

F-Secure Messaging Security Gateway: Zero-Hour Anti-Virus Module



As e-mail-borne viruses become increasingly malicious and proliferate more rapidly across the network, enterprises need new forms of protection at the very earliest stages of a new virus attack. The F-Secure® Zero-Hour Anti-Virus™ module, an additional component of the F-Secure Messaging Security Gateway™ protects enterprises against new viruses and other forms of malicious code during the critical first hours after new viruses are released and before anti-virus signatures have been updated—and adds an additional layer of anti-virus protection to your gateway defenses.

Global analysis, local protection

To protect large organizations from emerging virus attacks, F-Secure Zero-Hour Anti-Virus combines global analysis of internet traffic patterns with local containment of suspicious messages and attachments. F-Secure Zero-Hour Anti-Virus constantly analyzes millions of internet messages for anomalies that indicate a potential virus attack. Advanced pattern recognition technology is used to identify new viruses within minutes of their mass distribution over the internet with greater than 95% accuracy. At the customer's site, F-Secure Zero-Hour Anti-Virus analyzes incoming messages for similarities with suspected virus messages. Messages and attachments that exhibit recurrent pattern characteristics of the emerging virus are automatically quarantined at the enterprise gateway where they can be held until the availability of a production-ready virus signature.

Closing the zero hour gap

New virus distribution methods designed to thwart signature-based anti-virus technology—including "short span" attacks, serial variant attacks and attacks launched from botnets—are on the rise. Today's enterprise needs protection that can respond almost instantaneously to emerging threats. F-Secure Zero-Hour Anti-Virus identifies new virus activity and takes preventive action at the earliest stages of a virus outbreak, keeping your messaging systems safe until new antivirus signatures are updated.

Precise detection, minimal disruption

Unlike other virus outbreak solutions, F-Secure Zero-Hour Anti-Virus accurately detects and quarantines only those messages associated with an emerging virus, without stopping legitimate e-mail. Instead of quarantining all e-mail with attachment types deemed to be dangerous, F-Secure's solution temporarily delays only specific messages that are classified as being part of an emerging outbreak.

Rapid deployment

F-Secure Zero-Hour Anti-Virus works right out of the box with pre-configured, default policies designed to address the virus outbreak defence needs of most organizations. F-Secure's easy-to-use graphical interface also gives you fine-grained control over every aspect of your Zero-Hour policies.

Key Features

- > Protection against new viruses and other malware before antivirus signatures have been released
- > Global analysis of internet traffic patterns combined with local containment of suspicious messages and attachments
- > Precise detection of messages associated with an emerging virus without stopping legitimate e-mail
- > Easy to take into use with pre-configured default policies
- > Comprehensive reporting with graphical interface

Zero-Hour Anti-Virus in Action

F-Secure Zero-Hour Anti-Virus works in concert with other F-Secure defences to provide nearly impenetrable defence against viruses, worms and other forms of malicious code. Incoming messages are processed by a variety of defensive systems that allow only legitimate messages into your enterprise. Messages are first scanned for validity and other policy violations. They are then scanned by F-Secure's leading antivirus engines.

Zero-Hour scanning

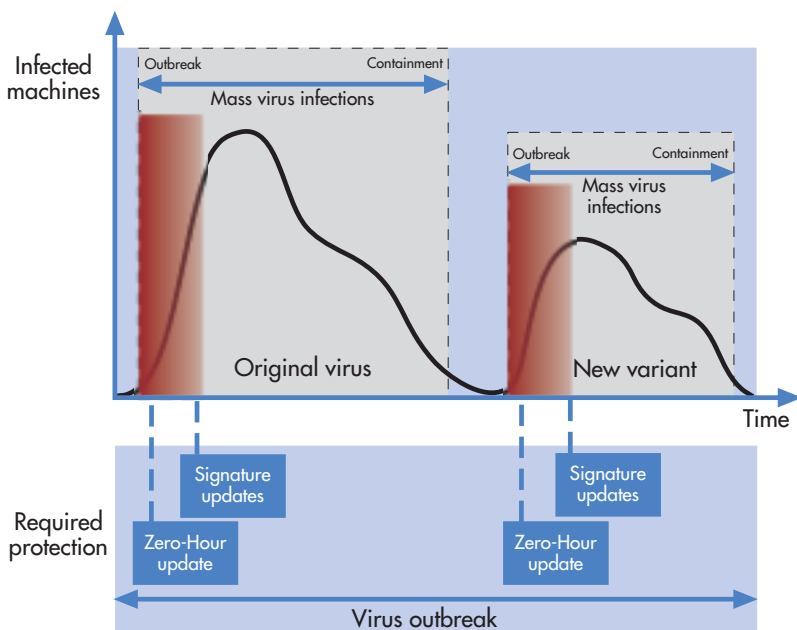
Messages that are declared clean by the antivirus engines are then passed to the Zero-Hour Anti-Virus module to determine if the message is part of a recent outbreak for which signatures are not yet available. If the Zero-Hour Anti-Virus module determines that the message is clean, it is delivered to its intended recipient. If the module determines that the message is part of a new virus outbreak, the message is classified as suspect and handled as specified by the Zero-Hour policies.

Zero-Hour quarantine

Suspect messages are assigned a severity (confirmed virus, high, or medium risk) and different policies may be triggered based on this risk level or other message attributes.

Comprehensive reporting

Like all of F-Secure's modular messaging defences, Zero-Hour Anti-Virus includes integrated reports that provide a complete view into the operation of your zero hour defences and virus activity in general. Built-in, graphical reports provide visibility into the volume of messages being classified by Zero-Hour policies, Zero-Hour virus trends, top Zero-Hour virus types including unverified messages, and verified virus volume trends—allowing you to quickly show ROI for your antivirus initiatives.



Customizable quarantine folders

F-Secure Zero-Hour Anti-Virus module protects against extremely rapidly spreading viruses using advanced pattern recognition technologies. When the F-Secure Zero-Hour Anti-Virus module is installed, quarantine folders can be customized with a "zero hour delay" behaviour that holds messages until a certain condition is met and then resubmits the messages for scanning by F-Secure Anti-Virus engines.

Customizable rules

Rules for the handling of suspicious messages can be customized in a variety of ways. F-Secure Zero-Hour Anti-Virus lets you define any number of policies including:

- > **Suspect message policies:** These policies define how to handle messages that contain suspected viruses. Typically, suspect messages are sent to a Zero-Hour quarantine where they are held for rescanning by future virus signature updates.
- > **Probable virus policies:** These policies define how to handle messages that are still suspected of virus contamination even after being quarantined and rescanned. Typically, these messages are sent to a "probable virus" quarantine where they can be held for some period of time before permanent deletion.

Proofpoint and Proofpoint MLX are trademarks or registered trademarks of Proofpoint Inc. All other trademarks contained herein are the property of their respective owners.

"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. Other product and company names mentioned herein may be trademarks of their respective owners. Copyright © 2006 F-Secure Corporation. All rights reserved.

fszhav061018