



iQ.Clustering

**Hochverfügbarkeit, Ausfallsicherheit,
Lastverteilung, Distributed Computing**

► Inhalt

| | |
|---|---|
| 1 Einleitung | 1 |
| 2 Übersicht | 1 |
| 2.1 Domino-Cluster | 1 |
| 2.2 Betriebssystem-Cluster | 2 |
| 2.3 iQ.Clustering..... | 2 |
| 3 Arbeitsweise bei der E-Mail-Prüfung | 6 |
| 4 Arbeitsweise für die Grabber-Überwachung | 7 |
| 5 Installationsvoraussetzungen | 7 |
| 6 Vorteile beim Einsatz von iQ.Clustering | 7 |
| 7 Über GROUP Technologies | 9 |

1 Einleitung

E-Mail ist heute eine der kritischen Anwendungen in einem Unternehmen. Andere unternehmenskritische Applikationen sind beispielsweise ERP-, Warenwirtschafts- oder Rechnungswesen- bzw. Controllingsysteme.

Von unternehmenskritischen Anwendungen werden eine ständige Verfügbarkeit, eine hohe Performance und eine hohe Skalierbarkeit erwartet. Die Fähigkeit von Lastverteilung, Einsatz in heterogenen Umgebungen und ein einfaches Systemmanagement sind weitere Anforderungen.

Die von IBM Lotus dafür angebotene Lösung ist der Domino-Cluster, der diese Anforderungen auf Datenbankebene abdeckt.

Im Bereich der E-Mail-Sicherheit steht die ständige, leistungsfähige und sichere Überwachung des gesamten E-Mail-Verkehrs an oberster Stelle, z.B. Virenschutz und Spam-Abwehr. Dafür ist das Domino-Cluster nicht ausreichend.

iQ.Clustering als E-Mail-Sicherheitslösung ist die ideale Ergänzung des Domino-Clusters mit dem Focus auf einen sicheren und effizienten E-Mail-Verkehr.

2 Übersicht

2.1 Domino-Cluster

Ein Domino-Cluster ist eine Gruppe von zwei oder mehr Domino-Servern. Ein Domino-Cluster gewährleistet den Benutzern einen ständigen, leistungsfähigen Zugriff auf Ihre Daten, auch bei wachsenden Umgebungen.

Ein Domino-Cluster hat folgende Möglichkeiten:

■ Hochverfügbarkeit von kritischen Datenbanken

Durch Replikation der Datenbanken zwischen den einzelnen Servern in einem Cluster hat der Benutzer ständig Zugriff auf die Datenbanken, auch wenn ein Server nicht verfügbar ist. Dieser Prozess wird auch als Failover bezeichnet. Damit sind auch Hardware- oder Software-Upgrades fast ohne Behinderung der Nutzer möglich.

Im Domino-Cluster werden die Datenbanken ständig synchronisiert, so dass die Informationen auf allen Servern gleich sind.

■ Lastverteilung

Beim Datenzugriff auf stark belastete Server erfolgt im Cluster eine automatische Umlenkung auf einen weniger belasteten Server. Damit kann die Auslastung relativ gleichmäßig über alle Server im Cluster verteilt werden, so dass eine hohe Performance gewährleistet ist.

■ Skalierbarkeit

Dem Cluster können weitere Server hinzugefügt werden, falls die Performance nicht mehr ausreichend ist. Eine wachsende Anzahl von Datenbanken oder Benutzern macht diese Maßnahme oftmals notwendig. In diesem Fall können weitere Server in das Cluster eingefügt werden. Damit

stehen alle Datenbanken aktuell zur Verfügung und die Benutzer werden durch die Lastverteilung automatisch auf den/die neuen Server umgeleitet (switch).

■ **Datensynchronisation**

Um die ständige Verfügbarkeit der Daten auch bei einem ausgefallenem Server zu gewährleisten, werden die Daten mittels der Replikationsmechanismen ständig synchronisiert.

■ **Hard- und Software, Systemmanagement**

Innerhalb des Domino-Clusters können die verschiedenen Domino-Server auf unterschiedlichen Hardware-Plattformen oder auch Betriebssystemen laufen. Damit wird der Einsatz in heterogenen Umgebungen unterstützt. Es ist nicht notwendig, alle Server im Cluster unter dem gleichen Betriebssystem bzw. auf der gleichen Hardware-Plattform zu betreiben.

