

Protection. Encryption. Large Files.

## Komfortable Sicherheit für die gesamte E-Mail-Kommunikation

Über 1500 Unternehmen vertrauen die Sicherheit Ihrer E-Mail-Kommunikation bereits NoSpamProxy® an, hier eine kleine Auswahl:



**KOMATSU**



 **Deutscher  
Ärzte-Verlag**



**NoSpamProxy®**

## Von Experten aus Kundenanforderungen entwickelte Lösung – sicher, vollständig und einfach

NoSpamProxy® bietet zuverlässigen Schutz vor Spam und Malware, sichere E-Mail-Verschlüsselung und einfachen, sicheren Versand großer Dateien. Unsere Gateway-Lösung überzeugt durch eine sehr einfache Handhabung und hohe Bedienerfreundlichkeit für Anwender und IT-Administratoren.

Die Sicherheit der Kommunikation gewinnt für Unternehmen, Behörden und Institutionen zunehmend an Bedeutung. Dabei geht es zum einen um die Wahrung der Vertraulichkeit von Informationen. So sollen E-Mails und Dateien den Empfänger erreichen, ohne dass unbefugte Dritte Einsicht erhalten können. Zum anderen geht es um den Schutz vor unerwünschten Nachrichten. Denn die Flut an Spam und Malware sorgt für hohen Arbeitsaufwand und Gefahren für die gesamte IT-Infrastruktur.

Es beginnt an der Quelle. Untersuchungen haben bewiesen: Der größte Risikofaktor für sichere Kommunikationsprozesse sind die Beteiligten selbst. Herkömmliche Sicherheitsmaßnahmen erfordern Zeit und Aufmerksamkeit, die viele Mitarbeiter nicht aufbringen können. Wenn hier das entsprechende Bewusstsein nicht vorhanden ist, können Security-Systeme nicht zuverlässig funktionieren.

NoSpamProxy® von Net at Work wurde aus Praxisanforderungen entwickelt und geht einen neuen Weg. Als Software auf Ihrem Windows Server oder als Managed-Hosting-Lösung werden zahlreiche Funktionen zur sicheren Übertragung und zum Schutz vor Spam und Viren zentral und automatisch ausgeführt. Das Ergebnis: Die Anwender sind entlastet und Administratoren können die IT-Infrastrukturen einfacher, transparenter und effizienter sichern.

## NoSpamProxy® Softwarekomponenten – Optimal eingebettet in Ihre Microsoft Server und Microsoft Exchange Umgebung

NoSpamProxy® kann in Ihrer IT Umgebung (On-Premise) oder als Managed Service betrieben werden und läuft auf Microsoft Windows Server. Die Bedienung und der Betrieb ist dank Einbindung in die Microsoft Management Console (MMC) für Administratoren von Microsoft Umgebungen intuitiver und effizienter als isolierte Appliance Lösungen.

Die zentralen Softwarekomponenten Protection, Encryption und Large Files bieten eine einzigartige Integration mit Active Directory und Konnectoren zu De-Mail und DOI.

Für den Betrieb des Web Portals, für die Übertragung großer Dateianlagen und für die verschlüsselte Kommunikation mit E-Mail-Empfängern, die noch nicht über ein eigenes Zertifikat oder Schlüssel verfügen, wird auf den in Microsoft Server enthaltenen Internet Information Server (IIS) aufgesetzt, so dass keine zusätzlichen Softwarekomponenten erforderlich sind.

Über ein Outlook Add-In bietet NoSpamProxy® den Endanwendern in der gewohnten Outlook Umgebung intuitiv zu bedienende Funktionen für Verschlüsselung und Verschicken großer Dateien an.



### NoSpamProxy® Protection

Proaktiver Echtzeitschutz mit integrierter Zero-Hour-Lösung.



