

Marshal Email Gateway Security

MailMarshal™ SMTP 6.4 – E-Mail-Sicherheit der Enterprise-Klasse für mittelständische Unternehmen

Die Beachtung aller E-Mail-Sicherheitsaspekte, wie Schutz vor Spam und Viren, die Einhaltung von Richtlinien und die Vermeidung von Datenlecks, kann mittelständischen Unternehmen als schier unlösbar erscheinen. Mit MailMarshal SMTP finden Sie eine kompakte Lösung, die alle benötigten Sicherheitsfunktionen aufweist und sowohl heute als auch in Zukunft nur minimalen Verwaltungsaufwand erfordert.

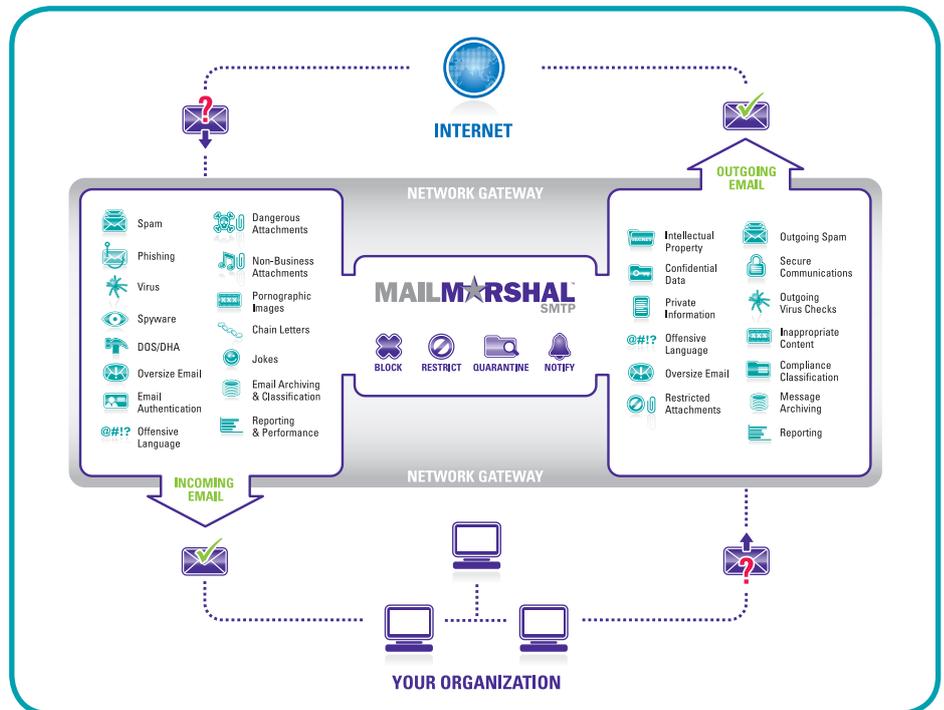
ÜBERBLICK

MailMarshal SMTP ist eine E-Mail-Sicherheitslösung für mittelständische Unternehmen. Die einzelne, flexible und einfach zu verwaltende Lösung vereint Schutz vor E-Mail-Bedrohungen, Content-Security, Richtliniendurchsetzung und Vermeidung von Datenlecks.

MailMarshal fungiert als E-Mail-Gateway für Ihr Unternehmen und filtert den gesamten eingehenden und ausgehenden E-Mail-Verkehr am Rand Ihres Netzwerks/des Internets. MailMarshal sperrt eingehende E-Mail-Bedrohungen wie Spam, Phishing, Viren, Malware und Denial-of-Service-Angriffe. MailMarshal sorgt außerdem für die Durchsetzung von Nutzungsrichtlinien und die Einhaltung von Richtlinien zum Schutz vor Datenverlust. MailMarshal bietet Ihnen Funktionen der Enterprise-Klasse in einer erschwinglichen Lösung für mittelständische Unternehmen.