Ein Upgrade eines Betriebssystems bzw. einer Hardware ist damit möglich, ohne die Verfügbarkeit der Daten einzuschränken.

Für die Backup- und Disaster Recovery-Strategie ist ein Cluster ebenfalls von Vorteil, da bei einem Ausfall (oder einer Datensicherung) eines Servers die Benutzer weiterhin auf alle Daten zugreifen können und automatisch auf einen anderen Server umgeleitet werden. Natürlich können einzelne Server im Cluster auch nur als Backup-Server verwendet werden.

2.2 Betriebssystem-Cluster

Neben dem Domino-Cluster gibt es die Möglichkeit des Betriebssystem-Clusters, z.B. Sun-Cluster, Microsoft-Cluster Services und IBM AIX HACMP. Diese Clusterarten verhindern einen Ausfall des Betriebssystems und anderer Servertasks, inklusive der Domino-Server.

Diese Clusterarten haben ebenso Ihre Stärken wie ein Domino-Cluster, sind aber betriebssystemabhängig. Weitere Details dazu sind den entsprechenden Unterlagen der jeweiligen Hersteller zu entnehmen.

Der Einsatz einer Kombination von Betriebssystem-Cluster und Domino-Cluster sichert die beste Ausnutzung aller Vorteile.

2.3 iQ.Clustering

iQ.Clustering ist Bestandteil der iQ.Suite und damit ein Applikations-Clustering. iQ.Clustering wird mit der Installation auf einem Domino-Server nach der Lizenzierung aktiviert. Es ersetzt nicht die Funktion eines Domino-Clusters. iQ.Clustering kann die Funktionen eines Domino-Clusters sinnvoll ergänzen. Ein Domino-Cluster ist **keine** Voraussetzung für iQ.Clustering. Ein Verbund im iQ.Clustering kann aus mehreren Domino-Servern (sinnvolles Limit ist 4 bis 6) mit installierter iQ.Suite bestehen.

Für eine einwandfreie Funktionsweise des iQ.Clustering wird eine gleichartige oder replizierte Konfiguration auf allen beteiligten Servern vorausgesetzt. Die Netzwerkverbindung zwischen den Servern im Cluster sollte ausreichend hohe Übertragungsraten erlauben, wie sie z.B. LAN-Verbindungen zur Verfügung stellen.

iQ.Clustering unterstützt die Fähigkeiten einer Domino-Umgebung für

■ Hochverfügbarkeit

Die Verfügbarkeit der iQ.Suite kann in großen Umgebungen durch iQ.Clustering abgestimmt werden. Innerhalb des iQ.Clustering wird der E-Mail-Fluss durch die Mail.box überwacht und die E-Mails werden durch die iQ.Suite bearbeitet.

Ist die iQ.Suite auf einem iQ.Clustering-Server nicht verfügbar, z.B. während eines Virenschanner-Updates, so übernehmen die anderen iQ.Clustering-Server dessen Aufgaben.

□ Beispiel

Sie betreiben ein Ausfallrechenzentrum für Ihre Domino-Server. Mit iQ.Clustering können sie sicherstellen, dass die Clustermaschine im Ausfallrechenzentrum sofort einspringt, sobald der Server im Normalbetrieb nicht mehr zur Verfügung steht. In diesem Fall betreiben Sie sinnvoller Weise die Kombination aus Domino-Cluster und iQ.Clustering.

■ Ausfallsicherheit

Fällt die iQ.Suite auf einem iQ.Clustering-Server aus, so übernehmen die anderen Server automatisch deren Aufgaben und leiten entsprechende Informationen weiter. Die Ausfallwahrscheinlichkeit der iQ.Suite und damit das Risiko wird mit iQ.Clustering deutlich gesenkt.

□ Beispiel

Sie betreiben an einem Standort mehrere Domino-Server. Mit iQ.Clustering können sie sicherstellen, dass ein Ausfall der iQ.Suite auf einem Server durch die anderen Server im Cluster voll kompensiert wird.

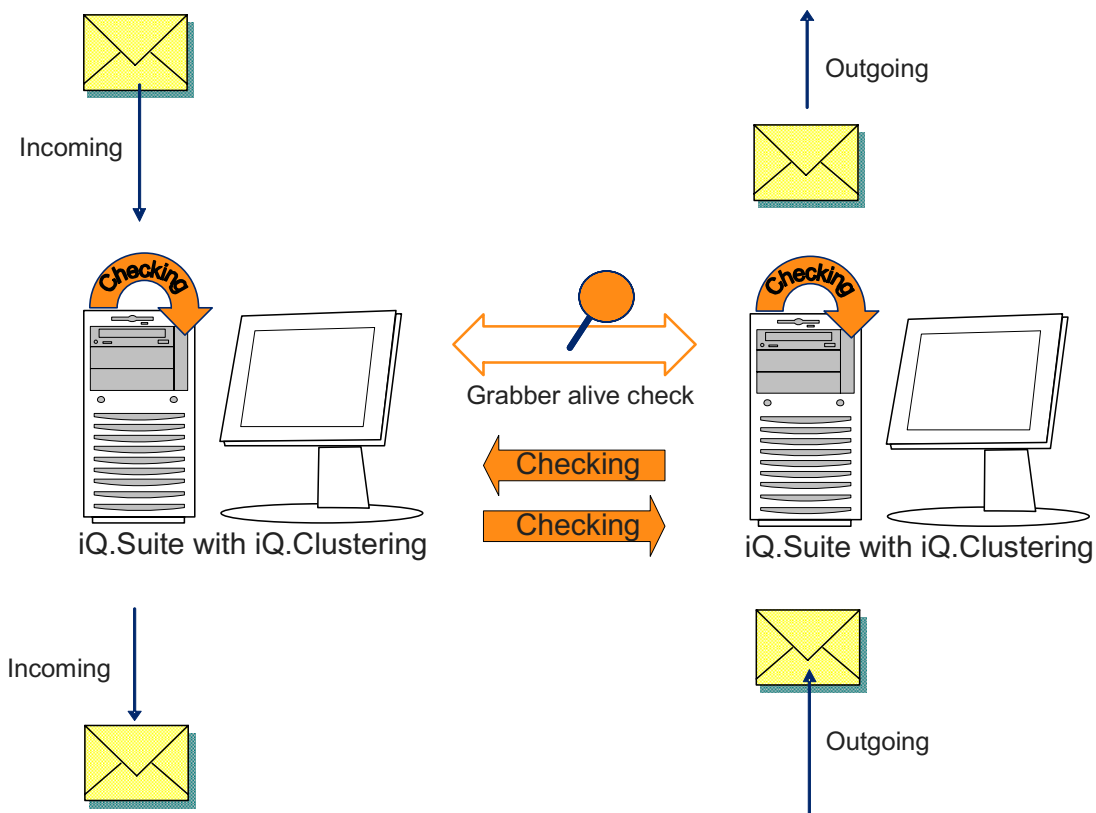
■ Lastverteilung

Mit iQ.Clustering wird die Lastverteilung zwischen unterschiedlich stark belasteten Servern mit installierter iQ.Suite ermöglicht. Ein weniger stark belasteter iQ.Clustering-Server übernimmt dabei die E-Mails zur Bearbeitung von einem stark belasteten iQ.Clustering-Server und gibt die sie nach der Bearbeitung wieder zurück. Damit wird die Gefahr eines E-Mail-Staus auf ein Minimum reduziert.

□ Beispiel

Sie betreiben an Ihrem Hauptstandort mehrere Domino-Server als Internet-Gateway. Das Gateway für eingehende E-Mails ist sehr stark belastet. Durch die Lastverteilungsfunktion im iQ.Clustering unterstützt das weniger belastete Gateway für ausgehende E-Mails die stark belastete Maschine für eingehende Mails im iQ.Clustering.

Grafische Darstellung für die gegenseitige Überprüfung der Mailboxen auf einem Internet-Gateway durch zwei PCs mit gleichzeitiger gegenseitiger Überwachung der MailGrabber:



■ Distributed Computing.

