Avira Exchange Security

Communicate securely: Central email management with Avira

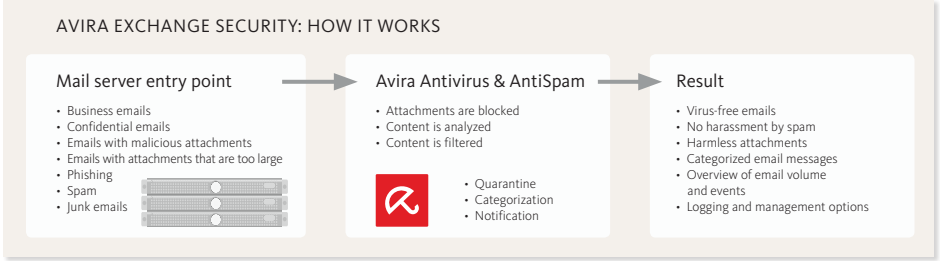
THE ADVANTAGES OF AVIRA EXCHANGE SECURITY

REAL-TIME PROTECTION FROM VIRUSES AND PHISHING ATTACKS

- Protection of the infrastructure from viruses, unsolicited file attachments, and phishing emails
- Checking of suspicious URLs and detection of phishing emails
- Reliable removal and quarantining of viruses and other malicious file attachments
- Recursive virus checking of all emails and file attachments in real time as well as on an event and time controlled basis
- Detection of file attachments using unique tamper-proof file patterns (fingerprints)
- Creation and use of company-specific fingerprints
- Definition of file restrictions through a combination of file name, file extension, and file size
- Application of file restrictions on archives, e.g. ZIP, RAR
- Cloud-based detection technology to block unknown attacks (zero day exploits)

MULTI-LEVEL SPAM BLOCKING AND SMART CONTENT ANALYSIS

- Powerful antispam technology
- Central quarantine management with user-specific access rights
- Blocking of emails from unsolicited senders
- User-specific management of whitelists and blacklists on the server
- Central checking of encrypted emails
- Flexible notification of blocked emails to administrators or sender/receiver
- Checking according to corporate guidelines of banned, undesirable, or confidential content



The majority of business processes only run smoothly if email communication works seamlessly – if the communications process is interrupted, costly delays ensue. If attackers penetrate the network and databases using prepared email attachments, the consequences can be serious enough to endanger the company's existence. If the company forwards infected emails to customers or business partners without noticing, it isn't just embarrassing – it can also be dangerous as it might harm everyone involved.

With Exchange Security companies can rely on a highly efficient protection system that doesn't sap the performance of either their Exchange infrastructure or the running processes. Dangerous attachments are detected and blocked with maximum reliability, and threats from phishers and spammers are blocked quickly.

Avira Exchange Security

SYSTEM REQUIREMENTS

Microsoft Exchange Server

- Microsoft Exchange Server 2007 (64-bit), including latest update rollups
- Microsoft Exchange Server 2010 (64-bit), including service packages up to SP2 and corresponding update rollups
- Microsoft Exchange Server 2013 (64-bit) on Windows Server 2012 (Avira Exchange Security installed on mailbox server)
- Microsoft Exchange Server 2016

Operating Systems

- Windows Server 2008 (including latest service packs and patches)
- Windows Server 2008 R2 (including latest service packs and patches)
- Windows Server 2012 (64 bit)
- Windows Server 2012 R2 (64-bit)

RAM: Exchange recommended + additional 64 MB
HDD: Minimum 400 MB
Extra: CD-ROM drive or network access; Microsoft .NET Framework 3.5 plus 4.0 .NET Framework Client Profile | 100 MB recommended for trace logging | Internet access required

LICENSING

Licensing prices are per protected mailbox
License periods: 1 year, 2 years, or 3 years

SCOPE OF LICENSE

- Free updates and upgrades for the term of the license
- Downloadable software and documentation
- Avira Gold Support

AVIRA TEST RESULTS

Avira products comply with all industry standards and regularly undergo third-party testing.

"Top Rated" (December 2015) and "Advanced+" Award for 100% detection with zero false alarms in the Real-World Protection Test from AV-Comparatives (March 2016).
www.av-comparatives.org

AV-Test (December 2015): "Best Repair" and "Best Usability" award.
AV-Test (February 2016): Highest score possible for detection performance and user friendliness on Windows.
www.av-test.org

AVIRA PROTECTION CLOUD: SMART ONLINE PROTECTION FOR YOUR BUSINESS

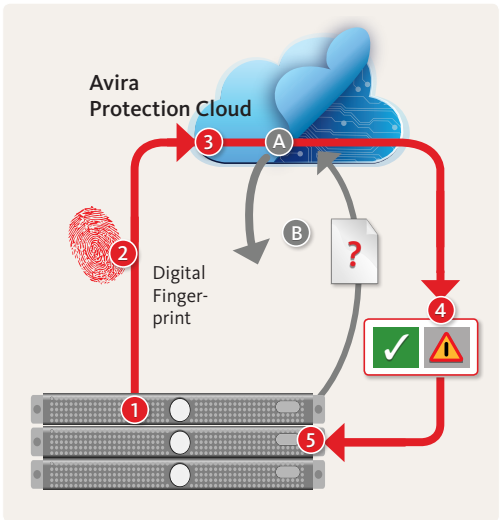
Avira Protection Cloud is the answer you're looking for to the increasingly more complex threats posed by viruses and cybercriminals, detecting threats in real time and successfully blocking them. Using advanced technology comprising the latest generation in file detection modules, convex functions, and artificial intelligence, it uses a global online security platform that is active 24x7, which is based on a network of millions of computers. In a split second, files are checked and reliably classified as either safe or infected.
Alongside significantly enhanced security and the short reaction time, Avira Protection Cloud offers another advantage: It requires hardly any local storage capacity. Avira Protection Cloud is user friendly and always up to date. It also integrates seamlessly into existing systems.

1. Avira Exchange Security detects a suspicious file in an email attachment.
2. The file's digital fingerprint is determined and sent to the Avira Protection Cloud for analysis.
3. This fingerprint is compared with files which were checked previously by Avira Protection Cloud. This can lead to two outcomes:

A. The fingerprint belongs to a file already scanned by the Protection Cloud and is immediately classified as either safe or malware.

B. Alternatively, Avira Protection Cloud doesn't know the fingerprint yet. So Protection Cloud uploads the file, analyzes it, and classifies it either as safe or malware.

4. Avira Protection Cloud then notifies Avira Exchange Security about the status of the fingerprint (safe or infected).
5. If the file is classified as malware, Avira Exchange Security stops the threat.



For information on Avira Protection Cloud, visit:
http://www.avira.com/en/avira-protection-cloud