MEDIALINE

IT Security

mailDefend

Medialine Managed Mail Security
maximum spam protection - maximum security - no administrative effort

Why Managed Mail Security? Receiving no unwanted or harmful emails on your own mail server is the obvious and simple benefit of a spam filter. Medialine's mailDefend offers much more. The main advantages at a glance:

Transparency and Control

With Medialine mailDefend, you determine the conditions for the email communication of your company. With maximum transparency and maximum control, you meet the requirements for modern communication within and outside the company - compliant and secure.

User-friendly and simple

For users, it is important that the operation of the spam filter service is as time-saving and simple as possible and that they are not pulled out of their daily work routine. mailDefend saves users the time-consuming task of deleting unwanted emails and ensures easy operation of the services.

Backup and Storage

With a false-positive rate of less than 0.00015 per clean mail, mailDefend ensures that the right messages land in your inbox. If your mail server is not accessible, incoming emails will be held for up to 7 days for the recipient and delivered automatically when it becomes accessible.

High availability and archiving

With the optional Continuity Service, users can continue to receive and send emails even if their mail server fails. The additional archiving service includes the tamper-proof storage of all incoming and outgoing messages.

Protection and security

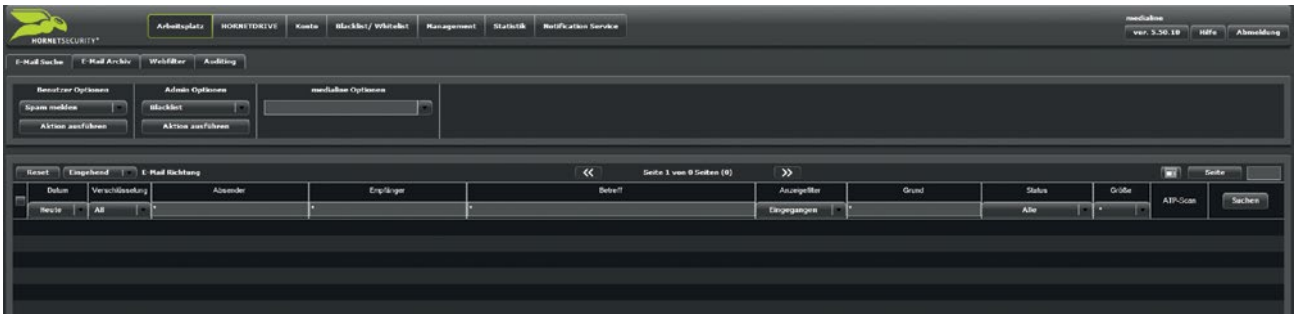
With a guaranteed spam detection rate of 99.9% and a virus detection rate of 99.99%, Medialine's mailDefend spam filter offers the highest detection rates on the market. It also includes protection of mail servers from DDoS attacks as well as protection of users from phishing. Over 95% of spam emails are blocked upon arrival and collected in quarantine in a clear overview.

Time savings and easy management

The demands on IT administrators are growing: as IT systems become more complex, attacks on IT security are becoming more frequent and intelligent. At the same time, legal and regulatory requirements are increasing. With Medialine mailDefend, you can handle the core task of a secure mail traffic without administrative effort.

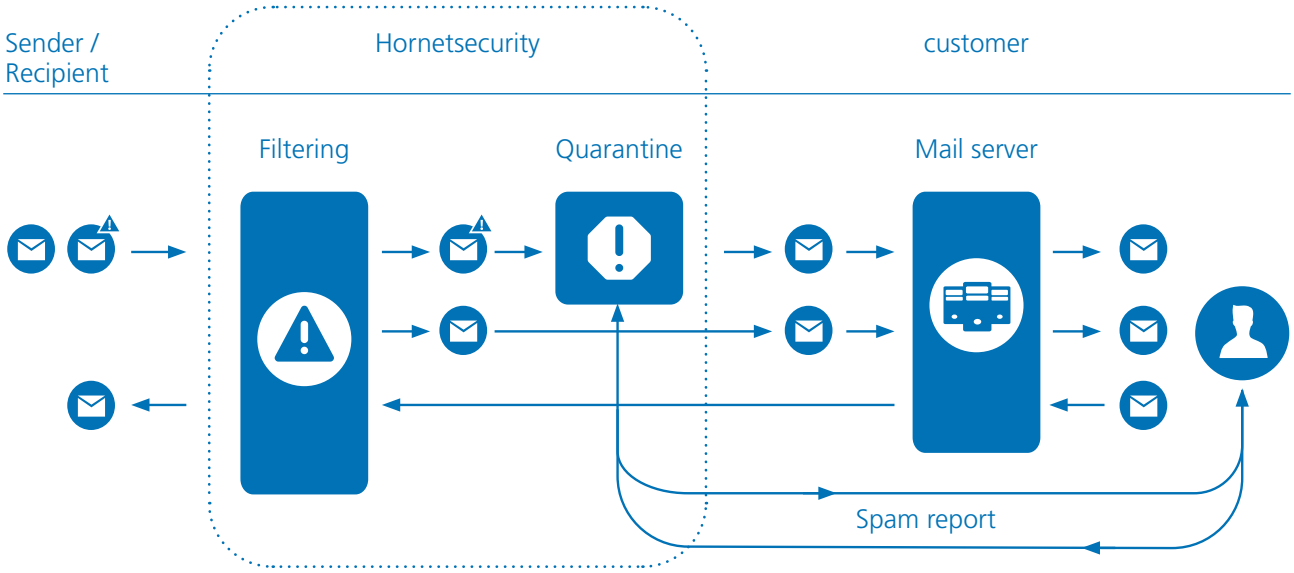
mailDefend Control Panel

The control panel allows users and administrators to easily monitor all email traffic. With the integrated full-text search function, emails can be easily found and then delivered, classified as spam, or assigned to a black or whitelist.