Für einige von Domino unterstützten Betriebssysteme stehen nicht alle Module der iQ.Suite zur Verfügung. Das betrifft im Besonderen die Mainframe-Systeme, z.B. iSeries, zSeries.

In Umgebungen mit solchen Betriebssystemen ermöglicht iQ.Clustering die Bearbeitung der E-Mails durch die iQ.Suite auf einer separaten Maschine. Das Host-System und die separate Maschine sind mittels LAN verbunden und unabhängig voneinander. Damit ist der Einsatz **aller** Module der iQ.Suite möglich. Gleichzeitig wird die Last auf eine oder mehrere - meist preiswertere - Maschinen verteilt. Voraussetzung ist ein installierter Domino-Server auf der separaten, mit der iQ.Suite ausgestatteten Maschine.

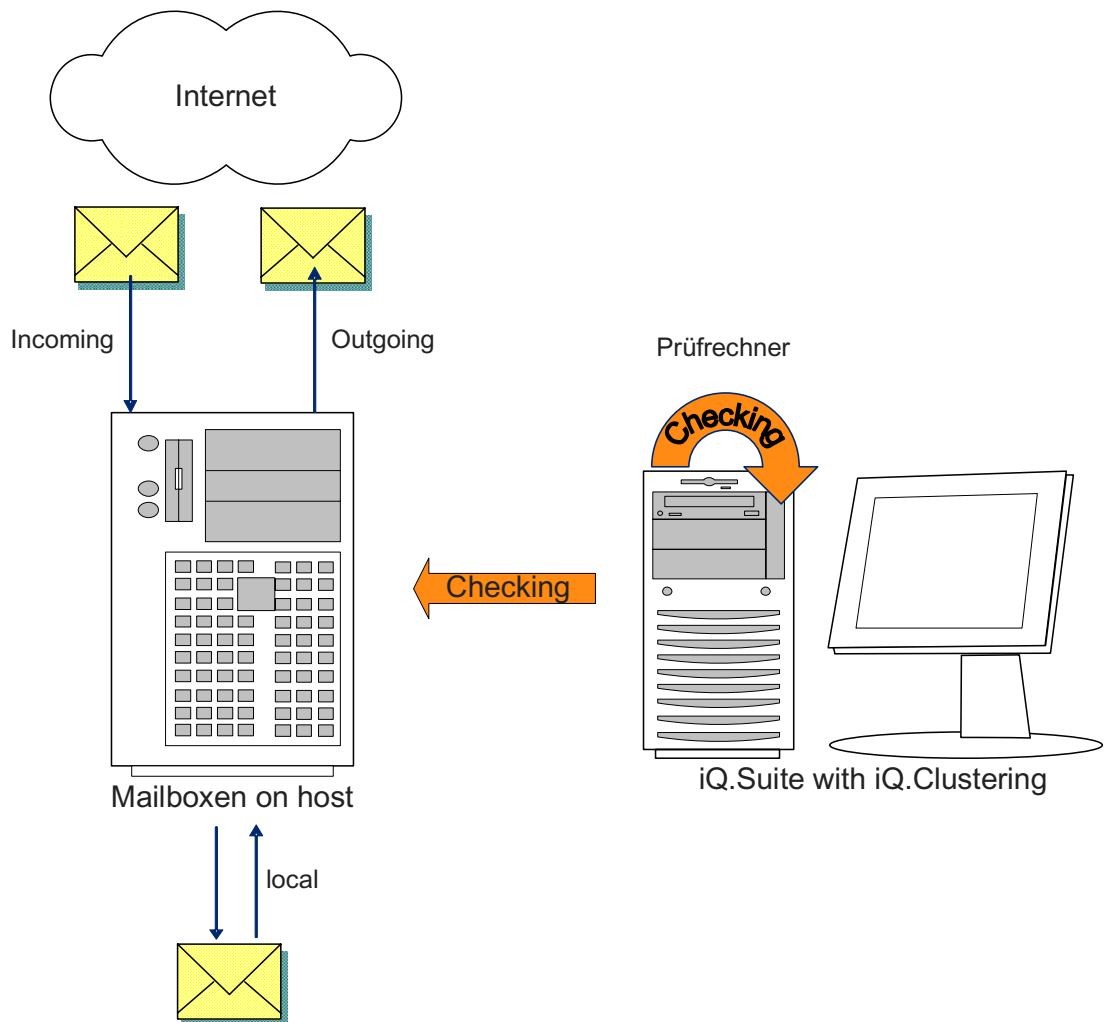
□ Beispiel

Ein vorhandener Mail-Host (mit Domino-Server) in einer Nicht-Windows-Umgebung soll mit der iQ.Suite ausgestattet werden. Ziel ist die Untersuchung von Anhängen auf Viren. Es soll ein Virens Scanner verwendet werden, der auf der Betriebssystem-Plattform nicht zur Verfügung steht. Um dieses Problem zu lösen, kann nun die Virenprüfung auf eine Windows-Maschine verlagert werden. Dazu wird die iQ.Suite mit den entsprechenden Funktionsmodulen (hier: Watchdog) zusammen mit dem Virens Scanner auf dieser Maschine installiert. Auf dem Mail-Host wird nun lediglich die EXTMGR_ADDIN te_hook installiert. Somit wird die E-Mail auf dem Host zur Bear-

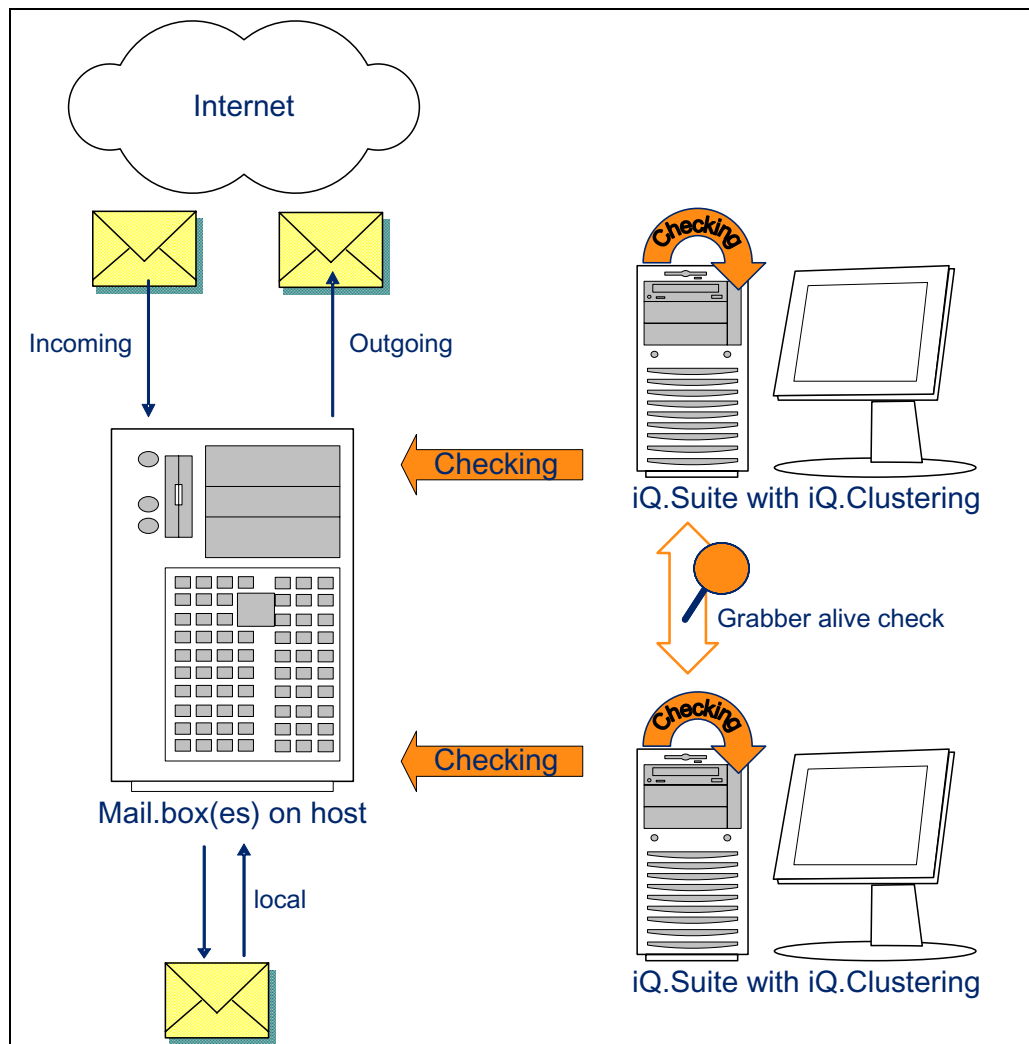
beitung durch die Hook gekennzeichnet und der MailGrabber kann anschließend die E-Mails auf der Maschine mit der iQ.Suite entsprechend bearbeiten.