### NoSpamProxy® Encryption

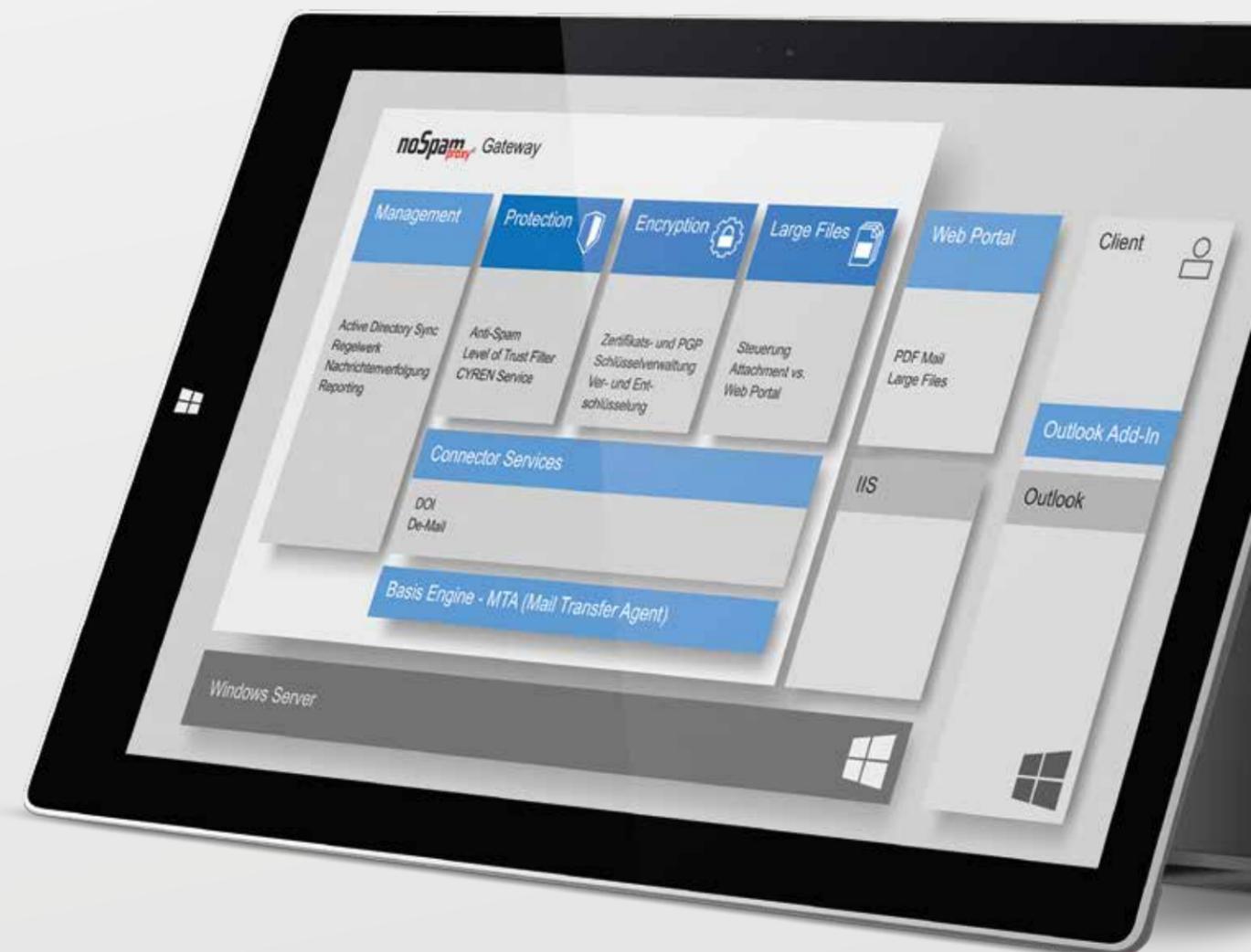
E-Mail-Verschlüsselung.  
S/MIME. PGP-Signatur.



### NoSpamProxy® Large Files

Große Dateien einfach, sicher und ohne Medienbruch versenden.

SecurITy  
made  
in  
Germany





### Transparenter Spam-Schutz ständig im Blick

Mit den Reporting-Funktionen von NoSpamProxy® Protection haben Sie Ihren E-Mail-Verkehr ständig unter Kontrolle. So lassen sich das Datenvolumen sowie das E-Mail- und Spam-Aufkommen detailliert bis auf Benutzerebene analysieren. Die integrierte Nachrichtenverfolgung protokolliert jede E-Mail und wie sie behandelt wurde. Welche Regeln waren aktiv? Welche Anti-Spam-Filter am E-Mail-Gateway haben Einfluss genommen und welche Aktionen wurden für die E-Mail ausgeführt? Administratoren haben mit den Protokollen und Berichten von NoSpamProxy® Protection alle Meldungen ständig im Blick.

