Intercepting and reading an email is not hard task even for malefactors-beginners. In order to protect your confidential info from security risks related to email exchange, you need to upgrade your security and utilize enhanced control and protection tools.

Main problems that may occur upon sending files through email:

1. Unsanctioned interception and modification of emails.
2. Reliability and availability of the service as a whole. Errors, such as typing in an incorrect address or destination mix-ups, can put data sent via email at risk.
3. Data is susceptible to malware.
4. Data can be compromised due to invalid format or user's actions that might compromise security system of email client or server.
5. Legal issues: the need to check the source of a message, etc.
6. Measures required for controlling remote access to email.

It means that we need to solve the following problems:

1. Form a complex approach towards file transfer security.

+44 20 7183 5820

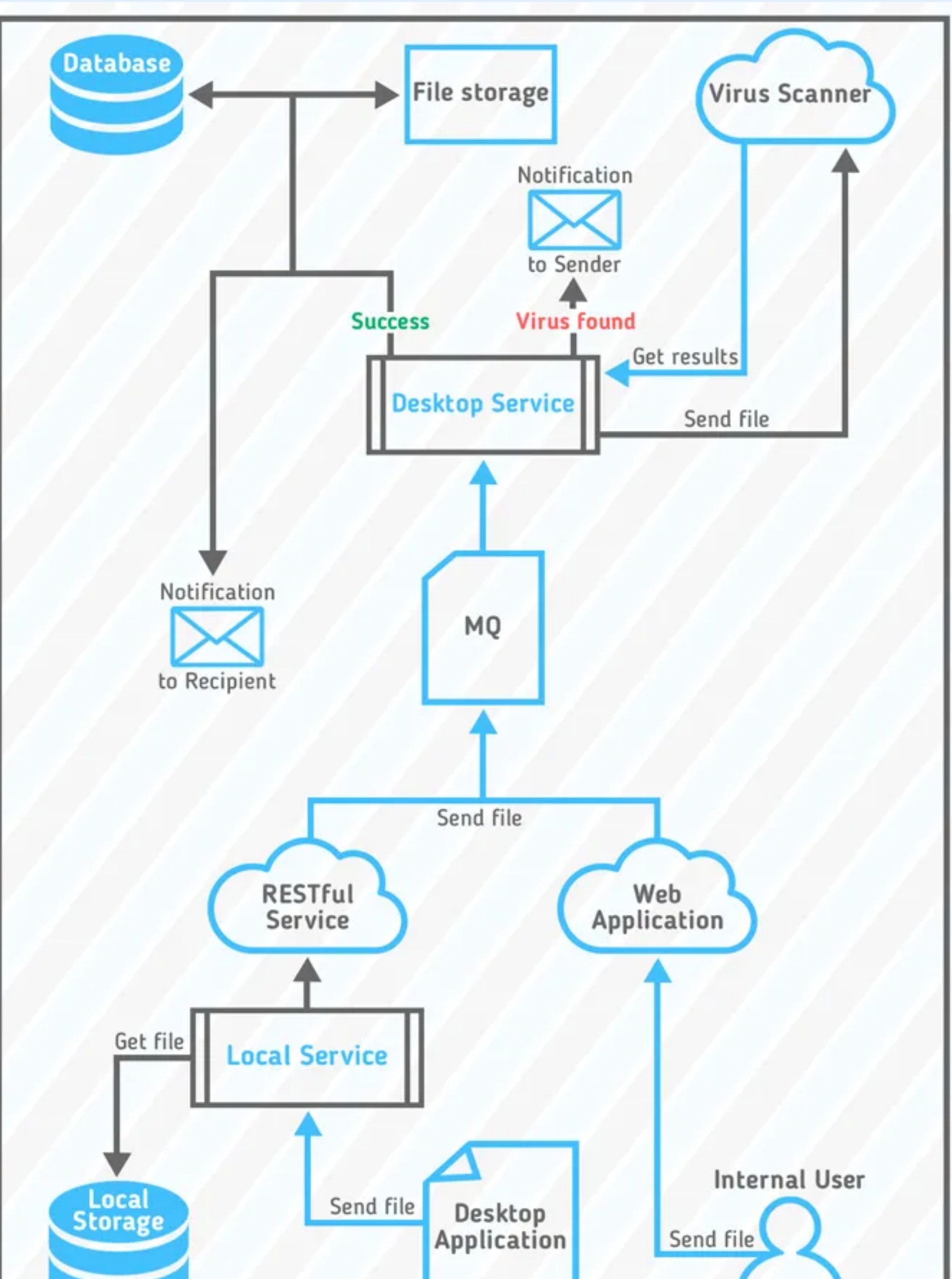
info@magora.co.uk
sales@magora.co.uk

2. Check content of files and messages for errors and malware.
3. Block leaks of confidential info in real time.
4. Security policy must comply with the law and industry standards.
5. All transferred files must be revised by the system admin on a regular basis.

General scheme of safe data exchange

Picture 1 schematically demonstrates the way the app works. According to this scheme, files can be sent by both internal and external users (with limitations). Each message is checked for malware and errors, and it also must meet size and quantity limitations. If a sender is an external user, an email must be revised and approved by the admin as well. Each email is signed with a Digital signature. It helps to eliminate the chance of interception. Upon receiving an email each user must be authorised with a one-off password sent through SMS. Each file has a limited receiving period. After it runs out, file will be encrypted and available only to the system admin. Upon detecting incorrect data, receiving and non-receiving files all parties involved get notifications. Usage of message and service queuing allows reducing database load and parallelizing processes run on the server.

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk


Database
File storage
Virus Scanner
Notification
to Sender
Success
Virus found
Get results
Desktop Service
Send file
Notification
to Recipient
MQ
Send file
RESTful Service
Web Application
Get file
Local Service
Local Storage
Send file
Desktop Application
Internal User
Send file

Picture 1 - General scheme of the software complex

Final points

Main criteria for a Security System evaluation:

- Compliance with requirements applied to High Load Systems
- Protection from all sorts of modern threats
- Compliance with the law
- Simple and intuitive User Interface

Described approach towards security allows distributing info swiftly and securely. It's also flexible, so it can be easily used by any organization.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk