mailDefend

Managed Mail Security von Medialine
maximaler Spamschutz – maximale Sicherheit – kein Administrationsaufwand

*** Stand: 01. Februar 2017**

Warum Managed Mail Security?

Keine unerwünschten oder schadhaften E-Mails auf dem eigenen Mailserver empfangen – das ist der offensichtliche und simple Vorteil eines Spamfilters. mailDefend von Medialine leistet noch wesentlich mehr. Die wichtigsten Vorteile hier auf einen Blick:

Transparenz und Kontrolle

Mit Medialine mailDefend bestimmen Sie die Rahmenbedingungen für die E-Mail-Kommunikation Ihres Unternehmens. Mit maximaler Transparenz und maximaler Kontrolle erfüllen Sie so die Anforderungen an zeitgemäße Kommunikation im und aus dem Unternehmen – compliancegerecht und sicher.

Bedienerfreundlich und Einfach

Für Benutzer ist es wichtig, dass die Bedienung des Spamfilterservices möglichst zeitsparend und einfach erfolgt und sie nicht aus ihrem Arbeitsalltag herausgerissen werden. mailDefend erspart Benutzern das zeitaufwändige Löschen unerwünschter E-Mails und gewährleistet eine einfache Bedienung der Services.

Sicherung und Aufbewahrung

Mit einer Falsch-Positiv-Rate unter 0,00015 pro Clean-Mail gewährleistet mailDefend, dass die richtigen Nachrichten in Ihrem Postfach landen. Sollte Ihr Mailserver einmal nicht erreichbar sein, werden eingehende E-Mails bis zu 7 Tage für den Empfänger vorgehalten und bei Erreichbarkeit automatisch zugestellt.

Ausfallsicherheit und Archivierung

Mit dem optionalen Continuity Service können Nutzer auch bei Ausfall Ihres Mailservers weiter E-Mails empfangen und senden. Der zusätzlich buchbare Archivierungsservice beinhaltet die revisionssichere Speicherung aller ein- und ausgehenden Nachrichten.

Schutz und Sicherheit

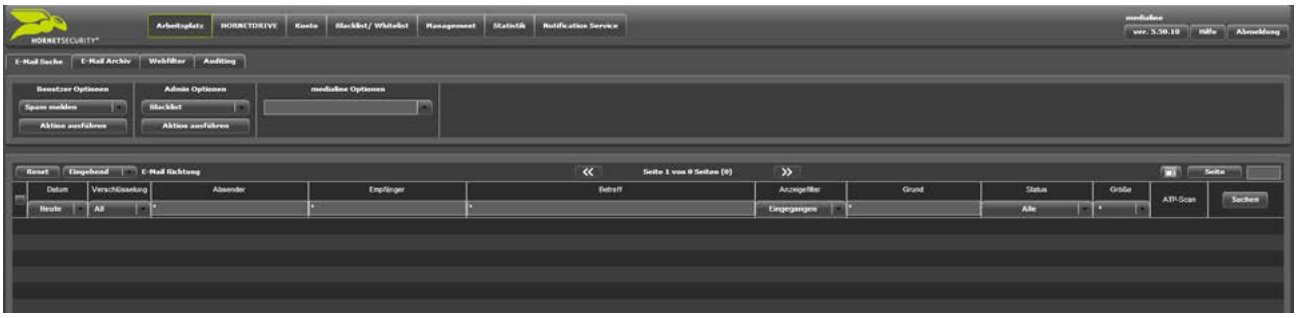
Mit einer garantierten Spamerkennung von 99,9% und einer Virenerkennung von 99,99% bietet der Spamfilter von Medialine mailDefend die höchsten Erkennungsraten am Markt. Er umfasst ebenso den Schutz der Mailserver vor DDoS-Angriffen wie auch den Schutz der Nutzer vor Phishing. Über 95% aller Spammails werden bereits beim Eintreffen blockiert und in der Quarantäne übersichtlich gesammelt.

