

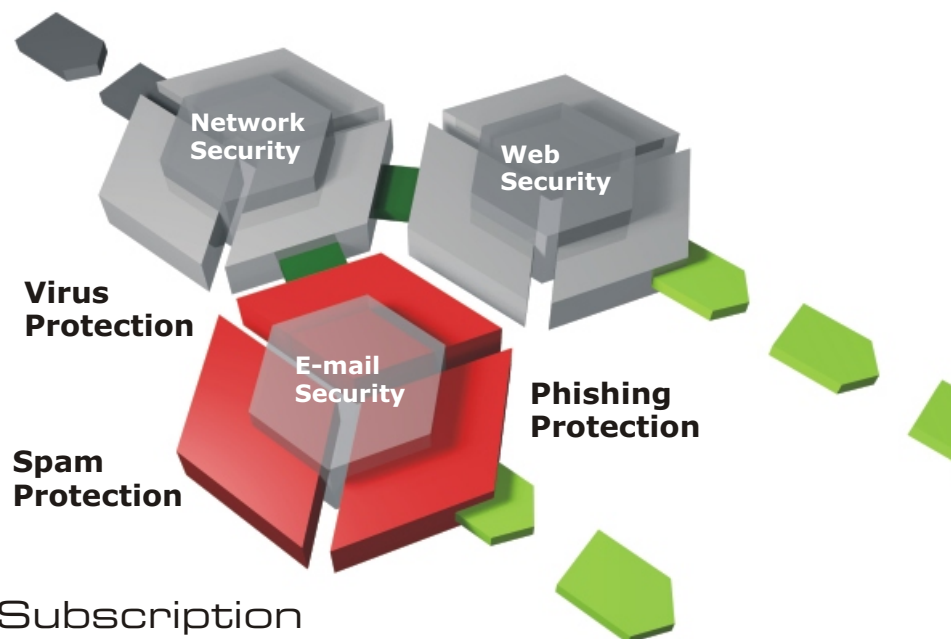
E-mail Security Subscription



E-mail Security

E-mail is a critical business tool. Unfortunately, it is also a major avenue for viruses, worms, and Trojans that can shut down computers and networks and cause the loss of critical data.

Lost productivity can be equally damaging. Opening and deleting spam messages can cost employees hundreds of hours every week. Phishing messages can lead to identity theft and the loss of confidential information.



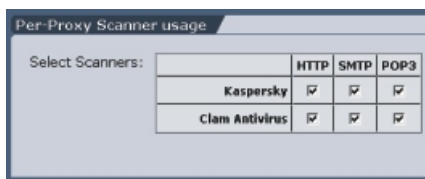
Astaro E-mail Security Subscription

- ▶ **Virus Protection for E-mail** catches viruses in SMTP and POP3 e-mails and attachments, even in compressed and archived formats.
- ▶ **Spam Protection** uses nine different techniques to filter out spam without stopping legitimate e-mails.
- ▶ **Phishing Protection** blocks e-mails from criminals trying to trick users into revealing confidential information.

Astaro's E-mail Security Subscription protects enterprises from computer viruses, spam, and phishing attacks transmitted through e-mail messages and attachments. Dual virus scanning engines and multiple spam and phishing detection methods provide the highest levels of protection. These applications are fully integrated with the other parts of Astaro Security Gateway appliances and software, so they are easy to deploy, configure and manage as part of a complete network security infrastructure.

Virus Protection for E-mail

Astaro's Virus Protection for E-mail application detects and blocks viruses in e-mail traffic. It scans inbound and outbound e-mail messages and e-mail attachments carried over industry-standard e-mail protocols (SMTP and POP3). Virus Protection for E-mail employs multiple detection methods and a database of over 100,000 virus signatures to ensure high accuracy and excellent performance.



Dual Virus Scanning Engines



Flexible Management

Dual Virus Scanning Engines

Astaro provides an extra margin of safety by including two virus scanning engines in sequence. Virus detection technology and signature databases from the ClamAV Open Source project and from anti-virus industry leader Kaspersky Lab provide a double layer of protection. Signature updates from

ClamAV's extensive user community, and from Kaspersky Lab's renowned international antivirus research team, ensure that new malware threats are identified and blocked as soon as they appear.