### Sichere Kommunikation durch Information des Absenders

Wenn NoSpamProxy® Protection eine Nachricht irrtümlich als Spam erkennt, verweigert das Anti-Spam-Gateway die Annahme der E-Mail. Im Gegensatz zu anderen Spam-Lösungen erhält der Absender die Nachricht, dass die E-Mail nicht zugestellt wurde. Er kann darauf reagieren, indem er den Absender anruft und bittet, ihm eine E-Mail zuzusenden. Diese spricht die Level of Trust Funktion des Gateways an, so dass E-Mails dieses Absenders künftig angenommen werden. Einen Spammer interessiert die Empfängeradresse aufgrund des Mehraufwandes erfahrungsgemäß nicht mehr. Das hat als zusätzlichen Vorteil den Effekt, dass nach einiger Zeit das Spam Volumen deutlich zurückgeht, das an NoSpamProxy®-geschützte Domains gesendet wird.

## Level of Trust:

### Das bietet keine andere Anti-Spam-Lösung

NoSpamProxy® Protection lernt kontinuierlich, mit wem Sie kommunizieren. Auch mit Verdacht auf Spam werden diese Partner nicht abgewiesen. Wir nennen diese Schlüsselkomponente, die bislang keine andere Spam-Lösung bietet, Level of Trust.

### NoSpamProxy® Protection

## Gute Nachrichten für Ihren Mailserver

Zum Schutz vor Spam, Spyware und Malware scannt NoSpamProxy® Protection jede E-Mail bereits beim Empfang als erstes SMTP-Gateway und klassifiziert sie anhand unterschiedlicher Anti-Spam-Filter. Wird eine E-Mail als Spam eingestuft, nimmt das System die E-Mail nicht an. Nur als vertrauenswürdig eingestufte Nachrichten können das Anti-Spam-Gateway passieren. Die Besonderheit: Wenn eine vertrauenswürdige E-Mail nicht angenommen wird, stellt das Funktionsprinzip von NoSpamProxy® Protection sicher, dass der Absender über die verhinderte Zustellung informiert wird.

### Viele Firmen setzen bereits seit längerer Zeit Lösungen gegen Spam ein und es gibt unüberschaubar viele Produkte am Markt. Warum also gerade NoSpamProxy®?

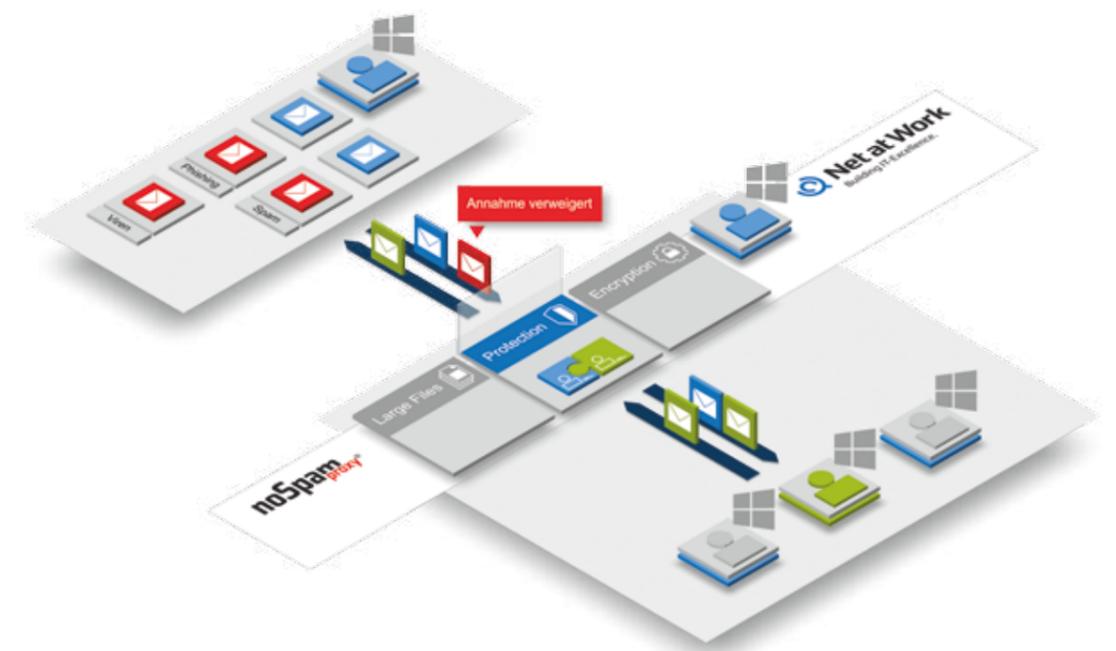
NoSpamProxy® stellt als eines von ganz wenigen Produkten eine in allen Bereichen des anspruchsvollen, deutschen Rechts konforme Lösung dar (insbesondere gemäß §206 StGB, §88 Telekommunikationsgesetz).

