluded. Wall prevents the unmonitored forwarding of business e-mails to private mailboxes at external service providers.

► **Problem:** You want to prevent pornographic and offensive content from being disseminated within your company.

Solution with Wall: Integrated image analysis with Xblock detects prohibited image attachments in real time, and prevents them from being disseminated via e-mail.

► **Problem:** You want to prevent the unauthorized transmission of confidential information and protect your intellectual property.

Solution with Wall: The use of text analysis and classification technology permits the detection and filtering of e-mails and file attachments with sensitive content. When Watchdog and Crypt are combined, unauthorized transmission prohibited by your company policies is no longer possible.

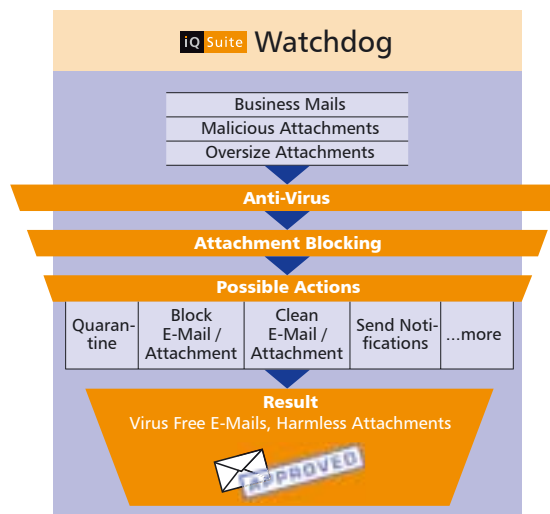
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



iQ Suite Watchdog

More than just virus protection.

- **Intelligent, centralized blocking of viruses and undesirable file attachments.**
- **Parallel operation with leading virus scanners possible.**
- **Protects against malicious code by using file pattern recognition.**
- Powerful virus scanner already integrated.
- Parallel operation of multiple virus scanners from different leading third-party vendors.
- Scans e-mail message text and attachments.
- Detects file attachments using unique, manipulation-proof file patterns (fingerprints).
- Users can define file restrictions through a combination of file name, extension, and size.
- Uses file restrictions in archives (e.g. zip, rar).
- Generates and uses internal file patterns to secure the exchange of current information (e.g. price lists, terms of business).
- Checks encrypted e-mails for viruses and content when used in combination with Crypt.



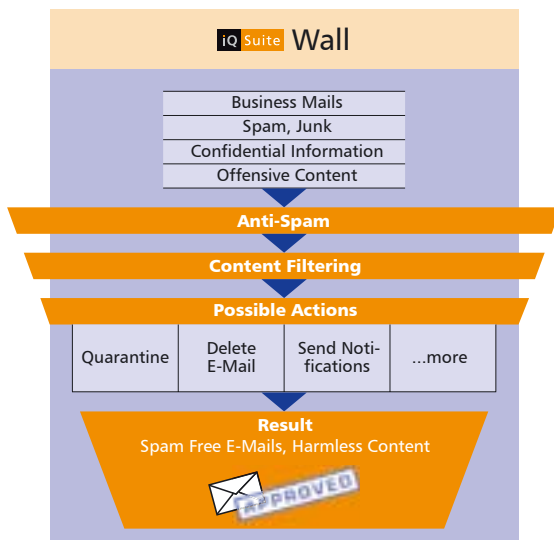
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



iQ Suite Wall

More than just a spam filter.

- **Reliably detects spam through intelligent, self-learning e-mail analysis (CORE).**
- **Analyzes all text, file, and image content within an e-mail.**
- **Prevents unauthorized transmission of sensitive or confidential information.**
- **Monitors and secures e-mail communication based on content and addresses.**
- Analyzes the entire content of an e-mail, including attachments (subject line, message text, file attachments).
- Checks for content that is prohibited, undesirable, or confidential according to company policy.
- Blocks e-mail from unwanted senders (spammers, mailing lists, etc.) as well as e-mails sent to undesirable recipients (e.g. competitors).
- Analyzes images for undesirable content (e.g. pornography) using the Xblock function
- Protects against mail flooding attacks (identical e-mails sent to multiple recipients within a given time period).
- Uses current spam pattern for rapid detection of new spammer tricks.
- User-specific administration of white and black lists to effectively block only undesirable e-mail.
- Specifies sender/recipient channels for dedicated e-mail communication.
- Centralized monitoring of encrypted e-mail through a combination of Wall and Crypt. This replaces client-based end-to-end encryption, which infiltrates centralized e-mail security checks.
- Flexible notification regarding blocked e-mails (direct or scheduled) to system administrator or to e-mail recipient/ sender.
- User-specific access to e-mails in quarantine.
- Centralized quarantine management is particularly efficient for enterprise/multiple-server environments.





iQ Suite

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

E-mail Classification

Accelerating to maximum speed. Classification and categorization of e-mail plays a decisive role in content-based handling within business processes. It is an essential component in e-mail lifecycle management, and can be deployed in many areas. Applications can include automatic organization and context-based archiving of contents, creating flexible delivery and distribution mechanisms, and automated indexing for e-mail archives.

► **Problem:** Manual distribution of incoming e-mail sent to general addresses such as info@company.com is tedious and time-consuming.

Solution with Wall and CORE: Automated pre-sorting and content-based delivery of incoming e-mail to the appropriate departments and employees. E-mail classification technology makes it possible to automatically distribute e-mail to any recipient address. Wall can be individually “taught” based upon your e-mail characteristics. It will then configure the system to deliver and forward e-mail to the responsible individuals or teams within your company.

► **Problem:** E-mails are delivered to employees without any structure or classification. The e-mail archive is not sorted.

Solution with Wall and CORE: Almost every user has an e-mail archive with a folder structure, although most people sort their e-mail manually. CORE technology provides users with automatically determined e-mail classification parameters, which are attached to the incoming message. This technology ranges from automatic sorting to assistance in prioritizing incoming e-mail.

► **Problem:** You want to store business-relevant e-mail in various logical archives, and eliminate the need for users to manually set keywords or indexes.

Solution with Wall and CORE: Using easily adaptable automatic categorization, you can archive e-mails in different logical archives, depending upon their content and origin. A (partially) automated definition of keywords based upon the classification results reduces user workloads and ensures uniform, standardized indexing.

