

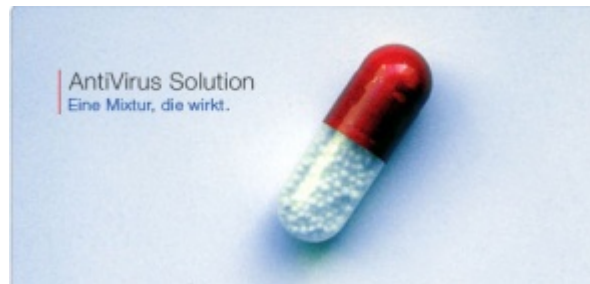


## AntiVirus Solution

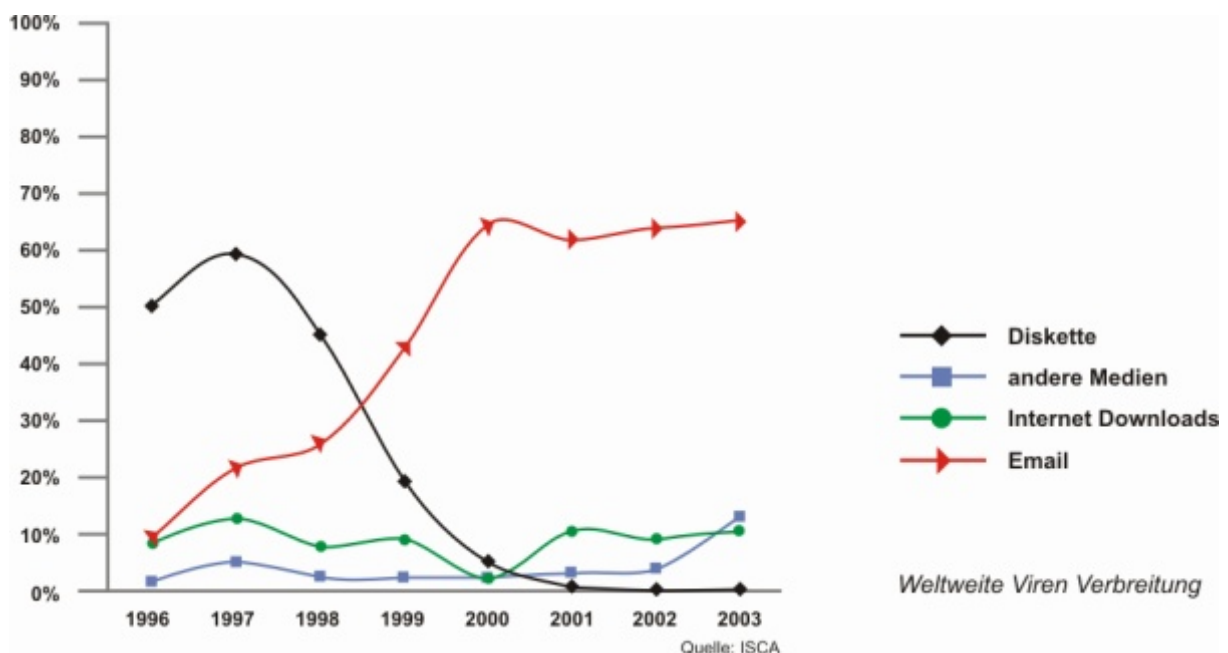
Minimierung des Risikofensters

### Einleitung:

Durch die ständig weiter ansteigende Zahl von Viren-Attacken und die Geschwindigkeit sowie die Vielseitigkeit mit welcher diese ausgeführt werden, verdeutlicht wie wichtig eine sichere und robuste Nachrichtenplattform ist. Das reine Erkennen und Blocken schon bekannter Viren ist da nicht mehr ausreichend. Bei den aktuell geführten Viren-Angriffen und dem damit verbundenen sprunghaft ansteigenden Nachrichtenvolumen sind herkömmliche E-Mail-Lösungen längst überfordert. Solche Situationen enden immer in einer Überlastung des Dienstes (DoS oder Denial-of-Service).



Die von Message Solution eingesetzten Antivirus- und System- Technologien verhindern solche Szenarien sicher und erfolgreich. Das Nachrichten-Betriebssystem M/OS erkennt DoS-Attacken automatisch und drosselt dynamisch die Bandbreite der betroffenen Netzwerkverbindungen (je gefährlicher eine Nachricht ist, desto langsamer wird sie verarbeitet). Die eingesetzten Antiviren Engines gehören zu den Marktführern ihrer Art und verfügen jeweils über weltweit vertretene Research Labs die 7 x 24 Stunden in der Woche arbeiten. Die Kombination mehrerer führender Antivirus-Engines minimiert weiter das Risikofenster und eliminiert semantische Fehler.