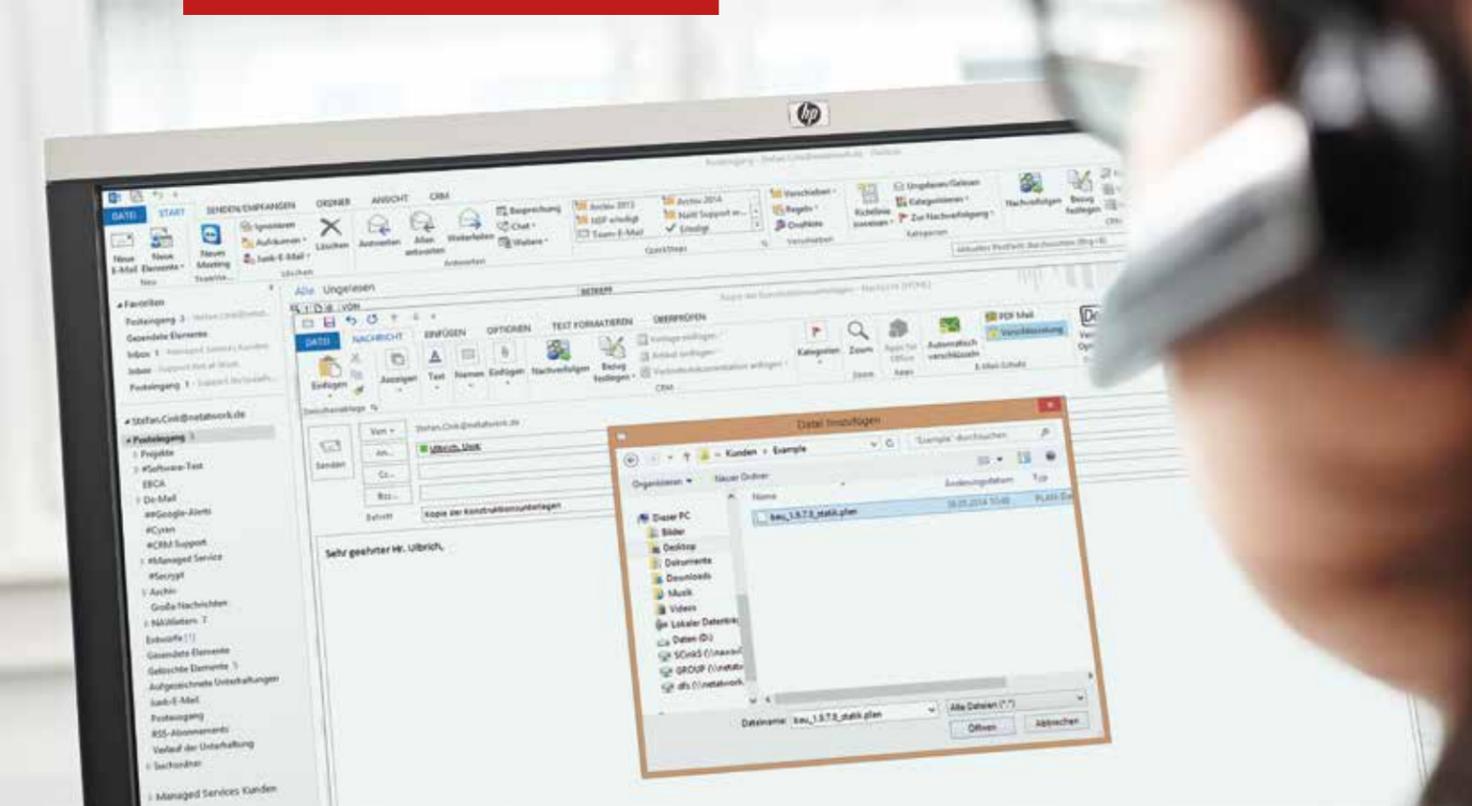
Es vermeidet die rechtlichen Konsequenzen, die sich allein schon aus der Annahme einer E-Mail durch das E-Mail-Gateway des Unternehmens ergeben. Auch die in aktuellen Gerichtsurteilen festgestellten Schadensersatzforderungen durch in Quarantäne-Bereichen verloren gegangene E-Mails können NoSpamProxy® Anwender nicht treffen. Hohe Produktivitätssteigerung und höchster Schutz bei gleichzeitig minimalem Betriebsaufwand zeichnen