► **Problem:** You want to make handling e-mail more efficient for your users, and more quickly assign responsibility for incoming queries.

Solution with Wall and CORE: Automatic categorization significantly increases response speed and improves customer service. Users can more quickly classify the contents of e-mail queries. With e-mail templates and other documents, users can respond more quickly or can forward a query to the right employee.

► **Problem:** Given the increasing volume of e-mail, you want to “separate the wheat from the chaff,” and make compliance-relevant e-mails pass through additional checks and approvals.

Solution with Wall and CORE: To comply with a variety of regulatory requirements, all affected e-mails must be subjected to the appropriate monitoring and archiving processes. To increase efficiency, irrelevant information must be sorted out from the enormous volume of e-mail. Reducing the volume of e-mail requiring processing to a manageable quantity, this approach can also be used for all e-mails, even if they will be further processed and archived in other business applications such as CRM, ERP, or ECM solutions.

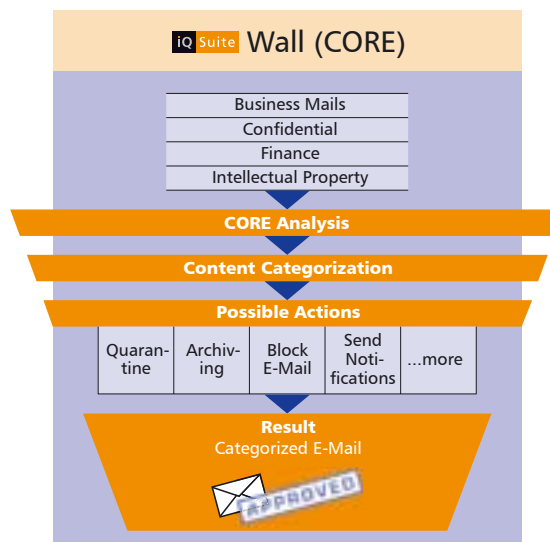
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



iQ Suite Wall

More than just e-mail sorting.

- **Intelligently categorizes and classifies e-mail based on a content check (CORE technology).**
- **E-mail Response Management optimizes internal workflows.**
- **Faster processing of customer inquiries.**
- **Prevents unauthorized transmission of sensitive or confidential information.**
- Creates company-specific e-mail categories.
- Classes are optimized by the CORE teaching capability, which uses small learning quantities.
- Automatically classifies e-mails into one or more categories (multiple classifications).
- Uses CORE, a statistical method based upon Support Vector Machines (SVM), to examine and automatically classify e-mails.
- Response management through defined classifications, such as customer support and automated forwarding of e-mail to qualified employees.
- Document protection: For example, all outgoing mails can be checked for company-relevant content, based upon corresponding categories. E-mail attachments can also be checked for content.





Content Recognition Engine (CORE)

CORE is a statistical method that uses Support Vector Machines (SVM) to classify e-mail. The CORE technology integrated into the Wall module analyzes e-mail with pinpoint accuracy and classifies it based upon your specifications. Spam, support queries, and customer questions can be automatically classified and processed as needed. With CORE, e-mail can also be automatically forwarded based upon content.



iQ Suite

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

E-mail Compliance

The challenge now is to “stay on the inside track.” The organization of internal e-mail-related workflows is increasingly governed by the need to comply with laws and regulatory compliance issues as well as internal company policies (corporate compliance). Reducing the risks associated with these multifaceted requirements is an integral component of e-mail lifecycle management.

► **Problem:** You want to fulfill regulatory compliance requirements such as SOX, HIPAA, GDPdU, etc., by checking all incoming and outgoing e-mail.

Solution with Bridge: Bridge supports seamless integration with a compliance system, and provides both pre-review mode (before delivery) and post-review mode (after delivery). Your individual policies, combined with automatic classification, guarantee that only business-relevant e-mails will be subjected to the review process. Classification results and additional information will be transferred to the compliance system and directly evaluated there. The interaction of iQ.Suite with your compliance system makes it possible to further process e-mail in compliance with the relevant laws, based upon the evaluation of each check result.

► **Problem:** Transmission of sensitive or confidential information via e-mail cannot be safely prevented.

Solution with Bridge: Transmission of suspect e-mails to a compliance application occurs proactively, before the e-mail is actually sent to a third party. Using the “four eyes” principle for security, e-mails being checked are stopped and placed into “Park” mode. Final transmission occurs only after the e-mail is released by an authorized person.

► **Problem:** To ensure compliance, you want to ensure that e-mails are checked, processed, and archived in accordance with the law, even during planned and unplanned absences.

Solution with Clerk: By specifying delegation rules and using absence management, you can make certain that your workflows and the associated regulatory control processes are safe. Previously defined actions are initiated for specific events based upon individual policies, and alternative business processes are activated.

► **Problem:** To comply with government or internal regulations, you must ensure that e-mails sent to specific persons and which contain sensitive or confidential contents are not forwarded or rerouted during their absence to unauthorized employees.

Solution with Clerk: Automatic classification of e-mail provides reliable detection of content and permits or prohibits forwarding or rerouting as necessary. Depending upon its content, e-mail can be rerouted to various authorized recipients.

► **Problem:** To maintain a high quality of service, inquiries received via e-mail must be processed and answered quickly, even when an employee in question is absent.

Solution with Clerk: Absence management can be activated at any time by the recipient, recipient’s administrative assistant, or other authorized personnel. The processes can be predefined and executed automatically. E-mail is processed in real time and customer satisfaction is increased.

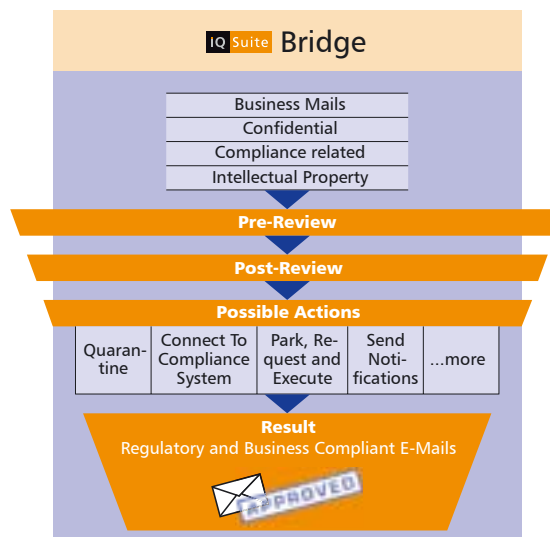
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



iQ Suite Bridge

More than just e-mail review.

- **Compliance with company policies for e-mail use.**
- **Full observance of and adherence to legal and regulatory provisions.**
- **Receipt and transmission of unauthorized e-mail content is blocked (“four-eyes” principle).**
- **Proactive pre-review:** E-mail is sent to a compliance system for review prior to delivery.
- **Post-review:** After delivery, e-mail is checked on a random sample basis or completely to ensure legal compliance.
- **Reroutes** incorrectly addressed e-mail based upon compliance specifications.
- **Post-review functions** guarantee seamless e-mail communication for audits.
- **Workflow principle:** E-mail is transmitted or forwarded only after release by authorized personnel based upon compliance requirements.
- **Archiving systems** are incorporated to enhance archiving functions.



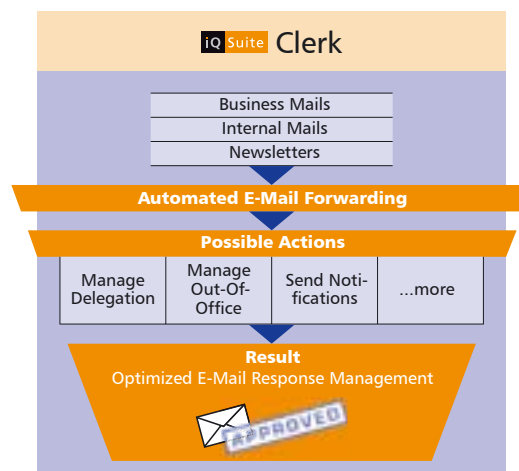
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



iQ Suite Clerk

More than just e-mail forwarding.

- **Forwards and processes important e-mail, even during the user's absence.**
- **Informs e-mail sender that the recipient is absent.**
- **Authorized user groups can manage absence rules.**
- **Guarantees that company policies on legal requirements are met.**
- Freely definable delegates and delegate groups.
- Prevents forwarding of confidential or personal e-mails.
- General rerouting of all or selected e-mails, e.g. from boss to secretary.
- Integrated into the iQ.Suite Portal.
- Authorized users can define forwarding settings for other users/user groups (e.g. if an employee is ill).
- Sends confirmation to absentee that delegate has read the e-mail.
- Internal and external e-mail forwarding is limited to authorized personnel.
- Central overview of all absences for authorized users.





iQ Suite

E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

E-mail Archiving, Retrieval, Retention

In the “final stretch” of e-mail lifecycle management, the focus is on archiving, administration, search and retrieval, as well as proper destruction of e-mail following the expiration of prescribed storage periods. Centralized storage of business-relevant e-mail can be implemented as an entry-level solution or in conjunction with an archiving system.

► **Problem:** You want to fully or selectively document your e-mail communication with business partners in order to monitor completeness, provide for follow-up, or make random checks.

Solution with Safe: Organized, traceable e-mail storage gives you constant access to information transmitted via e-mail. Using policies, you decide which business processes and communication partners should be included, and can specify access rights to archived e-mails.

► **Problem:** You want to safely archive your e-mail without purchasing a complete archiving system. Archived e-mails will be transferred into an archiving system later, however.

Solution with Safe: E-mails are centrally stored in clearly defined, logical archives when they are initially delivered. Multiple archives and search-and-retrieval archives are used. When you combine Safe and Bridge modules, you can transfer the e-mails archived in Safe into an audit-proof archiving system at any time.

► **Problem:** You want to set up e-mail journaling for selected persons, groups, or other users, and ensure that data remain confidential.

Solution with Safe: Using the policy settings, you specify the group of persons to be included in continuous journaling, and also specify access rights to archived e-mails. You can define which e-mails, if any, should be encrypted and supplemented with a digital signature. This guarantees that archived data cannot be modified. Selected personnel authorized to perform audits (e.g. for data privacy purposes) can monitor the keys being used.

► **Problem:** You want to combine the comprehensive functions and rule sets of the iQ.Suite with an archiving system for e-mail storage.

Solution with Bridge: The seamless integration of the iQ.Suite into leading archiving systems ensures efficient and appropriate e-mail archiving. Beginning immediately, only business-relevant e-mails will be archived, regardless of whether or not they are encrypted. Multiple archiving is prevented, and all irrelevant data are filtered out. This reduces the overall burden on the archiving infrastructure.

► **Problem:** You want to store all e-mail in an archiving system as soon as it is delivered, and thus reduce the load on your network infrastructure.

Solution with Bridge: As soon as an e-mail is delivered, file attachments can be removed and replaced with links to the archiving system. The data are saved only once in the archiving system, and are supplemented by index information from the e-mail classification. In contrast to scheduled automatic or manual archiving, you can guarantee seamless archiving of all e-mail.

► **Problem:** You want to comply with legal or internal company rules for e-mail archiving, and map this process based upon rules.

Solution with Bridge: The interface and integration module now makes it possible to set up e-mail archiving based upon defined policies for e-mail pre-processing, filtering, and classification. These capabilities provide a flexible, complete solution that meets all the various requirements, down to the last detail.

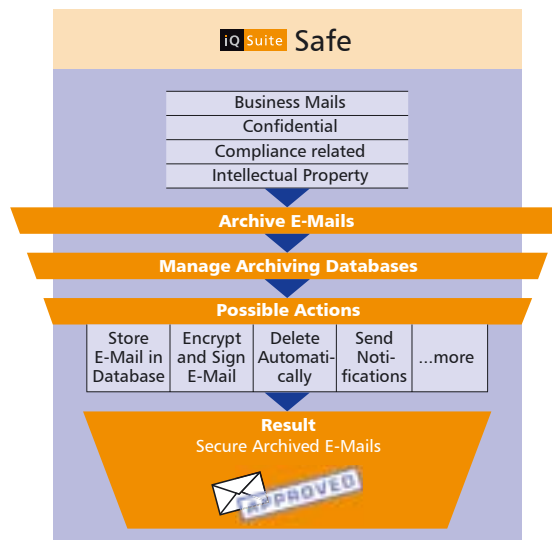
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



iQ Suite Safe

More than just e-mail archival.

