

## Your benefits

- All in one: protection against spam, anti-virus, outbreak filter, encryption
- Advanced malware protection: global, cloud-based sandbox protects against unknown ,zero-day' malware
- Self-service portal for administrators with access to spam quarantine
- High-availability due to redundancy; with backup and central management
- Comprehensive service by indevis: setup and design, service desk, reporting
- Scalable costs, investment shift from CapEx to OpEx



## DO YOU WANT TO KNOW MORE?

Your personal contact person will be happy to advise you and discover together with you what concept bestfits your needs.

+49 (89) 45 24 24-100  
sales@indevis.de  
www.indevis.de

## INDEVIS E-MAIL SECURITY FULL SUPPORT FOR YOUR E-MAIL SECURITY

E-mails are comparable to a simple postcard in terms of security and confidentiality of their contents. The current situation demonstrates that the challenges regarding spam and e-mail encryption remain as crucial as ever for many companies and organizations. For anti-spam and malware protection, indevis offers a comprehensive protection service based on market-leading technology: *indevis E-Mail Security*.

### ONLY POSITIVE MESSAGES WITH INDEVIS E-MAIL SECURITY

The indevis systems excel with a very high rate of spam detection. The superb performance is primarily achieved by the dynamic registration in a global database of IPs that send spam mails. Each IP address that sends a mail is assigned a rating in the database. Based on a global inspection of the trustworthiness of e-mail senders, legitimate senders can be effectively distinguished from senders of spam. Depending on the rating in the database, our systems either accept or reject e-mails.

### VIRUS PROTECTION AND OUTBREAK FILTER INCLUDED

*indevis E-Mail Security* includes the powerful Sophos anti-virus engine. Combine with your existing anti-virus solution to protect your organization against computer viruses at two levels. An integrated virus outbreak filter grants protection in the event of virus outbreaks by means of proactive filter policies while adequate signature files are not yet available for anti-virus products. Suspicious e-mails are stored in a quarantine folder and scanned again after a signature update before they are dispatched (with a delay) or deleted for good.

### ADVANCED MALWARE PROTECTION

Suspicious e-mails and e-mail attachments are checked using a global hash code database. Any e-mails or e-mail attachments that are not recognized are sent to a cloud-based sandbox. The sandbox method enables new and unknown malicious code (malware) to be detected. This is a unique protection against targeted zero-day attacks in which unknown malware is used to attempt to compromise companies.



## ENCRYPTED E-MAILS TO MEET THE STRICTEST SECURITY REQUIREMENTS

To meet the highest safety demands, the *indevi*s E-Mail Encryption add-on – a separate managed security service – enables the exchange of encrypted e-mails according to the S/MIME standard using a private key / public key infrastructure. The communication between companies and their business partners and clients who do not deploy their own encryption solutions is implemented by means of a cloud storage area, the so-called messenger portal. Senders send their encrypted e-mails as usual, but the recipients receive the messages as file attachments that can only be opened and viewed using a password-protected link set up using a web browser. The recipients also have the option of replying to the mails in encrypted form.

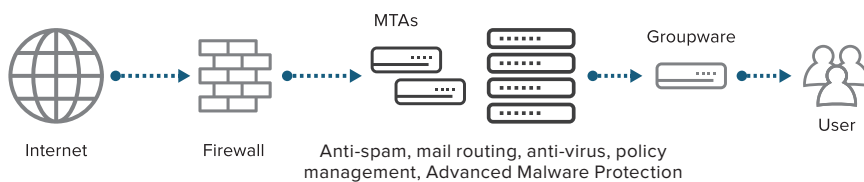
## DO-IT-YOURSELF USING THE SELF-SERVICE PORTAL

*indevi*s operates a web-based self-service portal through which clients of the *indevi*s E-Mail Security service can directly view their mail logs with a user login. The portal is made available to technically competent users and administrators to inspect incidents and examine e-mail histories. There are comprehensive search functions to track the progress and location of e-mails – for example, by searching for sender and recipient addresses, mail headers and subject lines.

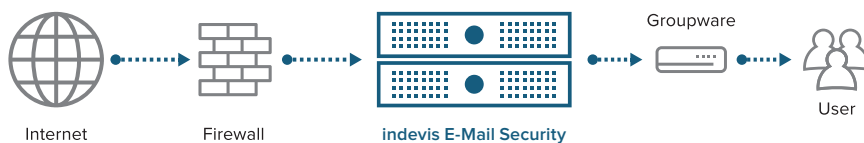
## DATA SECURITY AND DATA COMMUNICATION

E-mails are always transmitted using the SMTP protocol. *indevi*s supports encryption of the transmission by means of TLS (Transport Layer Security). *indevi*s always provides and supports encryption. The *indevi*s systems work with a valid certificate issued by an accredited Certificate Authority (CA). They also accept self-generated and non-accredited certificates used by the opposite side. In such cases, although the communication is encrypted, the integrity of the opposite side is not validated. Depending on the opposite side, e-mails can also be sent without encryption.

### Without *indevi*s E-Mail Security



### With *indevi*s E-Mail Security



Would you like to get to know *indevi*s E-Mail Security? We would be happy to present our service to you in a demo session and explain the benefits of a clean and secure e-mail communication solution.

## About *indevi*s GmbH

Since 1999 *indevi*s GmbH, ISO 27001 certified, has been providing IT security, datacenter and network solutions, accompanied by professional consulting, management and support services. In doing so, *indevi*s fully meets the demands and requirements set out by the economic sector and public authorities and higher education institutions.

As one of Germany's leading managed security service providers, *indevi*s is the partner for IT security and network technology for companies of all sizes and in any sector – after all, IT security is not a given, but rather has to be strategically planned.

*indevi*s offices are located in two cities in Germany: Munich and Hamburg. Additional staff members work at a number of other locations distributed throughout Germany.



*indevi*s GmbH

Irschenhauser Straße 10  
81379 München

Tel. +49 (89) 45 24 24-100  
Fax: +49 (89) 45 24 24-199

sales@indevi.de  
www.indevi.de