High Accuracy

Astaro's Virus Protection for E-mail utilizes three independent detection methods to catch the widest possible range of viruses:

- ▶ Virus signatures: E-mail messages and attachments are compared with known patterns contained in an extensive virus database.
- ▶ Heuristics: Sophisticated rules detect patterns and behavior that resemble known classes of viruses.
- ▶ Emulation: Suspicious code is executed in a protected environment, for example by unpacking archived files and by running scripts and macros.

There are no limits on the size of files scanned, the number of files scanned in parallel, or the amount of memory utilized for virus scanning.

Flexible Management

With Astaro's Virus Protection for E-mail, virus signatures can be updated automatically as often as hourly. Administrators can:

- ▶ Select which file formats to block in e-mail attachments.
- ▶ Select text strings to use to identify unwanted messages.
- ▶ Specify that messages with viruses should be quarantined for later evaluation or dropped.

Reports and detailed logs help administrators troubleshoot and identify patterns of activity.

Astaro's Virus Protection for E-mail complements desktop anti-virus packages by providing a single point of control where newly-discovered viruses can be blocked quickly, before they infect the internal network.

Complete Coverage

Astaro's Virus Protection for E-mail can open and scan more than 700 formats of archived and compressed files. Hackers and virus writers can not use obscure formats or complex archiving programs to sneak viruses into internal networks.

Embedded Mail Formats Supported:

Mime, MS Internet Mail, MS Mail, MS Outlook 5, Mail TNEF, and others.

Media Formats Supported:

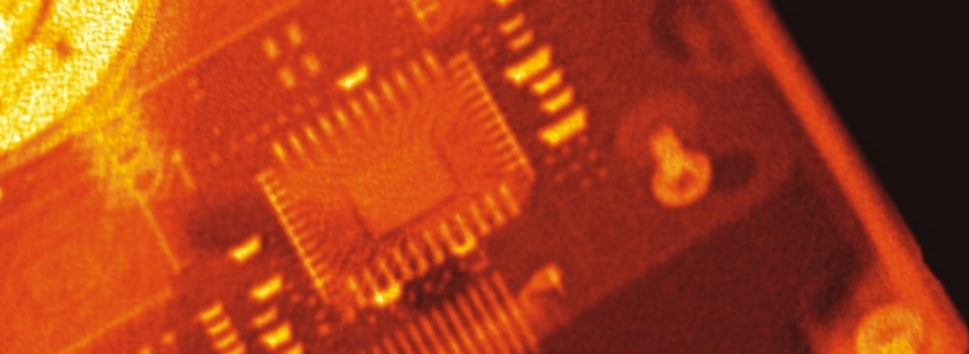
SYS, EXE, ELF, Java, HLP, OLE2, Access, Shell, Perl, XML, CHM, REG, WSF, LNK, VBA, WordBasic, PIF, VBS, BAT, HTML (including JavaScript, VBScript), MIRC.

Archive and Executable Formats Supported:

Astaro Virus Protection for E-mail can open and scan attachments in over 50 archive formats, including ARJ, GZIP, RAR, Tar, ZIP and CAB, and hundreds of packed executable formats.

Character Support:

All ANSI and Unicode based character sets.



Spam Protection

Astaro's Spam Protection application detects and blocks unsolicited e-mails. It uses multiple detection methods to pinpoint spam types while minimizing "false positives." It performs a series of tests and assigns a "spam score" to each message indicating the probability that the message is unsolicited. Messages whose score exceeds thresholds set by the administrator are dropped, returned to the sender, passed to the recipient with a warning, or quarantined.

When Spam Level exceeds:	03 (aggressive)
do this:	Warn
When Spam Level exceeds:	08 (conservative)
do this:	Quarantine

Management Control

Accurate Identification of Spam

Astaro's Spam Protection utilizes nine methods to pierce the disguises used by professional spammers:

- ▶ Sender Address Verification: Messages are tested to determine if they come from legitimate e-mail addresses.
- ▶ Realtime Blackhole Lists (RBLs) and spam databases: E-mail addresses are checked against databases of known spammers.
- ▶ Header Analysis: The header section of e-mails are checked for false or altered information and addresses with invalid characters.

- ▶ Body Analysis (Heuristics): Words and word patterns typical of spam are identified.
- ▶ SPF record checking: Rejects e-mails coming from a false "Mail From" address.
- ▶ URL scanning: URLs within e-mails are checked against a database of known spam URLs.
- ▶ Greylisting: Unknown mail servers are asked to resend messages before they are accepted.
- ▶ BATV Reverse Path Signing: Blocks e-mails from being "bounced back" to an e-mail server unless they really originated there.
- ▶ Whitelist and Blacklist: The administrator can list e-mail sources known to be legitimate and illegitimate.