- **Rule-based, centralized e-mail archiving and specialized databases.**
- **Seamlessly documents all e-mail traffic.**
- **Prevents subsequent manipulation and abuse of e-mail content.**
- **Saves the original e-mail.**
- Maintains a central log of incoming, outgoing, and internal e-mail, and stores it on central groupware servers/databases.
- Creates new journals based upon custom settings (size/time/thresholds).
- Automatically monitors available disk space.
- Sender-/recipient-specific e-mail archival.
- Enables encrypted archiving and protects against unauthorized access to the archive.
- Signed archiving to prevent manipulation of saved e-mails.

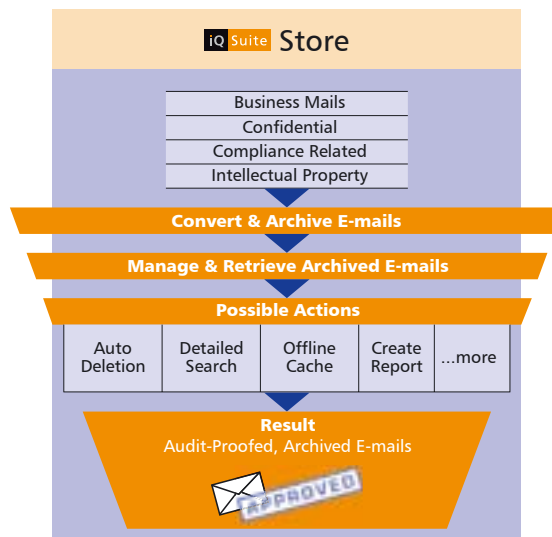


E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

iQ Suite Store

More than just e-mail archiving.

- **Intelligent e-mail archiving that's secure, reliable and legally compliant**
- **Centralizes archiving to drive down costs and free up resources**
- **Automates processes to improve e-mail/groupware system performance and availability**
- **Reduces complexity to enable efficient administration and intuitive access to archived content**
- **Increases data security to avoid down-time**
- **Offline availability for mobile users**
- Long-term archiving of e-mails and other documents
- Automatic conversion of document content and attachments to PDF or TIFF as desired
- Metadata storage
- Single-instance archiving for attachments
- Synchronous search and restore
- Inexhaustible rule-based archiving and search possibilities
- Freely configurable automated deletion settings
- Compressed archiving
- Detailed statistics



E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

iQ Suite Store

► **Challenge:** Our e-mail server is chronically short on storage. Server performance is constantly degrading. Backups rarely finish within their allocated time.

Solution: iQ.Suite Store offers across-the-board relief for your e-mail server, resulting in measurable performance improvements. Its rule-based approach lets you configure the archiving process to fit your business, reducing storage requirements and shortening backup durations.

► **Challenge:** Legal statutes and internal corporate policies are requiring us to securely archive all business-relevant e-mail for auditing purposes.

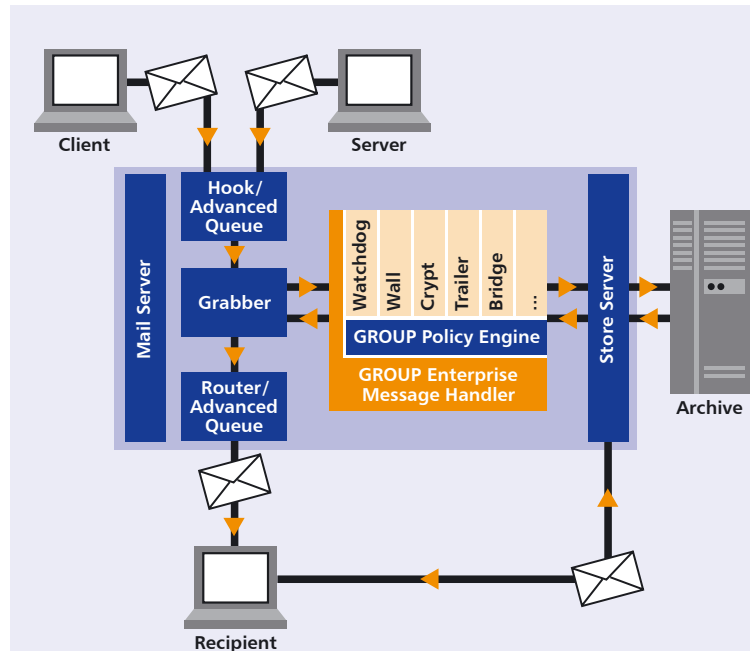
Solution: iQ.Suite Store securely archives all business-relevant data and provides intuitive, powerful search functions that allow crucial information to be restored at any time. Freely configurable deletion settings automatically purge data that is no longer needed.

► **Challenge:** Our existing solution redundantly archives identical e-mail attachments from multiple user mailboxes. This is quickly consuming our available storage.

Solution: iQ.Suite Store leverages an advanced Single-Instance Storage algorithm to ensure that identical attachments are only archived once. Optional compression of all archived data enables further reduction of storage requirements. Archiving in general becomes more efficient and costs less.

► **Challenge:** Our archiving solution is client-based. This is making it difficult for us to ensure that all business-relevant data gets archived. Worse, spam and viruses are now overloading our archiving system.

Solution: iQ.Suite Store's completely server-based process archives all business-relevant e-mail before it is delivered. Using iQ.Suite's rule-based policy engine, additional applications for spam and virus protection, encryption, filtering, etc., can be seamlessly integrated into the process to ensure that only business-relevant content is securely archived.



Technical Requirements

■ E-mail Platform

IBM Lotus Domino Server R5 / 6.x / 7.x
Microsoft Exchange Server 2000 (SP2+) / 2003

■ Operating System

Microsoft Windows 2000 (SP1+) / 2003

■ Hardware

NT File Systems (NTFS)
IBM Tivoli Storage Manager

Further archiving solutions on request.