Neben der Virenprüfung können Sie damit auch jedes andere Modul in jeder Umgebung betreiben, da Sie immer von einer Plattform aus prüfen können, in der das Modul zur Verfügung steht.

Grafische Darstellung für die Überprüfung der Mailboxen auf einer Host-Maschine durch einen PC:



Grafische Darstellung für die Überprüfung der Mailboxen auf einer Host-Maschine durch zwei PCs mit gleichzeitiger gegenseitiger Überwachung der MailGrabber:



3 Arbeitsweise bei der E-Mail-Prüfung

Hier die Reihenfolge der Abarbeitung von E-Mails mit iQ.Clustering:

1. Der MailGrabber prüft auf neue Dokumente in den zu überwachenden Mail.box(en).
2. Der MailGrabber versucht, gefundene Dokumente für sich zu reservieren
→ neuer Status in der Ansicht: **dispatched for <Servername>**
3. Die Arbeitsthreads bearbeiten nur Dokumente, die der Server für sich selbst reservieren konnte.
Das wird über das Feld `$TKCheckServer` entschieden.
4. Sollten Dokumente reserviert sein und nicht innerhalb von 15 min. bearbeitet werden, werden sie wieder „in den Topf geworfen“.
5. Sollten reservierte Dokumente beim Herunterfahren bzw. Starten des MailGrabbers vorhanden sein, wird die Reservierung entfernt.

4 Arbeitsweise für die Grabber-Überwachung

1. Der MailGrabber prüft auf den zu überwachenden Servern in der Mail.box / Mail1.box auf ein Profildokument.
2. Dieses Profildokument enthält die letzte Aktion des Grabbers auf dem überwachten Server mit zugehöriger Uhrzeit.
3. Dieses Profildokument wird vom zu überwachenden Grabber geschrieben (min. 1/Minute) und von den überwachenden Servern gelesen und gelöscht (ca. alle 5 Minuten).
4. Wird kein Profildokument gefunden, wird der zuletzt gelesene Status als der gültige angenommen.

5 Installationsvoraussetzungen

Neben den allgemeinen Installationsvoraussetzungen für die iQ.Suite sollten folgende Bedingungen auf den eingesetzten Prüfrechnern erfüllt sein:

- Eins der folgenden Betriebssysteme: Microsoft Windows, Linux, Sun, AIX
- Schnelle Netzwerkverbindung
- Virens Scanner (für securiQ.Watchdog)
- PGP (für securiQ.Crypt)

6 Vorteile beim Einsatz von iQ.Clustering

Der Einsatz von iQ.Clustering hat folgende entscheidenden Vorteile:

■ Hochverfügbarkeit der Analyse des E-Mail-Verkehrs

Die Kontrolle aller E-Mails entsprechend der Unternehmensrichtlinien wird gesichert. Jederzeit ist z.B. der Virenschutz oder die Verhinderung des Versandes von sensiblen Informationen gewährleistet. Damit wird das Sicherheitsrisiko deutlich gesenkt. Updates und Upgrades sind ohne Einschränkung der Arbeitsfähigkeit möglich.

■ Ausfallsicherheit der iQ.Suite

Die Bearbeitung aller E-Mails entsprechend der Sicherheitsrichtlinien eines Unternehmens ist gewährleistet. Damit wird das Sicherheitsrisiko deutlich gesenkt.

■ Lastverteilung

Die gleichmäßige Bearbeitung aller E-Mails durch die iQ.Suite ist gewährleistet. Weniger belastete Server entlasten stark belastete Server. Damit gibt es keinen Stau in der Mail.box eines Domino-Servers, wenn die Analyse einer E-Mail entsprechend den Unternehmensrichtlinien sehr lange dauert. Zeitkritische E-Mails werden schnell zugestellt.