The spam management process

Incoming emails are checked in a three-stage process: A large majority of spam messages are rejected at the blocking stage. The remaining emails reach the active analysis stage, where the email flow is cleaned through a variety of filter rules. As a third stage, the user can access the quarantine and check individual unclear emails.



Integrated Services	Description
Spam detection	Market-leading detection and filtering rates ensure that only desired emails reach the user's inbox. 99.9% guaranteed spam detection, with less than 0.00015 false positives per clean email.
Virus detection	Independent, multiple filtering ensures optimal protection against known and new malware. Five independent virus and phishing filters guarantee a virus detection rate of 99.99%.
Traffic encryption	Your data is protected from spying while being transported on the World Wide Web. The transport path between our processing systems and your email system is encrypted with TLS.
Flexible size limitation	Protection for your mail server from disruptions caused by excessive data volume from incoming and outgoing emails.
Bounce-management	Effective protection against backscatter and bounce attacks.
Content filter	Effective protection tailored to your company policies. File blocking in various formats, determined by the file type, internal structure, name, and extension. Filterable formats include executable files (EXE, SYS, DLL, etc.), Microsoft Office documents (DOC, DOT, DOCX, XLS, XLT, XLSX, PPT, PPS, PPTX, etc.), RTF documents, ZIP, RAR, and ARJ archives, video files (AVI, MPG), and music files (MP3, OGG).
Comprehensive statistics	Keep track of your email traffic and the effectiveness of the spam filter.
DHA protection	Protect your email servers from directory harvesting attacks (DHA), which heavily burden the email server and reduce its capacity.
Maximum recipient protection	Filtering outgoing emails for viruses/spam protects you and the recipients of your emails from unnoticed distribution of malware via your mail servers.
Comprehensive reports	Reports on incoming emails, outgoing emails, "top 10" (top 10 spam sources, top ten recipients, etc.), overall main statistics, and more.
Checking formal characteristics	The application recognizes spam based on typical characteristics: modification of the sender's address, lack of an associated IP address in the DNS, inappropriately large number of recipients, hiding of the recipient addresses, unusual format, and size of the message.
SMTP status display	Checking the whereabouts of delivered emails based on the message ID on the target server.
Adaptation to your corporate design	Design adaptation of control panel, notification emails and reports.

Additional Services[1]	Description
Audit-proof	Legally compliant storage of email traffic through an additional archiving service.
Defense against advanced threats	With the additional Advanced Threat Protection (ATP), incoming emails are subject to further analysis. Equip yourself with ATP against targeted attacks, ransomware, blended attacks, and digital espionage and use real-time alerts to intervene in case of emergency.
Encryption of email contents	The optional encryption service via S/MIME certificate or PGP takes over your complete certificate management. Encryption and signing take place automatically and transparently without user intervention. Protect your company from espionage and gain maximum compliance, transparency, and control over the entire encrypted email traffic – without archiving data sheet.

(1) Optional and subject to an additional fee.

Optional: Advanced Threat Protection : Your benefits in detail

Secure protection against ransomware & Co. - with the mailDefend add-on service Advanced Threat Protection (ATP) you effectively protect your company against attacks such as CEO-Fraud, Ransomware and Phishing.

The dangers in the digital world are growing. Attackers and systems are getting more intelligent, the threats are more diverse and sophisticated. To effectively protect your company against malware and cyber attacks, you need to arm your company specifically and in a timely manner. The mailDefend add-on service Advanced Threat Protection equips you with state-of-the-art and comprehensive protection against threats and helps you effectively secure valuable information of your company.

Highly personal: Targeted Attacks

High-ranking employees are increasingly becoming the target of individual attacks, so-called spearphishing, whaling, or CEO fraud. These attacks almost always remain undetected when using conventional methods, as they easily bypass tried and tested security systems. ATP, on the other hand, offers a comprehensive package of detection mechanisms to effectively prevent this type of attack.

Cleverly spread: Blended Attacks

In blended attacks, attackers combine a variety of attack paths. For example, an email may contain an attachment that in turn contains a link to download malware files. ATP deals with an equally comprehensive and effective combination of detection mechanisms to effectively prevent these types of attacks.

Up-to-date: Real time alerts

With ATP real time alerts, you will be informed in real-time about acute attacks on your company. This enables the swift implementation of internal measures and legal proceedings. With this information, you can sensitize your employees early on to recognize and defend against further attacks, for example, by phone. If e-mails that have already been delivered are subsequently identified as potentially harmful, the ex-post alert enables the affected accounts or systems to be examined.

Quickly spread: Ransomware

Ransomware refers to so-called polymorphic viruses such as Locky, Tesla or Petya. They can cripple individual computers or entire networks by encrypting locally stored files. With the use of ATP, these difficult to detect viruses are detected and disabled using a sandbox engine and targeted freezing.

Spied on: Digital espionage

According to a survey by the IT industry association Bitkom, 50% of German companies have already been affected by data theft, sabotage, or espionage. The mailDefend Spy-Out Forensics system detects known and new patterns for spying on information. Through immediate reaction and informing the responsible parties, valuable information can be secured before it leaves the company.

as of: 03/2021