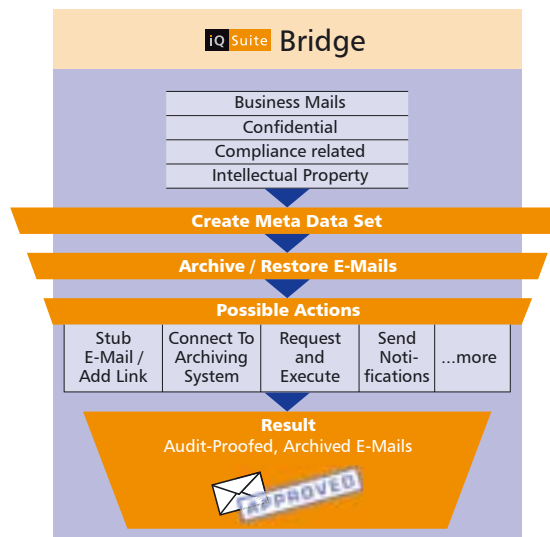
E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent Content Analyzing	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Based Routing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition		Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			



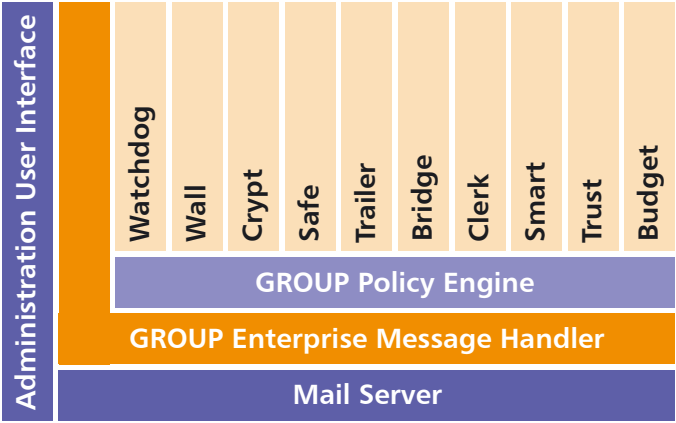
iQ Suite Bridge

More than just an e-mail interface.

- Long-term archiving based upon company policies and compliance with prevailing laws.
- Frees up valuable hard drive space on the messaging server.
- Seamlessly integrates e-mail into your business processes.
- Can be integrated into existing archiving systems.
- Integrates leading archiving systems into the e-mail system.
- Retrieves archived e-mails with an easy, interactive import function.
- Seamlessly archives e-mails prior to delivery through proactive or scheduled export.
- Replaces high-volume e-mail content with links to the archived data.
- Flexible metadata set and ability to pre-classify e-mail.
- Classical archiving system functions can be used: legally compliant, audit-proof archiving of data, indexing (metadata), search, and retrieval of data in the archive.



Technical Requirements



E-Mail Pre-Processing	E-Mail Firewall	E-Mail Classification	E-Mail Compliance	E-Mail Archiving	E-Mail Retrieval	E-Mail Retention
En-/Decryption	Anti-Virus	Intelligent	Pre-/Post-Review	Storage	Search	Long-Term Storage
Pack/Unpack	Anti-Spam	Content Analyzing	Delegation Management	Indexing	Restore	Automated Deletion
Signature	Image Recognition	Content Based Routing	Auditing	Content Management		
Disclaimer	Content Filtering		Risk Management			

iQ.Suite Technical requirements

E-mail platform

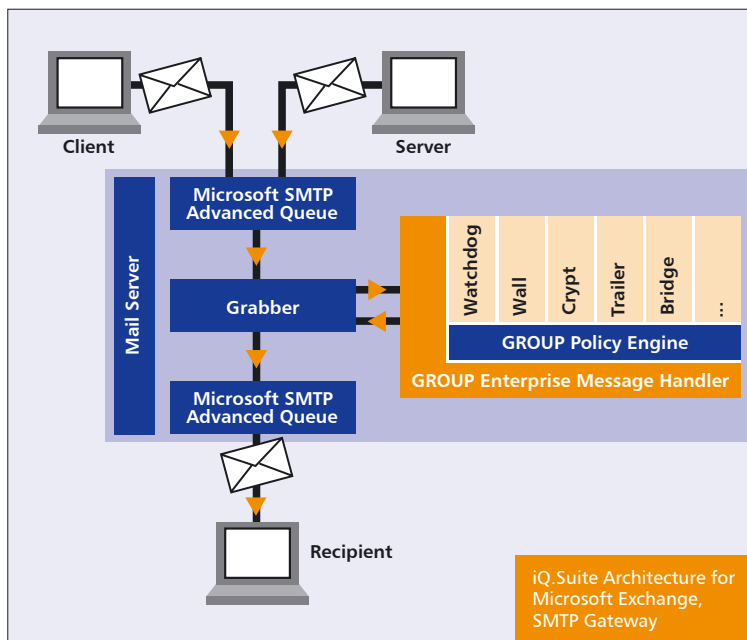
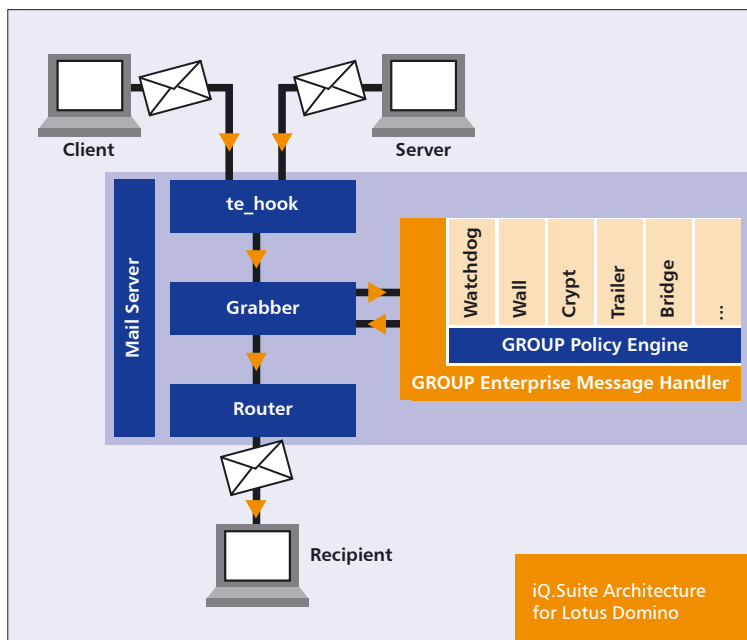
Microsoft Exchange 2000/2003
 Microsoft Windows 2000/2003 SMTP
 Microsoft ISA Server
 IBM Lotus Domino Server R5, 6.x, 7.x

Operating systems

Microsoft Windows 2000/2003 Server
 Microsoft Windows NT 4.0 Server
 Novell/SuSe Linux
 Red Hat Enterprise Linux
 SUN Solaris/SPARC
 IBM eServer pSeries AIX
 IBM eServer iSeries OS/400
 IBM eServer zSeries OS/390, z/OS, zLinux

Hardware

Please refer to the manufacturer's recommendations.
 Enhancements depend upon configuration and number of users.
 Hard drive capacity: 500 MB



Professional Services



We are always there for you.