Zeitersparnis und einfache Verwaltung

Die Anforderungen an IT-Administratoren wachsen: bei steigender Komplexität von IT-Systeme werden die Angriffe auf die IT-Sicherheit immer häufiger und intelligenter. Gleichzeitig steigen gesetzliche und regulatorische Anforderungen. Mit Medialine mailDefend erledigen Sie die Kernaufgabe eines sicheren Mailverkehrs ohne administrativen Aufwand.

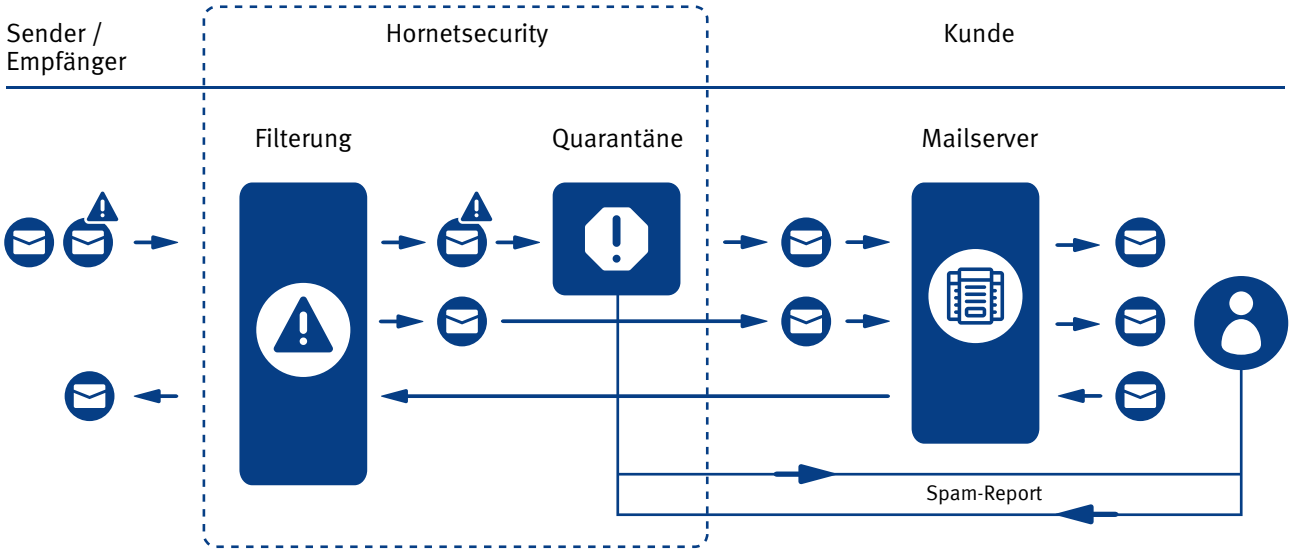
mailDefend Control Panel

Das Control Panel ermöglicht Nutzern und Administratoren den einfachen Überblick über den gesamten E-Mail-Verkehr. Mit der integrierten Volltext-Suchfunktion lassen sich E-Mails leicht auffinden und anschließend zustellen, als Spam klassifizieren oder einer Black- oder Whitelist zuordnen.



Ablauf des Spam-Managements

Eingehende E-Mails werden in einem dreistufigen Prozess geprüft: Ein Großteil der Spam-Nachrichten werden bereits im Blocking-Stadium zurückgewiesen. Die übrigen Mails erreichen die aktive Analyse, in welcher der E-Mail-Strom durch eine Vielzahl von Filterregeln gereinigt wird. Als dritte Stufe kann der Nutzer auf die Quarantäne zugreifen und vereinzelte unklare E-Mails prüfen.