■ Distributed Computing

Unterstützung auch der Domino-unterstützten Betriebssysteme, auf der nicht alle Module von iQ.Suite zur Verfügung stehen (z.B. Mainframe-Systeme: u.a.: iSeries, zSeries). Dadurch wird die Flexibilität beim Einsatz der iQ.Suite in Enterprise-Umgebungen maßgeblich gesteigert.

7 Über GROUP Technologies

GROUP Technologies ist der Lösungsanbieter für prozessorientiertes, sicheres und gesetzeskonformes E-Mail-Management. Unabhängig von ihrer Größe, sind Unternehmen damit in der Lage, ihre E-Mail-Kommunikation in Übereinstimmung mit den aktuellen gesetzlichen Anforderungen und betrieblichen Vorgaben zentral in die Geschäftsprozesse einzubinden.

Die Kernlösungen GROUP MailSecure und GROUP MailArchive ermöglichen das Verarbeiten, Speichern und Verwalten von E-Mails - von deren Entstehung bis zur Löschung. Dazu zählen Viren- und Spamschutz, Daten- und Inhaltskontrolle, Verschlüsselung, Klassifizierung, automatisierte Speicherung und intelligente Rückgewinnung von E-Mails und deren Anlagen. Dadurch wird nicht nur der höchstmögliche Sicherheitsstandard für Unternehmensdaten erzielt, sondern zugleich auch die Effizienz der gesamten Organisation gesteigert. Zusätzlich werden Unternehmen und ihre Entscheidungsträger vor Bußgeldern bewahrt, die bei Verstößen gegen unter anderem datenschutzrechtliche Vorschriften oder Kennzeichnungspflichten drohen.

Zu den Kunden von GROUP Technologies zählen neben mehr als drei Viertel der Sparkassen und Volksbanken in Deutschland, unter anderem auch zahlreiche internationale Unternehmen wie ABN AMRO, Allianz, Deutsche Bank, Ernst & Young, Honda, Heineken und Miele. Mehr als drei Millionen User bauen bereits auf die Expertise des Lösungsanbieters.

www.group-technologies.com

© 2005 GROUP Technologies

Die Produktbeschreibungen haben lediglich allgemeinen und beschreibenden Charakter. Sie verstehen sich weder als Zusicherung bestimmter Eigenschaften noch als Gewährleistungs- oder Garantieerklärung. Spezifikationen und Design unserer Produkte können ohne vorherige Bekanntgabe jederzeit geändert werden, insbesondere, um dem technischen Fortschritt Rechnung zu tragen.

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der GROUP Technologies zum Zeitpunkt der Veröffentlichung dar. Da GROUP Technologies auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens der GROUP Technologies dar und GROUP kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren.

Dieses Dokument dient nur zu Informationszwecken. Die GROUP Technologies schließt für dieses Dokument jede Gewährleistung aus, sei sie ausdrücklich oder konkludent. Dies umfasst auch Qualität, Ausführung, Handelsüblichkeit oder Eignung für einen bestimmten Zweck.

Alle in diesem Dokument aufgeführten Produkt- oder Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.



European Headquarters:

GROUP Technologies

MesseTurm
60308 Frankfurt
Deutschland

Head Office:

Fon +49 (0)69-789-8819-0
Fax +49 (0)69-789-8819-99

Sales:

Fon: +49 (0)721-4901-0
Fax: +49(0)721-4901-199

Hotline:

Fon 01805-4901-11
+49(0)721-4901-112
Fax +49(0)721-4901-1922

hotline@group-technologies.com
info@group-technologies.com
<http://www.group-technologies.com>

In the US:

GROUP Technologies

c/o Relavis Corporation
40 Wall Street
New York, New York 10005
USA

Head Office:

Fon +1 212-995-2900
Fax +1 212-995-2206

Sales:

Fon +1 212-995-2900

Hotline:

Fon 01805-4901-11
+1 877-476-8755
(US and Canada Only)

us.support@group-technologies.com
info@group-technologies.com
<http://www.group-technologies.com>