Message Solution bietet die Möglichkeit für jede Art von Nachrichten-Anomalie eigene E-Mail-Pipelines und eigene Quarantäne- Bereiche zu definieren. So können per Definition z. B. virulente, verschlüsselte, nicht untersuchbare und bereinigte Nachrichten parallel in eigenen E-Mail-Pipelines oder Quarantäne- Bereichen weiter verarbeitet werden. Diese Technologie schafft eine bisher nicht erreichte Transparenz in der Nachrichtenverwaltung und das stellt die Zentrale Managebarkeit sicher.



## Benefits / Philosophie:

### Leistungsmerkmale

- Die Kombination mehrerer führender Antivirus-Engines minimiert das Risikofenster und eliminiert semantische Fehler
- DoS-Attacken werden automatisch erkannt und unterbunden
- Die gemeinsame Definition eigener E-Mail-Pipelines und Quarantäne- Bereiche für z. B. virulente, verschlüsselte, nicht untersuchbare und bereinigte Nachrichten schafft eine bisher nicht erreichte Transparenz, sowie ein zentrales Management verhaltensauffälliger Nachrichten
- AntiVirus Solution passt sich dynamisch und schnell an die jeweils geforderten Unternehmensprozesse an
- Message Solution ist eine hochverfügbare, skalierbare und robuste Unternehmenslösung

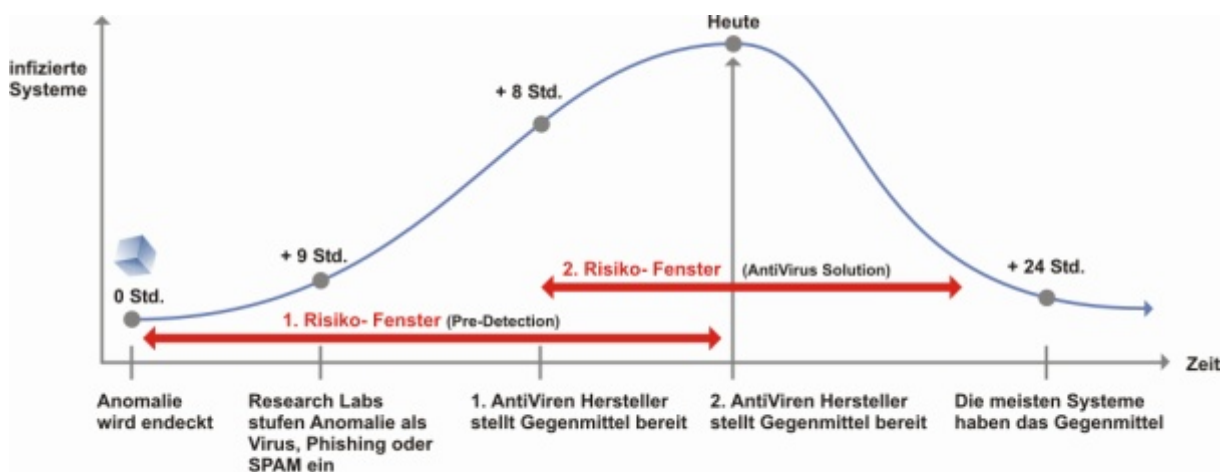


## Technik:

Die von Message Solution integrierten Antiviren-Engines untersuchen sämtliche ein- und ausgehenden Nachrichten auf „malicious code“. Durch die modulare System-Architektur können Scan-Vorgänge parallel und mit hoher Geschwindigkeit ausgeführt werden. Dabei werden unterschiedlichste Methoden eingesetzt, um alle Formen und Arten von Viren zu erkennen und zu eliminieren. Die von Message Solution eingesetzte Emulationstechnologie arbeitet in isolierten Bereichen und kann polymorphe Viren selbst dann erkennen, wenn der virulente Code im Inhalt nicht sichtbar ist, der Virus sich selbstständig weiter modifiziert oder sich selbst verschlüsselt. Durch den integrierten Online-Dekompressor und die OLE2-Engine, kann direkt in mehrschichtigen Archiven nach „malicious code“ und Macro-Viren gesucht werden.

## Minimierung des Viren Risikofensters

Während einer Viren-Attacke ist es wichtig den Zeitraum zwischen dem Ausbruch des Virus und der Erkennung durch die Antiviren-Engines zu überbrücken. Durch die von Message Solution verwendete Senderbase Technologie (siehe *Pre-Detection Solution*) werden weltweit E-Mail-Anomalien innerhalb weniger Minuten erkannt, isoliert und unter Quarantäne gestellt bis die Antiviren Research Labs entsprechende Gegenmittel entwickelt haben.



*AntiVirus Solution, Vorsprung bei neuen Virenausbrüchen*



## Dynamische Richtlinien

Message Solution kann auf jeden nur erdenklichen klassifizierten Zustand einer Nachricht mit dynamischen Richtlinien reagieren. Richtlinien können z. B. verschlüsselte oder nicht untersuchbare Nachrichten in besonders isolierte Bereiche stellen und den Empfänger persönlich informieren das eine für ihn bestimmte Nachricht, bis auf weiteres, isoliert werden musste. Es ist auch möglich virulente Nachrichten in Quarantäne zu stellen und nur den originären Inhalt einer Nachricht als Text an den Empfänger zu übermitteln, mit dem Hinweis dass die original Nachricht isoliert werden musste und nach Beendigung der Quarantäne automatisch zugestellt wird.