Integrierte Leistungen	Beschreibung
Spamerkennung	Durch marktführende Erkennungs- und Filterraten landen nur noch erwünschte E-Mails im Postfach des Nutzers. 99,9 % garantierte Spamerkennung; weniger als 0,00015 Falsch-Positive pro Clean-Mail
Virenerkennung	Voneinander unabhängige, mehrfache Filterung gewährleistet optimalen Schutz vor bekannter und neu auftretender Schadsoftware. Fünf unabhängige Viren- und Phising-filter garantieren eine Virenerkennung von 99,99 %.
Verschlüsselung des Datenverkehrs	Das Ausspähen Ihrer Daten beim Transport durch das World Wide Web wird verhindert. Der Transportweg zwischen unseren verarbeitenden Systemen und Ihrem E-Mail-System ist TLS verschlüsselt.
Flexible Größenbegrenzung	Schutz Ihres Mailservers vor Beeinträchtigungen durch zu großes Datenvolumen von ein- und ausgehenden E-Mails.
Bounce-Management	Effektiver Schutz vor Backscatter- und Bounce-Attacken.
Content-Filter	Wirksamer Schutz individuell abgestimmt auf Ihre Firmenpolicies. Blockierung von Dateien in zahlreichen Formaten, wobei der File-Typ sowohl über die innere Struktur der Datei als auch über Name und Erweiterung bestimmt wird. Filterbare Formate: ausführbare Dateien (EXE,SYS, DLL und andere); Microsoft Office Dokumente (DOC, DOT, DOCX, XLS, XLT, XLSX, PPT, PPS, PPTX usw.); RTF-Dokumente; Archive ZIP, RAR und ARJ; Videodateien (AVI, MPG); Musikdateien (MP3, OGG).
Umfangreiche Statistiken	Behalten Sie den Überblick über Ihren Mailverkehr und die Effektivität des Spamfilters.
Schutz vor DHA	Schutz Ihrer E-Mail-Server vor Directory Harvesting Attacken (DHA). DHA belasten den E-Mail-Server stark und vermindern seine Durchlassfähigkeit.
Maximaler Empfängerschutz	Durch Filterung ausgehender E-Mails auf Viren/Spam schützen Sie sich und die Empfänger Ihrer E-Mails vor unbemerktem Versand von Malware über Ihre Mailserver.
Umfangreiche Reports	Reporting: Eingehende Mails, Ausgehende Mails, „Top-10“ (Top-10 Spamquellen, Top-Ten Adressaten, uvm.), ganzheitlicher Hauptbericht mit allen Daten.
Prüfung formaler Merkmale	Die Anwendung erkennt Spam anhand von typischen Merkmalen: Modifikation der Absenderadresse, Fehlen einer dazugehörigen IP-Adresse im DNS, unangemessen große Empfängerzahl, Verbergen der Empfängeradressen, ungewöhnliches Format und Größe der Mitteilung.
SMTP-Status Anzeige	Überprüfung des Verbleibs zugestellter E-Mails anhand der Message ID im Zielserver.
Anpassung an Ihr Corporate Design	Design-Anpassung von Control Panel, Benachrichtigungs-E-Mails und Reports.

Zusatzleistungen (1)	Beschreibung
Revisionssicherheit	Rechtskonforme Speicherung des Mailverkehrs durch zusätzlichen Archivierungsservice.
Abwehr von Advanced Threats	Mit der zusätzlichen Advanced Threat Protection (ATP) werden eingehende Mails weiterführenden Analysen unterzogen. Wappnen Sie sich mit ATP gegen Targeted Attacks, Ransomeware, Blended Attacks und digitale Spionage und nutzen Sie Real Time Allerts um im Ernstfall in Echtzeit eingreifen zu können.
Verschlüsselter E-Mail-Inhalte	Der optionale Verschlüsselungsservice via S/MIME-Zertifikat oder PGP übernimmt Ihr komplettes Zertifikatsmanagement. Ver-/Entschlüsselung und Signierung erfolgen automatisch und transparent ohne Benutzereingriffe. Schützen Sie ihr Unternehmen vor Ausspähung und erlangen Sie maximale Compliance, Transparenz und Kontrolle über den gesamten verschlüsselten Mailverkehr – ganz ohne Archivierungsdatenblatt.

(1) Optional zubuchbar und kostenpflichtig

Advanced Threat Protection – Ihre Vorteile im Detail

Sicherer Schutz vor Ransomware & Co. – mit dem mailDefend Zusatzservice Advanced Threat Protection (ATP) schützen Sie ihr Unternehmen effektiv vor Angriffen wie CEO-Fraud, Ransomware und Phishing.

Die Gefahren in der digitalen Welt wachsen. Angreifer und Systeme werden intelligenter, die Bedrohungen vielfältiger und ausgeklügelter. Um Ihr Unternehmen wirkungsvoll vor Maleware und Cyberattacken zu schützen, müssen Sie Ihr Unternehmen gezielt und zeitgemäß dagegen wappnen. Der mailDefend Zusatzservice Advanced Threat Protection rüstet Sie topaktuell und umfassend gegen Bedrohungen und hilft Ihnen schützenswerte Informationen Ihres Unternehmen effektiv zu abzusichern.

Ganz persönlich: Targeted Attacks

Hochrangige Mitarbeiter werden immer öfter Ziel individueller Angriffe, sogenanntem Spearphishing, Whaling oder auch CEO Fraud. Auf herkömmlichem Weg bleiben diese Attacken nahezu immer unerkannt, da Sie altbewährte Sicherheitssysteme spielend umgehen. ATP bietet dagegen ein umfassendes Paket an Erkennungsmechanismen, um diese Art von Angriffen effektiv zu unterbinden.

Geschickt verbreitet: Blended Attacks

Bei Blended Attacks kombinieren die angreifer eine vilzahl von Angriffswegen. So enthält beispielsweise eine mail einen Dateianhang, der wiederum einen Link zum Download der Malware Dateien enthält. ATP geht mit einer ebneso umfangreichen wie wirkungsvollen Kombination dagegen vor: URL-Scan, URL-Rewriting, Sandboxing und Freezing bieten die optimale Abwehrstrategie für solch vielseitige Angriffsszenarien.

Up-to-Date: Real Time Alerts

Mit den ATP Real Time Alerts werden Sie in Echtzeit über akute Angriffe auf ihr Unternehmen informiert. Dies ermöglicht die schnelle Einleitung interner Maßnahmen und juristischer Vorgehensweise. Sensibilisieren sie dank dieser Informationen frühzeitig Ihre Mitarbeiter, um so auch weitere Angriffe zum Beispiel per Telefon zu erkennen und abzuwehren. Sollten bereits zugestellte E-Mails nachträglich als potentiell schädlich erkannt werden, ermöglicht die Ex-Post-Alarmierung eine Untersuchung der betroffenen Konten oder Systeme.

Schnell verbreitet: Ransomware

Ransomware beschreibt sogenannte polymorphe Viren wie Locky, Tesla oder Petya. Sie können einzelne rechner oder ganze Netzwerke lahmlegen in dem Sie lokal gespeicherten Dateien verschlüsseln. Unter dem Einsatz von ATP werden diese nur schwer zu entdeckende Viren mit einer Sandbox-Engine und gezieltem Freezing enttarnt und lahmgelegt.

Ausgespäht: Digitale Spionage

Laut Umfrage des IT-Branchenverbandes Bitkom waren bereits 50% der deutschen Unternehmen von Datendiebstahl, Sabotage oder Spionage betroffen. Das mailDefend Spy-Out Forensiksystem erkennt bekannte und neuartige Muster zum Ausspähen von Informationen. Durch unmittelbare Reaktion und Information der Verantwortlichen können schützenswerte Informationen gesichert werden bevor sie das Unternehmen verlassen.