NoSpamProxy® ebenfalls gegenüber vielen anderen Lösungen aus. Gerade in Microsoft Server basierten IT Umgebungen lohnt sich ein Wechsel schon nach wenigen Monaten.

### Die Quarantäne-Falle herkömmlicher Anti-Spam-Lösungen

Das Problem aller Spam-Schutzlösungen ist, dass eine Software entscheidet, ob eine E-Mail als Spam klassifiziert wird oder passieren darf. Dabei werden aber nicht alle Spam-Nachrichten erkannt und auch gute E-Mails blockiert (False Positives). Genau diese False Positives stellen bei herkömmlichen Anti-Spam-Lösungen ein Risiko dar. Wenn solche Nachrichten gelöscht oder in eine Quarantäne abgelegt werden, können falsch klassifizierte E-Mails nicht mehr zweifelsfrei gefunden werden.





## NoSpamProxy® Encryption

# Der Schlüssel zur sicheren Kommunikation

Die Signatur und die Verschlüsselung von E-Mails mit PGP oder S/MIME verschafft Ihnen zeitgemäßen Datenschutz und Rechtssicherheit. E-Mail-Verschlüsselung – nicht so wichtig? Diese Einstellung hat sich deutlich geändert, wie in vielen aktuellen Umfragen sichtbar wird. Die Gründe dafür liegen in der deutlich gestiegenen Bedrohung vor Industriespionage und automatisiertem E-Mail-Screening durch Geheimdienste. NoSpamProxy® Encryption übernimmt als Gateway-Lösung die zentrale Verwaltung von Zertifikaten und Schlüsseln. Und macht Einführung und Betrieb Ihrer E-Mail-Verschlüsselungs-Lösung so einfach wie noch nie.

In vielen Branchen wird verschlüsselte Kommunikation mit Lieferanten oder externen Dienstleistern für eine Auftragsvergabe vorausgesetzt (z.B. Automobilebranche, Lebensmitteldiscounter). Immer häufiger werden per E-Mail verschickte Rechnungen abgefangen und modifiziert. E-Mail-Verschlüsselung gibt Ihnen Rechtssicherheit beim Nachweis, welche Aufträge Sie per E-Mail erteilt haben und welche Rechnungen Sie per E-Mail gestellt haben. Durch das Angebot verschlüsselter E-Mail-Kommunikation mit Kunden oder Mandanten können sich Unternehmen aber auch wirksam differenzieren.

### Vertraulichkeit geht schnell und einfach

Durch zentrale E-Mail-Signatur und E-Mail-Verschlüsselung am NoSpamProxy® Encryption Gateway kommunizieren Sie mit Partnern besonders sicher und einfach. Da Schlüssel und Zertifikate nur auf dem Gateway und

nicht auf den Clients verwaltet werden, entfällt für den Anwender der umständliche Umgang mit elektronischen Schlüsseln.