DIE WICHTIGSTEN FUNKTIONEN

- Unübertroffener Schutz vor Spam, Phishing, Viren und Malware
- Schutz vor Denial-of-Service- und Directory-Harvest-Angriffen
- Content-Security für eingehende Daten
- Richtliniendurchsetzung und Regeleinhaltung für ausgehende Daten
- Schutz vor Datenlecks
- Sichere Verschlüsselung von E-Mails
- Nachrichtenarchivierung
- Erkennung pornografischer Bilder (optional)
- Berichterstellung und Nachrichtenklassifizierung
- Einfache Administration



DIE WICHTIGSTEN VORTEILE

MailMarshal schützt Ihr E-Mail-Gateways vor allen Bedrohungen

Sie gewinnen den wahren Geschäftswert Ihres E-Mail-Systems zurück, da es wieder sicher und wirtschaftlich in der Nutzung wird. MailMarshal schützt vor allen E-Mail-Bedrohungen und sperrt z. B. Spam, Phishing-Mails, Viren, Trojaner, Würmer, Denial-of-Service- und Directory-Harvesting-Angriffe sowie gespooftete E-Mails.

Niedrige Gesamtbetriebskosten

Umfassende und aussagekräftige Verwaltungsberichte stellen die Wirksamkeit der Anti-Spam- und Sicherheitsmaßnahmen heraus und kennzeichnen mögliche Regelverletzungen, so dass der Systemadministrator von einer schnellen Kapitalrendite profitiert.

Low Total Cost of Ownership

Einfache Bereitstellung, minimale Verwaltungskosten und Konsolidierung aller E-Mail-Sicherheitsfunktionen in nur einer Verwaltungsschnittstelle zusammen mit Zero-Day-Sicherheitsupdates und detaillierter,

jedoch klarer Berichterstellung, haben MailMarshal gemeinsam zur bevorzugten E-Mail-Sicherheitslösung gemacht.

Ermöglicht die Regeleinhaltung und die Vermeidung von Datenlecks

Mit MailMarshal können Unternehmen das Senden vertraulicher Informationen per E-Mail auf bestimmte Personen und Daten einschränken, um diese Angaben vor neugierigen Augen zu schützen. MailMarshal ermöglicht außerdem eine kontextbezogene E-Mail-Archivierung. So werden etwa alle Nachrichten zu einem bestimmten Thema oder die gesamte E-Mail-Korrespondenz mit bestimmten Domänen separat abgespeichert.

Bietet Schutz vor Haftungsansprüchen

Unangemessene oder anstößige Inhalte werden aus eingehenden E-Mails herausgefiltert und ausgehende Mails werden automatisch auf Regeleinhaltung geprüft. Mit MailMarshal können mittelständische Unternehmen nachweisen, dass alle angemessenen Maßnahmen ergriffen wurden, um die Mitarbeiter zu schützen und Sicherheitsrichtlinien korrekt umzusetzen.

Marshal Email Gateway Security

MailMarshal™ SMTP 6.4 – E-Mail-Sicherheit der Enterprise-Klasse für mittelständische Unternehmen

Verbessert die Netzwerkeffizienz und spart Kosten

Durch die Überwachung der Bandbreitennutzung hält MailMarshal die Netzwerkleistung auf einem einheitlichen Niveau und verhindert eine nicht geschäftsbezogene Verwendung von E-Mails.

Verbessert die Produktivität der Mitarbeiter

Der Einsatz von MailMarshal bedeutet, dass Mitarbeiter weniger Zeit mit der Verwaltung von Spam verbringen. Dies trägt zur Durchsetzung der Nutzungsrichtlinien bei, um das Senden persönlicher E-Mails oder andere zeitaufwändige, nicht arbeitsbezogene Aktivitäten zu überwachen.

Schützt den Ruf des Unternehmens

MailMarshal verhindert die unberechtigte Verbreitung vertraulicher oder kritischer Informationen per E-Mail und stellt sicher, dass die Benutzer Ihr Unternehmen nicht durch unangemessene Inhalte oder Datenlecks per E-Mail in Verruf bringen können.

Schafft ein sichereres Arbeitsumfeld für Mitarbeiter

Durch die konsequente und sorgfältige Anwendung von Sicherheits- und Nutzungsrichtlinien lassen sich Probleme wie sexuelle oder rassistische Belästigung per E-Mail vermeiden.

TECHNISCHE MERKMALE – SCHUTZ VOR BEDROHUNGEN

Schutz vor Spam und Phishing

- Die Anti-Spam-Engine von MailMarshal kombiniert mehrschichtige Spam-Filter miteinander und bietet so unübertroffenen Schutz, Leistung und Genauigkeit.
- Zuverlässige Spam-Erkennungsrate von 99,5 % bei weniger als 0,001 % Fehlalarmen, bei minimalem Tuning- oder Verwaltungsaufwand.
- Unterstützung der IP Reputation Services (Schwarze/Weiße Listen) und DNSBL-Datenbanken wie Spamhaus, mit einzigartigen Automated Adaptive Whitelists, um auszuschließen, dass E-Mails von bekannten Partnern gesperrt werden.

IM MAILMARSHAL CONFIGURATOR DEFINIEREN SIE DIE RICHTLINIEN IHRES UNTERNEHMENS. DER CONFIGURATOR ERMÖGLICHT SCHNELLEN UND EINFACHEN ZUGRIFF AUF EINE REIHE VON RICHTLINIENELEMENTEN, WIE STANDARDWÖRTERBÜCHER ZUR LEXIKALISCHEN ANALYSE VON E-MAIL-KONTEN

DIE SEITE MAILMARSHAL CONSOLE TODAY ENTHÄLT EINE DASHBOARD-ANSICHT IHRER E-MAIL-UMGEBUNG MIT EINGEGANGENEN, GESENDETEN UND ISOLIERTEN NACHRICHTEN. DIE WICHTIGSTEN BEDROHUNGEN DES TAGES, WIE SPAM, VIREN UND WEGEN REGELVERSTÖßEN GESPERRTE NACHRICHTEN WERDEN DETAILLIERT ANGEZEIGT

- Umfassende Anti-Spam-Berichterstellung, einschließlich individualisierter Berichte für Mitarbeiter und Freigabe aus der Spam-Quarantäne für Endbenutzer.

Schutz vor Viren und Malware

- Mehrschichtige Antiviren-Strategie, basierend auf der nahtlosen Integration einer Reihe unterstützter Antiviren-Anbieter, wie z. B. McAfee, Norman, Sophos, Symantec und anderen.
- Unterstützt die Integration dedizierter Anti-Spyware-Scanner, darunter CounterSpy und PestPatrol.
- Erkennt und dekomprimiert Archivdateitypen und ermittelt Viren, die in mehrfach komprimierte Dateien eingebettet sind.
- Identifiziert und sperrt gefährliche Dateitypen anhand des Inhalts anstatt des Dateinamens oder der Erweiterung, um

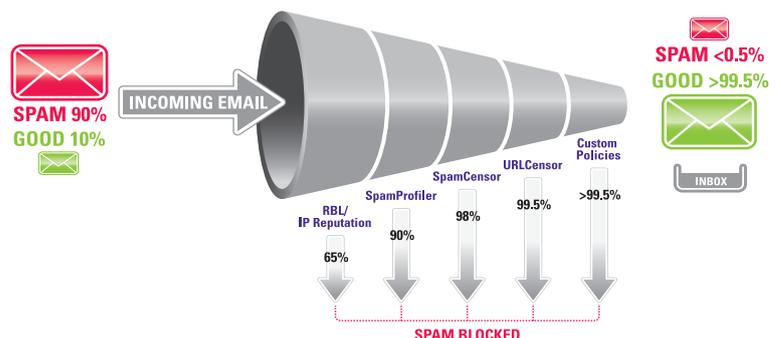
absichtlich falsch benannte Anhänge zu entdecken.

- Erkennt und isoliert Nachrichten, die potenziell schädlichen Code oder Links zu bekannten gefährlichen Websites enthalten.
- Wendet den Virenschutz auf ein- und auf ausgehende E-Mails an und bietet umfassende Berichterstellung bezüglich Viren und Malware.

Schutz vor Denial-of-Service- und Directory-Harvest-Angriffen

- Erkennt und behandelt untypisches Verhalten, wie etwa schnelle gleichzeitige Verbindungen von einer einzelnen IP-Adresse oder mehrere E-Mails, die an ungültige E-Mail-Adressen gesendet werden.
- Nach Erkennung verdächtiger Denial-of-Service- oder Directory-Harvesting-

MAILMARSHAL ANTI-SPAM ENGINE



Marshal Email Gateway Security

MailMarshal™ SMTP 6.4 – E-Mail-Sicherheit der Enterprise-Klasse für mittelständische Unternehmen

Angriffe werden Verbindungsversuche des entsprechenden SMTP-Servers zurückgewiesen. Nach einer definierten Zeitspanne wird der normale Dienst automatisch wieder aufgenommen.

TECHNISCHE MERKMALE – FILTERN VON INHALTEN

Umfassende Sicherheit

- Setzt jede Richtlinie auf der Basis nahezu jedes Nachrichtenattributs durch. Nachrichtensteuerung anhand folgender Kriterien:
 - Wer ist an der Nachricht beteiligt? (Absender, Empfänger, Quell-IP-Adresse oder Ursprungsland)
 - Was ist in der Nachricht enthalten? (Spam, Malware, Schlüsselwörter und Wendungen, Größe der Nachricht, Dateianhänge, alphanumerische Muster)
 - Welche Maßnahmen sollen ergriffen werden? (Sperrungen, löschen, archivieren, verzögern, verschlüsseln, kopieren, eine E-Mail-Adresse benachrichtigen, Anhang löschen, Nachricht für Berichterstellung klassifizieren)
- Prinzipiell lässt sich jede gewünschte Richtlinie automatisch mit MailMarshal durchsetzen.

Content-Security für eingehende Daten

- Ergreifung einer Reihe von Maßnahmen für eingehende E-Mail-Nachrichten anhand einer bestimmten vordefinierter Bedingung.
- Zurückweisung von Nachrichten, die eine bestimmte Größenbegrenzung überschreiten oder deren IP-Adresse, Domäne oder Land sich auf der Schwarzen Liste befindet.
- Steuerung eingehender Nachrichten anhand des Vorhandenseins unzulässiger Dateitypen, der Anzahl von Anhängen oder unangemessener Schlüsselwörter (wie z. B. vulgärer, rassistischer oder sexistischer Ausdrücke).
- Implementierung von Richtlinien gemäß Benutzer, Abteilung, Domäne, bestimmter Gruppe oder für das gesamte Unternehmen.

- Verdeutlichung der Sicherheit eingehender E-Mails durch umfassende Berichterstellung und E-Mail-Benachrichtigungen.
- Verwaltung der E-Mail-Authentifizierung und Anti-Spoofing über Unterstützung von Normen für die Absender-ID und Absenderrichtlinienumgebung

Richtliniendurchsetzung und Regeleinhaltung für ausgehende Daten

- Wendet automatisch Richtlinien auf ausgehende Nachrichten an.
- Setzt Richtlinien gemäß Größe der ausgehenden Nachricht, Anhängen, Schlüsselwörtern oder Empfänger durch.
- Sperrt profane oder unangemessene Sprache in ausgehenden E-Mails.
- Setzt Unternehmensrichtlinien durch, damit die Nachrichten rechtliche Anforderungen erfüllen.
- Fügt automatisch einen Haftungsausschluss ein oder verschlüsselt die Daten anhand der Richtlinien.
- Archiviert automatisch die gesamte ausgehende (und eingehende) Korrespondenz, um alle gesetzlichen Verpflichtungen zu erfüllen.
- Bietet umfassende Berichte zu ausgehenden E-Mail-Inhalten und versuchten Richtlinienverletzungen.
- Bietet Beispiel-Richtlinienvorlagen, beispielsweise zu SOX und HIPAA.

Schutz vor Datenlecks

- Bietet eine speziell für die Verteilung vertraulicher Dateien und geistigen Eigentums konzipierte Fingerabdruck-Technologie.
- Isoliert Dateien, die von unbefugten Benutzern gesendet wurden, und benachrichtigt die benannten E-Mail-Adressen.

Sichere E-Mails

- Bietet integrierte TLS-Verschlüsselung zwischen Gateways, um vertrauliche

Daten zu schützen und sicherzustellen, dass Richtlinienanforderungen eingehalten werden.

- Lässt sich an ein optionales S/MIME-PKI-Verschlüsselungsmodul, MailMarshal Secure, anbinden. MailMarshal Secure bietet umfassende E-Mail-Verschlüsselungsfunktionen mit vollständiger Zertifikats-/Schlüsselverwaltung und pflegt automatisch die Verschlüsselungsbenutzergruppen per LDAP.

Nachrichtenarchivierung

- Archiviert täglich und automatisch eingehende/ausgehende Nachrichten.
- Ermöglicht das Archivieren von Nachrichten anhand von Bedingungen, z. B. von wem die Nachricht stammt und worauf sie sich bezieht.
- Ermöglicht die unbegrenzte Archivierung von Nachrichten oder das automatische Löschen nach einem definierten Aufbewahrungszeitraum.
- Findet wichtige Nachrichten mit umfassenden Suchfunktionen und ermöglicht vollständige Berichterstellung über archivierte Nachrichten.

