

## Ihre Vorteile

- All-in-one: Spam-Schutz, Anti-Virus, Outbreak-Filter, Verschlüsselung
- Advanced Malware Protection: globale, cloud-basierte Sandbox schützt vor unbekannter „Zero-Day-Malware“
- Self Service Portal für Administratoren mit Zugriff auf Spam-Quarantäne
- Hochverfügbarkeit dank Redundanz; mit Backup und zentralem Management
- Rundum-Service durch indevis: Setup und Design, Service Desk, Reportings
- Skalierbare Kosten; Investitions-Verschiebung von Capex zu Opex



## SIE WOLLEN MEHR ERFAHREN?

Ihr persönlicher Ansprechpartner berät Sie gerne und findet mit Ihnen heraus, welches Konzept am besten zu Ihnen passt.

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

## INDEVIS E-MAIL SECURITY KOMPLETTBETREUUNG IHRER E-MAIL-SICHERHEIT

Eine E-Mail ist in Bezug auf Sicherheit und Vertraulichkeit ihres Inhalts vergleichbar mit einer Postkarte. Die aktuelle Situation zeigt, dass die Herausforderungen Spam-Abwehr und E-Mail-Verschlüsselung für viele Unternehmen und Organisationen unverändert wichtig sind. indevis bietet beim Thema Anti-Spam und Malware Protection einen umfangreichen Schutz-Service auf Basis einer marktführenden Technologie: *indevis E-Mail Security*.

### NUR GUTE NACHRICHTEN MIT INDEVIS E-MAIL SECURITY

Die indevis-Systeme zeichnen sich durch eine sehr hohe Spam-Erkennungsrate aus. Diese hervorragende Leistung wird primär über die dynamische Registrierung spamversendender IPs in einer globalen Datenbank erreicht. Jede mailversendende IP-Adresse bekommt in dieser Datenbank ein Rating. Aufgrund dieser globalen Überprüfung der Vertrauenswürdigkeit von E-Mail Absendern lassen sich legitime Absender von Spam-Sendern wirkungsvoll unterscheiden. Abhängig vom Rating in dieser Datenbank nehmen unsere Systeme E-Mails an oder lehnen sie ab.

### VIRENSCHUTZ UND OUTBREAK FILTER INKLUSIVE

*indevis E-Mail Security* beinhaltet die leistungsfähige Sophos Anti-Virus Engine. In Kombination mit Ihrer bestehenden Anti-Virus Lösung schützen Sie Ihre Organisation somit zweistufig gegen Computerviren. Ein ebenfalls integrierter Virus Outbreak Filter schützt bei Viren-Ausbrüchen durch proaktive Filterrichtlinien, solange noch keine adäquaten Signatur-Dateien für Anti-Virus Produkte verfügbar sind. Verdächtige E-Mails werden in einem Quarantäne-Ordner gespeichert und nach einem Signatur-Update erneut gescannt und anschließend (zeitversetzt) zugestellt oder endgültig gelöscht.

### ADVANCED MALWARE PROTECTION

Verdächtige E-Mails und E-Mail-Anhänge werden gegen eine globale Hash-Datenbank geprüft. Sollten die E-Mails oder E-Mail-Anhänge nicht bekannt sein, werden die Daten in eine cloudbasierte Sandbox gesendet. Das Sandbox-Verfahren ermöglicht es, neuen und unbekanntem Schadcode zu erkennen. Dieses Verfahren ist ein einzigartiger Schutz vor gezielten „Zero-Day-Angriffen“, bei denen mit unbekanntem Schadcode versucht wird, Unternehmen zu kompromittieren.





## VERSCHLÜSSELTE E-MAILS FÜR HÖCHSTE SICHERHEITSANSPRÜCHE

Für höchste Sicherheitsansprüche ermöglicht der separate Managed Security Service indevis E-Mail Encryption den Austausch verschlüsselter E-Mails von Unternehmen mit Geschäftspartnern und Kunden, die keine eigene Verschlüsselungslösung im Einsatz haben. Die Kommunikation erfolgt über einen Cloud-Zwischenspeicher, das sogenannte Messenger Portal. Der Absender verschickt seine verschlüsselte E-Mail wie gewohnt, der Empfänger erhält die Nachricht aber als Datei-Anhang, die er nur über eine per Web-Browser aufgebaute und passwortgeschützte Verbindung zum Server öffnen und einsehen kann. So hat er auch die Möglichkeit, verschlüsselt auf diese Nachricht zu antworten.

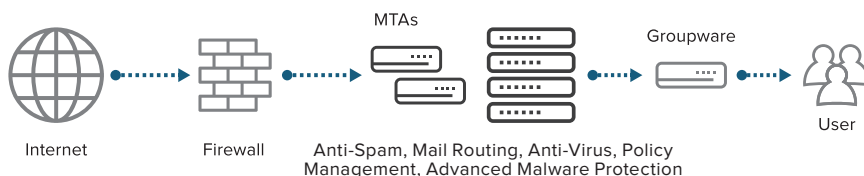
## DO-IT-YOURSELF DANK SELF SERVICE PORTAL

Die indevis betreibt ein webbasiertes Self Service Portal, über das Kunden des E-Mail Security Services mittels Benutzer-Login direkt Einblick in ihr Mail-Log nehmen können. Das Portal steht technisch versierten Benutzern oder Administratoren zur Störungsuntersuchung und E-Mail-Nachforschungen zur Verfügung. Es bestehen umfangreiche Suchfunktionen, um den Verlauf und den Verbleib von E-Mails zu untersuchen – beispielsweise nach Absender- und Empfänger-Adressen, Mail Header und Betreffzeilen.

## DATENSICHERHEIT UND DATENÜBERTRAGUNG

E-Mails werden grundsätzlich mit dem SMTP-Protokoll übertragen. Die indevis unterstützt die Verschlüsselung der Übertragung mittels TLS (Transport Layer Security). Eine Verschlüsselung seitens indevis wird immer angeboten und unterstützt. Die indevis-Systeme arbeiten mit einem validen Zertifikat von einer akkreditierten Certificate Authority (CA). Die indevis-Systeme akzeptieren auch selbsterstellte oder nicht akkreditierte Zertifikate der Gegenstellen. In diesem Fall wird zwar verschlüsselt, allerdings die Integrität der Gegenstelle nicht validiert. Abhängig von der Gegenstelle kann eine Übertragung der E-Mail auch unverschlüsselt erfolgen.

### Ohne indevis E-Mail Security



### Mit indevis E-Mail Security



## Über die indevis GmbH

Die ISO 27001 zertifizierte indevis GmbH bietet seit 1999 IT-Sicherheits-, Data-center- und Netzwerklösungen, flankiert von professionellen Consulting-, Management- und Support-Dienstleistungen. Dabei erfüllt indevis sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist indevis der Partner für IT-Sicherheit und Netzwerktechnik für Unternehmen jeder Größe und Branche – denn IT Sicherheit passiert nicht von alleine, sondern muss strategisch geplant werden.

indevis betreibt zwei Niederlassungen: in München und Hamburg. Weitere Mitarbeiter agieren von mehreren Standorten über Deutschland verteilt aus.



indevis GmbH

Irschenhauser Straße 10  
81379 München

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

sales@indevis.de  
www.indevis.de