Die Sicherheitsregeln im Sinne der Corporate Governance des Unternehmens werden automatisch zentral umgesetzt. Natürlich werden auch empfangene

Nachrichten bereits am Gateway entschlüsselt und stehen dem Anwender wie gewohnt für die Weiterverarbeitung zur Verfügung. Dies ermöglicht den Zugriff über per SSL-Verschlüsselung gesicherte Verbindungen mit Smartphones und Tablets, sowie die Archivierung der E-Mails in unverschlüsselter Form.

### PDF Mail: E-Mails und Dokumente sicher versenden

Für den häufigen Fall, dass Empfänger keinen PGP-Schlüssel oder persönliches Zertifikat haben, bietet NoSpamProxy® Encryption mit der PDF Mail Funktion einen weiteren einfachen Weg für den sicheren Versand von E-Mails und Dokumenten, der keine Anforderungen an den Empfänger stellt. Dazu wandelt NoSpamProxy® Encryption die E-Mail mit allen Anhängen automatisch in ein passwortgeschütztes PDF-Dokument um. Dieses Passwort wird dem Empfänger automatisiert per SMS zugesandt oder der Empfänger kann über die Anmeldung im NoSpamProxy® Web Portal ein eigenes Passwort vergeben. Der Empfänger benötigt lediglich einen PDF-Reader, um anschließend die Nachricht zu öffnen. PDF Mail ist vor allem für Unternehmen interessant, die sensible oder personenbezogene Daten auch

ohne E-Mail-Zertifikat, Verschlüsselungssoftware oder SSL-Verschlüsselung versenden möchten.

### E-Mail-Verschlüsselung und Zertifikate

Im Rahmen der sicheren Verschlüsselung von E-Mails sind Zertifikate erforderlich, die für das S/MIME Verfahren nach dem X.509-Standard oder mit einem PGP-Schlüssel genutzt werden können. NoSpamProxy® Encryption zentralisiert und automatisiert die Verwaltung dieser Zertifikate. Für Anwender ist der Erwerb der Zertifikate automatisiert. IT-Administratoren profitieren von einer Vielzahl hilfreicher Managementfunktionen.

### PGP Mail

Pretty much better in privacy: Natürlich können mit NoSpamProxy® Encryption auch PGP-Schlüssel generiert, importiert und verwaltet werden.

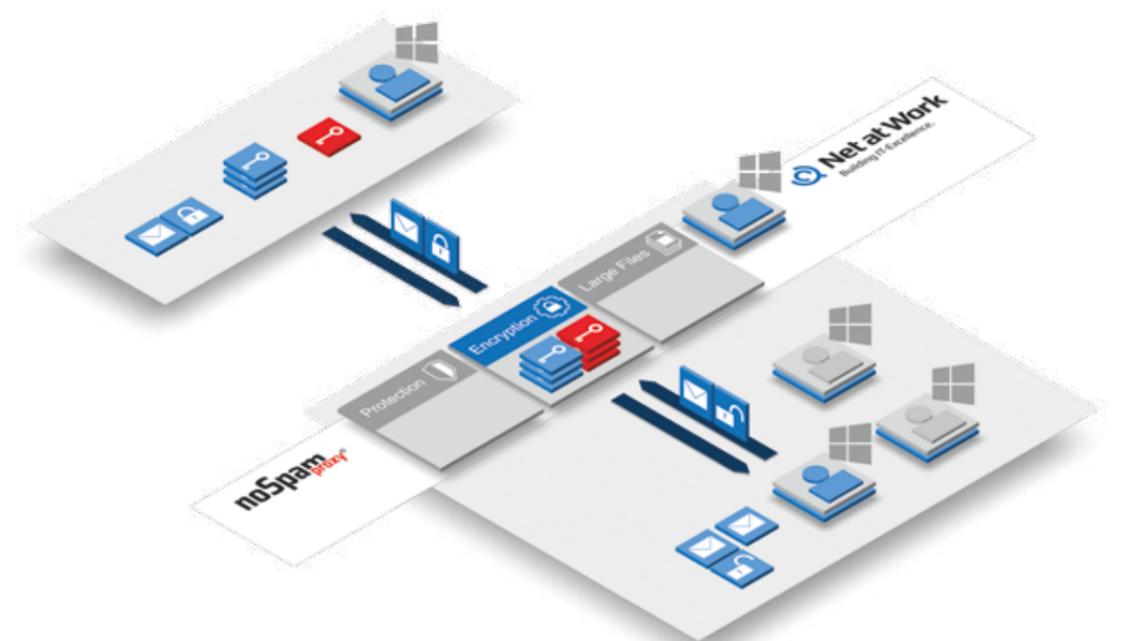
Mit der Unterstützung von PGP E-Mail bietet NoSpamProxy® Encryption eine weitere Möglichkeit zum bequemen Austausch von verschlüsselten Daten und Nachrichten.