Ereignis	dynamische Richtlinie (Beispiele)
<b>Virus gefunden</b>	➔ Nachricht säubern und zustellen
<b>Virus in DOC Datei der Rechtsabteilung gefunden (<i>kann nicht gesäubert werden</i>)</b>	➔ Nachricht in den Quarantäne Bereich der Rechtsabteilung stellen und den Empfänger sowie die Administration informieren
<b>Nachricht verschlüsselt</b>	➔ Nachricht in einen isolierten Quarantäne Bereich stellen und den Empfänger sowie die Administration informieren
<b>Nachricht nicht untersuchbar</b>	➔ Inhalt der Nachricht als Plain-Text dem Empfänger zustellen, original Nachricht in einen isolierten Quarantäne Bereich stellen und die Administration informieren

*AntiVirus Solution, dynamische Richtlinien*

## Managebare Quarantäne-Bereiche für Viren

Jedes Quarantäne-System von Message Solution kann weiter in beliebige Quarantäne-Bereiche, in Abstimmung mit bereits erstellten Richtlinien, unterteilt werden. Dabei entsteht eine, in der anomaliebasierten Nachrichtenverwaltung, bisher nicht erreichte Transparenz. Jeder erstellte Quarantäne-Bereich ist einzeln verwaltbar. Administratoren können nach bestimmten Nachrichten-Anomalien suchen, virulente Nachrichten sicher und isoliert downloaden, Quarantäne-Zeiten festlegen, Nachrichten in Archive überführen und vieles mehr.



## Frequently asked question:

### Was bedeutet 7x24 Antivirus Research Labs?

- Mit 7x24 Antivirus Research Labs sind Antiviren Forschungszentren gemeint die 7 Tage die Woche und 24 Stunden am Tag einsatzbereit sind (also rund um die Uhr).

### Was sind Nachrichten-Anomalien?

- Nachrichten-Anomalien sind E-Mails die durch bestimmte Indikatoren besonders verhaltensauffällig sind. Z. B. wenn ein bestimmter Nachrichtentyp innerhalb von wenigen Minuten, weltweit überproportional ansteigt. Dabei ist es nicht zwingend notwendig dass auch sofort virulenter Code erkannt wird.

### Was ist ein Viren Risiko Fenster?

- Als Viren Risiko Fenster wird der Zeitabschnitt zwischen dem tatsächlichen Ausbruch eines Virus und der Erkennung durch ein Antiviren Research Lab, sowie die Bereitstellung von Gegenmitteln, bezeichnet.

### Was versteht man unter dem Begriff DoS oder DDoS?

- Der Begriff DoS ist ein Akronym und steht für „Denial of Service attack“ (zu Deutsch in etwa Dienstverweigerungs-Angriff). Damit sind Angriffe gemeint die sich gegen ein System richten, mit dem Ziel einen oder mehrere Dienste, durch Überlastung arbeitsunfähig zu machen. Solche Angriffe erfolgen meistens durch eine größere Anzahl von Rechnern gleichzeitig. Man spricht deswegen auch von DDoS bzw. „Distributed Denial of Service attacks“.

### Was sind polymorphe Viren?

- Als polymorphe Viren werden Viren bezeichnet, die die Fähigkeit haben sich selbst zu verändern um ihre Erkennung zu verhindern.

### Was verbirgt sich hinter dem Begriff „malicious code“?

- „malicious code“ oder malware steht als Oberbegriff für alle Arten von bösartiger Software wie z. B. Viren, Trojanische Pferde oder Würmer.

### Was ist eine E-Mail-Pipeline?

- Eine E-Mail-Pipeline ist ein, in Message Solution, definierter Nachrichtenweg. Eine E-Mail-Pipeline zwingt Nachrichten bestimmte Wege über frei definierbare Message Solution Instanzen zu nehmen.

### Was sind Richtlinien in Verbindung mit Message Solution?

- Richtlinien sind unumgängliche Regeln (Security-Policys) die in Message Solution festgelegt werden können um Nachrichten zu kontrollieren.

### Was sind Quarantäne-Systeme?

- Quarantäne-Systeme sind physisch eigene Bereiche in Message Solution, in denen verhaltensauffällige oder virulente Nachrichten isoliert werden.

# „good messages, every day“



MESSAGE  
SOLUTION

## Kontakt

Für Fragen, Anmerkungen und weitere Informationen stehen wir Ihnen auch gerne persönlich zur Verfügung:

Message Solution  
Biegenstr. 20  
D-35037 Marburg  
Tel.: +49 (0) 6421 / 175 17 60  
Fax: +49 (0) 6421 / 175 17 69  
E-Mail: [sales@message-solution.com](mailto:sales@message-solution.com)  
Web: <http://www.message-solution.com>