Before and after your purchase, we provide individualized support to help you achieve your e-mail lifecycle management goals. Our staff of e-mail security experts has extensive industry experience to give you the best possible advice.

Service

We support you in the creation of more secure and efficient e-mail business processes. In consultation with you, we prepare a Needs Analysis, provide recommendations, and assist you in designing company-specific rule sets. Our team can answer your questions and solve your problems.

Hotline

Need help installing, configuring, updating, and maintaining our products? Our expert support team is happy to answer questions and support you on-site as needed.

Maintenance

E-mail lifecycle management is not a static condition, it is a dynamic process. Risks and requirements are changing constantly. Regular adaptation and enhancement of software is essential for e-mail lifecycle management. Get comprehensive service with a GROUP Technologies maintenance agreement. Our team of specialists will provide you with regular updates and new functions to guarantee maximum security and efficiency.

Professional Services – E-mail Audit



What percentage of your e-mail traffic is Spam?

How many e-mails have file attachments, and what are these attachments?

Is confidential company information getting into the wrong hands?

More than just e-mail analysis.

- **Comprehensive reports on e-mail traffic throughout the company**
- **Detailed analyses of all e-mail file attachments**
- **Identification and reporting of non-business content**
- **Identification and evaluation of e-mail costs**
- **Optimization of your e-mail platform**
- **Implementation of e-mail lifecycle management**

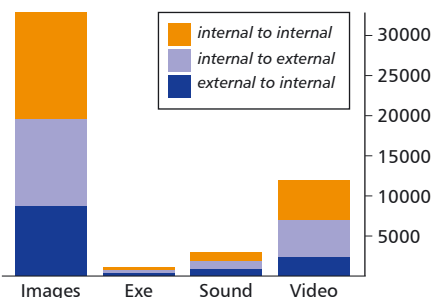
Recent studies have shown that spam, viruses, and the loss of confidential information result in enormous costs for many companies. Productivity losses, network downtime, and process costs add up to billions of euros every year.

With an e-mail audit by GROUP Technologies, you can record, analyze, and evaluate your e-mail traffic. Our experienced Professional Services Team will provide you with recommendations to improve your e-mail security, show you ways to increase efficiency, and advise you on all topics related to e-mail lifecycle management.

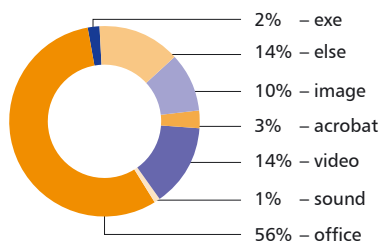
We will help you to install and configure your iQ.Suite, analyze data and performance, and make concrete, easy-to-implement recommendations. Your individual requirements will define the type and scope of the e-mail audit to be conducted.

The results of the e-mail audit will: reveal how many e-mails pass through your system; how this affects your resources; where there are risks of sensitive data loss; areas in which your company-wide e-mail policies are not being followed; potential damages that may result from imminent dangers; and the actual costs incurred by your e-mail system.

Inbound/Outbound vs. Internal Mail Traffic



Size of Attachments



Highlights

■ Comprehensive e-mail traffic reports

The e-mail audit highlights important factors and performance indicators related to your company-wide e-mail traffic, e.g. e-mail costs, number and size of e-mails, type and scope of file attachments, file size of attachments in relation to quantity, hourly volume and throughput statistics, as well as the quantity and type of file types being transmitted, such as videos, music, images, games, etc.

■ Measurement of spam and viruses

Learn more about the economic effects and damage caused to your company by spam and malicious code. Identify the quantity and types of dangers that threaten your e-mail platform. You can use the results of the e-mail audit as a valuable basis for decision-making on practical investments in e-mail lifecycle management, and to improve your company policies. This will reduce your costs and increase productivity.

■ Informative reports

You will receive the complex data analyses in a comprehensive and easy-to-understand format, with diagrams, graphics, and tables. These will give you a quick overview of how your e-mail system is currently being used, and where there are still potential areas for improvement.

■ We are at your side

An e-mail audit by GROUP Technologies is more than just a standardized analysis. Our Professional Services Team works on-site together with you to determine your individual requirements, and optimizes your e-mail system to help you achieve significant competitive advantages through increased efficiency.

The e-mail audit at a glance

■ Day 1: Project definition

Our Professional Services Team consults with you to determine your requirements, review your e-mail platform and environment, and define objectives.

■ Day 2: Installation and configuration

Our Professional Services Team installs the analytical software and configures the system rules based upon your requirements.

■ Day 3: E-mail data preparation

Our Professional Services Team uninstalls the analytical software, prepares the data analysis, and restores your original system status.

■ Day 4: Report preparation

Our Professional Services Team prepares detailed e-mail analyses and generates reports for an informative, results-oriented presentation.

■ Day 5: Recommendations

Our Professional Services Team presents the results of the e-mail audit and makes recommendations for improving security, efficiency, and the cost situation on your e-mail platform.



Partner Program



Successful partnerships.



Seize the opportunity to grow along with GROUP Technologies.

As a GROUP Technologies Business Partner, not only will you profit from our attractive product portfolio, you will also receive comprehensive support from GROUP Technologies.

With our customized partner training program, you can gain a decisive competitive advantage in expertise and knowledge.

A uniform global partner program establishes the basic framework for collaboration and creates the best foundation for shared success.

The GROUP Partner Program was developed specifically to support you in developing new sales opportunities, acquiring new clients, and maximizing profits. In this program, we provide you with expert advice and resources that are precisely adapted to the needs of your market segment and business model.

Partnerships play an important role in our business. We want to work with you to acquire new clients, and to support them as they create e-mail business processes and implement e-mail lifecycle management.