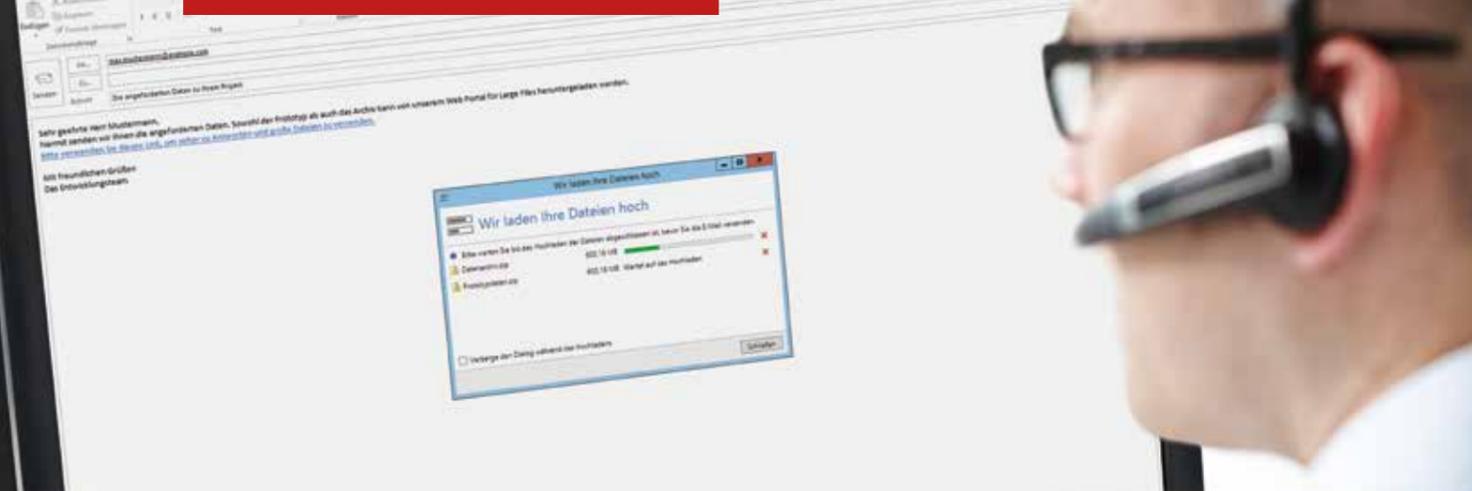
### Weitere Funktionen von NoSpamProxy® Encryption sind die Anbindung an

- DOI (für die Kommunikation zwischen Behörden, die an DOI angeschlossen sind)
- De-Mail (für die Kommunikation per De-Mail mit De-Mail Teilnehmern)



Auf der CeBIT 2015 wurde NoSpamProxy® von Net at Work mit dem "FP Award 2015 – De-Mail Innovation" ausgezeichnet. Mit dem De-Mail-Innovationspreis prämiiert Francotyp-Postalia innovative Konzepte rund um die De-Mail.