Erkennung pornografischer Bilder (optional)

- Image Analyzer™ ist ein optionales Modul zur Erkennung unangemessener oder pornografischer Bilder per tiefer Bildanalyse.
- Die Erkennung pornografischer Bilder lässt sich auf eine Reihe unterstützter Bildformate anwenden.
- Image Analyzer trägt dazu bei, die Darstellung anstößiger Inhalte zu verhindern und schult die Benutzer bezüglich angemessener Inhalte.

Berichterstellung und Nachrichtenklassifizierung

- Bietet umfassende Sicherheit und Berichterstellung über E-Mail-Aktivitäten.

Marshal Email Gateway Security

MailMarshal™ SMTP 6.4 – E-Mail-Sicherheit der Enterprise-Klasse für mittelständische Unternehmen

- Überprüft Bandbreitenberichte anhand von Absender, Empfänger, Domäne und Dateityp.
 - Analysiert die Anti-Spam-Leistung pro Benutzer über individualisierte webbasierte Berichte.
 - Ermöglicht das Sortieren und Speichern von Nachrichten anhand des Inhalts und das Erstellen von Berichten über gespeicherte Nachrichten zu Prüfzwecken.
 - Zeigt die Anti-Spam-/Antiviren-Leistung und versuchte Richtlinienerletzungen an und identifiziert potenzielle E-Mail-Übergreifer anhand von Sicherheitsberichten.
- Synchronisierung von E-Mail-Konten.
- Enthält intuitive Suchfunktionen, die dem Benutzer bei der Suche nach Nachrichten in Quarantäne helfen, aber verhindern, dass potenziell gefährliche Nachrichten (wie etwa ein Virus) versehentlich in Ihrer Umgebung wiederhergestellt werden.
 - Stellt sicher, dass Sie über Ihr gesamtes E-Mail-System informiert sind, angefangen bei der Bandbreitennutzung pro Einzelbenutzern bis hin zu den 10 häufigsten Regelverstößen in der vorangegangenen Woche sowie umfassender und aussagekräftiger Berichterstellung.

Einfache Administration

- Bietet vorkonfigurierte Standardrichtlinien für alle Bedrohungen – von Spam bis hin zu Viren, übergroßen Nachrichten und unangemessener Ausdrucksweise.
- Ermöglicht das einfache Definieren neuer Richtlinien in leicht verständlicher Sprache mit einem Assistenten für die Regelerstellung, der den Benutzers schrittweise durch die Erstellung benutzerdefinierter Richtlinien führt (vergleichbar mit Microsoft Outlook-Regeln).
- Die Seite MailMarshal Today bietet Informationen über Ihre E-Mail-Umgebung im Überblick, die Sie auf mögliche Probleme hinweisen.
- Einfaches Setup unterstützt die Einbindung von LDAP und Active Directory für den Import und die automatische

SYSTEMVORAUSSETZUNGEN

Prozessor - Mind. Pentium 4

Festplattenspeicher - Mind. 10 GB (NTFS)

Arbeitsspeicher - Mind. 512 MB

Betriebssystem - Windows Server Standard; Enterprise 2003; Windows XP Professional SP1 oder höher

Datenbank (optional) - MSDE 2000 SP3a oder höher; SQL 2005 Express; Microsoft SQL Server 2000 SP3a oder höher; SQL Server 2005 Microsoft Data Access Components (MDAC) 2.7 oder höher

Bitte beachten Sie: MailMarshal SMTP unterstützt keine 64-Bit-Versionen von Windows

TESTVERSION

Marshal bietet eine kostenlose Testversion von MailMarshal SMTP. Besuchen Sie uns unter www.marshal.com und klicken Sie auf Evaluation Center, um eine kostenlose und voll funktionsfähige Testversion

CONTACT MARSHAL

EMEA

Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email: emea.sales@marshal.com

Americas

Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404-564-5800
Fax: +1 404-564-5801

Email: americas.sales@marshal.com

Asia-Pacific

Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com

info@marshal.com | www.marshal.com

MARSHAL™
Secure. Protect. Comply.