Sales cooperation

- Cooperation agreements and specification of sales goals
- Regular sales and target forecasts
- Specialization in the sale of the iQ.Suite

Marketing support

- High margins on list prices and favorable terms when purchasing software for internal use
- Active sales support
- Dedicated account manager
- Forwarding of qualified inquiries
- Technical support and training
- Listing of partner on the GROUP web site, with a link to the partner's web site
- Logos, graphics, presentations, and documentation provided
- Joint PR activities
- Supply of advertising materials

- Participation in GROUP Partner Incentive programs
- Exclusive online access to GROUP Technologies' Partner.Net
- Development of joint activities and campaigns

Training and certification program

Sharing information and knowledge is a central element in our concept of good partnership. We provide regular training sessions to make sure that our partners meet the quality standards for consulting and expertise demanded by the market. Participation in the multilevel GROUP Technologies certification program guarantees and documents knowledge and experience in working with the iQ.Suite and e-mail lifecycle management. Regular product information sheets, release updates, and newsletters on relevant topics complete the spectrum of services offered.

References



More than 6 million users at 2,000 companies worldwide protect and organize their systems with GROUP Technologies products.



Security is a matter of trust. Over 40% of the top 100 German financial services companies rely on our iQ.Suite. Our clients include many well-known companies from every industry sector.

Manufacturing

Abbott, Germany, worldwide
AGIP Austria, Austria
Bunge North America, USA
Coca-Cola Icecek, Turkey
Debitel, Germany
Diehl Informatik, Germany
Haniel Textile Services International, Germany
Heineken, Netherlands
Honda, Europe
Hutchinson Technology, USA
Kingston Technology, USA
Linde Gas, worldwide
MAN B+W Diesel, Germany
Mercedes-Benz, USA
Miele, Germany
Scania Deutschland, Germany
Unipart Advanced Learning Systems, UK

Financial services companies

ABN Amro, Netherlands, worldwide
ALLIANZ, Switzerland and Austria
Bank One, USA
Commonwealth Bank, Bahamas
Crédit Agricole Indosuez, Luxemburg
Danish National Bank, Denmark
Deutsche Bausparkasse Badenia, Germany
Deutsche Bank, Germany, worldwide
Deutsche Börse, Germany
Ernst & Young, Germany, worldwide
Fiducia, Germany
GAD, Germany
HSBC Trinkaus & Burkhardt, Germany
MLP Finanzdienstleistungen, Germany
Raiffeisen Datennetz Gesellschaft, Austria
Royal & Sun Alliance, UK
SEB, Germany
Société Générale Bank & Trust, Luxemburg
Sparkassen-Finanzgruppe, Germany
Swiss Re, worldwide
Sumitomo Bank, UK, USA
Yapi Kredi Bankasi, Turkey

Service

Atos Origin, Germany
Anderson Merchandisers, USA
Apria Healthcare Group, USA
Bayhealth Medical, USA
DFS Deutsche Flugsicherung, Germany
Edeka, Germany
E-Plus Mobilfunk, Germany
Enpoint Research, Canada
Marconi Selenia Communications, Italy
PWC Deutsche Revision AG, Germany
Singapore Airlines, worldwide
Telegraaf Media ICT, Netherlands
Terra Networks, Spain
TV Azteca, Mexiko
Thames Water, UK
United Health Services, USA
WAZ Mediengruppe, Germany

Public institutions

Bundesversicherungsanstalt für Angestellte, Germany
Centre Informatique de l'Etat, Luxemburg
City of Heidenheim, Germany
Freie Universität Berlin, Germany
Hungarian Tax Office, Hungary
Kansas City, USA
Ministry of Justice, Slovakia
Southwest Florida Water Management District, USA
Translation Centre for the bodies of the European Union, Luxemburg
US Customs, USA

Customer Success Stories



Join the many who rely on the iQ.Suite from GROUP Technologies.





The challenge

Bayhealth is the second largest healthcare system in the state of Delaware (USA) with over 2,400 employees, 391 hospital beds, and a medical staff of over 350 physicians. It's an environment in which the electronic transmission of medical and patient information is on the rise. So too is the proliferation of cyberattacks in the form of NIMDAs and Code Reds that are crippling networks worldwide. Protecting patient and medical information from malicious intent is of paramount importance to leading healthcare providers such as Bayhealth. Of equal importance, is the need for Bayhealth to become compliant with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA requires healthcare providers to ensure secure and private electronic transmission of patient records.

The optimal solution

To address a broad range of e-mail security issues that go beyond mere anti-virus protection, Bayhealth purchased the complete iQ.Suite for comprehensive e-mail security as iQ.Suite can handle enterprise concerns related to legal liability, information security, and business uptime. It safeguards Bayhealth's Lotus Domino platform and its 750+ users from threats and vulnerabilities from e-mail and Internet communication.

iQ.Suite gives Bayhealth a highly flexible, configurable and scalable solution that meets the organization's current and future security requirements.

The benefits

Through deployment of Wall, Watchdog, and Trailer, Bayhealth is able immediately address e-mail security concerns aimed at: stopping harmful viruses and e-mail attachments from entering the network; protecting users from spam and junk mail; safeguarding the enterprise from legal liability; and preparing for HIPAA compliance.

The iQ.Suite's unique and extensive rule-based functionality provides maximum safety through the use of intelligent control mechanisms for scanning e-mails and databases. Rule sets, which can be mapped to organizational and IT policies, are configured for every required protection function and are adaptable depending on user, group, or domain. Therefore, Bayhealth can map its e-mail security to organizational policies.

The future

iQ.Suite's modularity enables Bayhealth to keep pace with evolving business requirements and increase the scope of their HIPAA compliance. For example, with the combined deployment of Crypt, Watchdog, and Wall, Bayhealth can benefit from user-transparent, centralized e-mail encryption with simultaneous central virus protection and anti-spam capabilities.

As Bayhealth's e-mail community grows, it will be able to customize e-mail legal disclaimers by department or specialty with Trailer. With Safe, Bayhealth will have centralized archival of all electronic business processes, which will increase its protection from legal liability. And, Wall can deliver added protection and an advanced solution to protecting users from unwanted image files – not only by file type but also by actual content. In real time, Wall effectively detects and blocks objectionable graphical content and safeguards against breaches in confidentiality from internal or external e-mail misuse.

With iQ.Suite, Bayhealth is effectively executing a corporate e-mail strategy aimed at protecting the confidentiality of patient records and increasing hospital efficiency.