## NoSpamProxy® Large Files

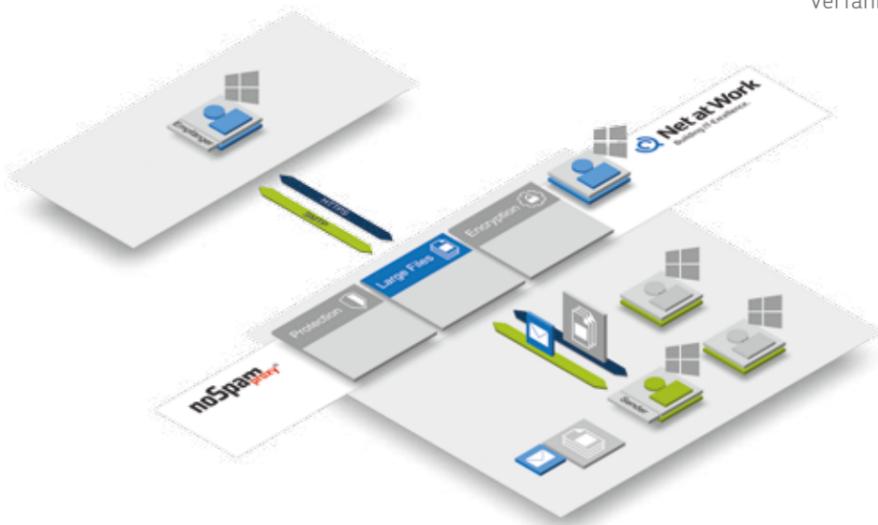
# Große Dateien austauschen – Einfach, sicher und ohne Medienbruch

NoSpamProxy® Large Files erlaubt es Benutzern, beliebig große Dateien direkt aus dem E-Mail-Client zu versenden. Anwender können auf diese Weise große Dateien, die die Beschränkungen des E-Mail-Programms überschreiten, ohne Medienbruch mit einem einzigen Klick absetzen. Der Einsatz ist unkompliziert und mit dem Versand herkömmlicher Dateianhänge vergleichbar. Im Gegensatz zu den verbreiteten File-Transfer-Diensten werden die Daten hier über einen kundeneigenen Web-Server bereitgestellt und via SSL-Verschlüsselung übertragen. Damit werden die Anforderungen an sicherheitskritische Business-Anforderungen sowie die IT-Governance erfüllt.

Auf der Administrationsoberfläche von NoSpamProxy® Large Files können die Einstellungen schnell und einfach vorgenommen werden. Das Interface bietet zusätzlich auch Reporting-Funktionen, um z.B. bei Vertriebsaktionen festzustellen, welche Adressaten einer E-Mail-Kampagne die angebotene Datei heruntergeladen haben.

## Vorteile mit NoSpamProxy® Large Files

- Entlastung der vorhandenen E-Mail-Infrastruktur und Bandbreite
- Höhere Sicherheit durch Übertragung großer Dateien mit SSL-Verschlüsselung
- Vermeidung der Mehrfacharchivierung von Dateien in Outlook-Ordnern und Reduzierung der Backup-Kosten
- Vollständige Integration in die E-Mail-Kommunikation ohne Medienbruch wie bei FTP-Servern oder Cloud-Diensten
- Konfigurierbare Möglichkeit, mit der E-Mail-Antwort ebenfalls große Dateien über das gleiche Verfahren zu verschicken



Die 1995 gegründete Net at Work GmbH ist Softwarehaus und Systemintegrator mit Sitz in Paderborn. Gründer und Gesellschafter des Unternehmens sind Geschäftsführer Uwe Ulbrich und Frank Carius, der mit [www.msxfaq.de](http://www.msxfaq.de) eine der renommiertesten Websites zu den Themen Exchange und Lync betreibt. Net at Work liefert ein breites Lösungsportfolio rund um die IT-gestützte Kommunikation und die Zusammenarbeit im Unternehmen.

Darüber hinaus entwickelt und vermarktet Net at Work mit NoSpamProxy® ein innovatives Secure E-Mail-Gateway mit einer integrierten Verschlüsselungslösung für eine vertrauliche und rechtssichere elektronische E-Mail-Kommunikation. Die Windows-Server-basierten Systeme schützen bereits über 1.500 Unternehmen zuverlässig vor Spam und Malware und ermöglichen eine leistungsfähige, vollständig im Hintergrund ablaufende Verschlüsselung. Die konsequente Automatisierung zahlreicher Funktionen verringert dabei nachhaltig den Administrationsaufwand.

[www.netatwork.de](http://www.netatwork.de)

Weitere Informationen, download, testen, Angebot anfordern unter:  
[www.nospamproxy.de](http://www.nospamproxy.de)

Net at Work GmbH  
Am Hoppenhof 32 A  
33104 Paderborn  
GERMANY

T +49 5251 304-600  
F +49 5251 304-650  
[info@netatwork.de](mailto:info@netatwork.de)  
[www.netatwork.de](http://www.netatwork.de)