Management Control

Administrators can tune spam protection to balance stringent blocking against the risk of missing legitimate messages. Options include:

- ▶ Enabling or disabling tests.
- ▶ Taking actions based on "spam score" thresholds.
- ▶ Specifying that suspect messages should be:
 - ▶ Dropped
 - ▶ Rejected and error notification returned to the sender
 - ▶ Passed through the recipient with a warning message
 - ▶ Quarantined for later evaluation and disposition

In addition, a digest of blocked messages can be sent to each user daily.

If the user sees an e-mail that was incorrectly blocked, he or she can click

on a link and receive the e-mail automatically.

Performance and Simplicity

Astaro's Content Filtering Framework™ integrates spam protection with the firewall and virus scanning into a single extensible system. This improves performance and simplifies ongoing management:

- ▶ Performing spam testing, virus scanning and packet filtering on the same system eliminates delays vectoring files to separate systems.
- ▶ Local whitelists, blacklists and network configurations can be entered just once and shared by all of Astaro's security applications.
- ▶ Reports track statistics on e-mail messages processed, their size and spam score, and the number of viruses found.

Working with the E-mail Server

Astaro Spam Protection can add headers to e-mail messages so that a recipient e-mail application can take specific actions, such as sending suspicious e-mail messages to a "spam" folder on an e-mail user's desktop. Information added to e-mail headers can include:

- ▶ A spam flag
- ▶ The "spam score"
- ▶ Expression match (flag that the message contains suspicious text)
- ▶ RBL warning (flag that the message comes from a domain identified in a Realtime Blackhole List)

Phishing Protection

Phishing e-mails mimic legitimate messages from financial institutions, web merchants, and other sources in order to mislead users into sending confidential information to criminals.

While most attacks are designed to capture personnel information, there is increasing potential for phishing methods to be used to capture user IDs, passwords, and other confidential information that could aid hackers in penetrating corporate databases.

Astaro's Phishing Protection application detects and blocks e-mails that attempt to capture confidential information that can be used for identity theft, fraud, and attacks on corporate networks.

Accurate Identification of Phishing

Astaro's Phishing Protection utilizes a variety of methods to identify and block Phishing e-mails:

- ▶ Text in e-mails is compared with known examples of Phishing messages. Messages containing known phishing patterns are blocked before they reach the user's inbox.
- ▶ Phishing e-mails contain links to fraudulent web sites. Users who click on these links will be prevented from reaching the phishing web site if Astaro's Content Filtering application (part of the Web Security Subscription) is set to block links that are

uncategorized or that are categorized as "suspicious".

- ▶ uncategorized or that are categorized as "suspicious".
- ▶ Content downloaded from web sites will be blocked if it matches patterns of phishing content.



About Astaro

Astaro was founded in 2000, with the goal of creating integrated, easy-to-use network security products. The company's leading Unified Threat Management product, Astaro Security Gateway, protects more than 25,000 customers, ranging from small businesses, to government and non-profit agencies, to global enterprises. Astaro's firewall is **ICSA Labs certified**. The company's technology has received recognition and awards such as **Editors' Choice** and **Best Business Security Solution of the Year** from PC Magazine, **Best Security Solution** from LinuxWorld Expo, **10 Stars** and **Test Center Recommended** from CRN Magazine, **Five Stars** from SC Magazine, "**Extremely Cost-Effective**" from The Tolly Group, and "**Excellent**" from InfoWorld Magazine.

Astaro is co-head-quartered in Karlsruhe, Germany and Boston, United States, with offices and solutions partners in over 40 countries.

Learn More

Download the free trial software at www.astaro.com or request a free trial appliance today!
Contact Astaro at:

Europe, Middle East, Africa

Astaro AG
Amalienbadstrasse 36
76227 Karlsruhe
Germany
T: +49 721 255 16 0
F: +49 721 255 16 200
emea@astaro.com

The Americas

Astaro Corporation
3 New England Executive Park
Burlington, MA 01803
USA
T: +1 781 345 5000
F: +1 781 345 5100
americas@astaro.com

Asia Pacific Region

Astaro Corporation
30th Floor Bank of China Tower
1 Garden Road, Central
Hong Kong, China
T: +852 2251 8514
F: +852 2251 8515
apac@astaro.com

Your Astaro Solutions Partner