Miele

The challenge

Since its founding in 1899, Miele has become a model for pioneering achievements as a manufacturer of electrical household appliances. Miele is also well-known for the good relationships it maintains with its business partners. In these relationships, many of the company's departments, such as sales, product development, manufacturing, and purchasing, exchange increasingly large volumes of confidential customer information via e-mail. Miele wanted to improve the protection of its e-mail communications. It was looking for an integrated solution that was easy to manage and use, and which also provided first-class security.

The optimal solution

"GROUP Technologies' iQ.Suite won us over with its modularity and its flexibility," says Ralf Berhorst, who is responsible for Miele's messaging infrastructure. With the iQ.Suite, GROUP Technologies offers an integrated solution for a number of security-related core topics, such as checking of file types, virus check, encryption, and content check for e-mails and file attachments.

Because iQ.Suite Crypt supports S/MIME, PGP, and GnuPG as encryption standards, Miele can be particularly flexible when setting up its rules. This is an important prerequisite for a company with many partners. The module also provides an enormous administrative benefit because of its centralized, server-based encryption. If encryption had to be performed on each client, then the server-based content and virus check would no longer be possible, because e-mails would already be encrypted upon arrival.

The benefits

Most importantly, e-mail communication at Miele has become much more secure because of e-mail encryption. The company can now also perform simultaneous server-based e-mail content checks. All of the necessary processes take place on the e-mail servers, and thus require no additional expense for user training. This reduces costs significantly. Monitoring of incoming and outgoing e-mail ensures that it is free of viruses, spam, and confidential information. This also frees employees from the tedious process of cleaning spam e-mail out of their inboxes.

The future

Ralf Berhorst sums it up as follows: "We have been very impressed by GROUP Technologies and the iQ.Suite, primarily because of their flexibility. They have fulfilled our security requirements in every respect, from adaptability to changing requirements and future threats to scalability and the seamless integration of additional iQ.Suite products. We have found GROUP Technologies to be a partner who fits ideally into our corporate philosophy of 'always do it better.' As a global company, this is a very important aspect for us."

Swiss Re



The challenge

The Swiss reinsurance company Swiss Re was searching for an e-mail solution that could minimize the costs associated with electronic attacks and reduce productivity losses. "We urgently needed stable products that could filter incoming spam, check e-mails for their content, provide optimal virus protection, and also perform e-mail encryption," explains Jens Mathiessen, Senior System Engineer/ Groupware Services at Swiss Re.

The optimal solution

When searching for appropriate solutions, Swiss Re decided to use the iQ.Suite as a comprehensive security package for the leading e-mail platforms. The IT managers at Swiss Re selected iQ.Suite Watchdog. This application checks and cleans e-mails before they are stored on the e-mail servers. It also detects viruses and worms, and filters file attachments based on various criteria. The company also purchased Wall, which protects against spam such as junk e-mail, advertising e-mail, and hoaxes. Crypt was also selected because it could guarantee confidential communications.

The benefit

For Swiss Re, the advantages of the iQ.Suite were obvious. Centralized administrative capability and completely server-based operation significantly reduce administrative and maintenance costs. This means that the company no longer needs to install the software on every PC. Watchdog detects a number of different file types based on unique digital fingerprints. Using these, it can identify and block dangerous files. It also prevents manipulation of files. Wall is used for additional content checks. This module uses complex text analyses to prevent the transmission or receipt of offensive content, and filters information based on specific criteria.

For Swiss Re, the decisive factors in choosing Crypt were the savings in user training and support. Crypt is completely server-based and user-transparent. The most convincing argument, however, was the ability to combine the encryption software Crypt with other iQ.Suite modules, to ensure both encryption and comprehensive content security at all times.

The future

Mathiessen notes that "for companies who seeking a powerful complete solution, we recommend that they consider not only the product itself, but also other aspects. In addition to having outstanding technology, factors such as support, flexible licensing conditions, and a synergy between software vendor and customer also play an important role. We look forward to further collaboration with GROUP Technologies."

About GROUP Technologies



GROUP Technologies is a world leader in e-mail lifecycle management. The company's fully integrated iQ.Suite products ensure efficient security and effective organization of e-mail, from encryption, virus protection, and spam filters to e-mail classification and secure archiving.

The iQ.Suite is modular, fully scalable, and offers a high degree of investment security. The modules are completely server-based, can be centrally administered at a low cost, and are available for Lotus Domino, Microsoft Exchange and SMTP platforms.

With the iQ.Suite, companies can reduce costs, optimize the performance of their e-mail environment, and increase productivity. GROUP's clients include many well-known companies such as Deutsche Bank, Ernst & Young, Honda, Heineken, and Miele. More than 6 million users at 2,000 companies worldwide protect and organize their systems with GROUP Technologies products.

GROUP Technologies is headquartered in Karlsruhe/Germany. It maintains a subsidiary in the USA, and distributes its products internationally, both directly and through partner companies.



Still have questions?



Talk to us!

We can help you make your e-mail safe and efficient.

Please call us at

Fon +49 (0)721-4901-0

Fax +49 (0)721-4901-199

or simply send an e-mail to:

info@group-technologies.com

© GROUP Technologies AG. All rights reserved. GROUP Technologies and iQ.Suite are trademarks of GROUP Technologies AG and/or trademarks registered by GROUP Technologies AG in certain countries. All other brand names and product names are registered trademarks of their respective owners.

All product descriptions are merely of a general and descriptive character. They are to be understood neither as assurances of specific properties nor as statements of guarantee or warranty. The specifications and design of our products may be changed at any time without prior notice, particularly in order to incorporate technological advances.

GROUP Technologies AG assumes no explicit or implicit warranty for quality, execution, adherence to normal commercial practice, or suitability for a specific purpose.

Your authorized GROUP Technologies Partner

**Worldwide Headquarters
GROUP Technologies AG**

Ottostrasse 4
76227 Karlsruhe / Germany
Fon +49 (0) 721-49 01-0
Fax +49 (0) 721-49 01-199
info@group-technologies.com
www.group-technologies.com

**North American Headquarters
GROUP Technologies**

321 Fortune Boulevard
Milford, MA 01757 / USA
Fon +1 508-473-3332
Fon 877-476-8755 (US and Canada)
Fax +1 508-473-9940
info.us@group-technologies.com
www.group-technologies.com

