

Proofpoint Zero-Hour Anti-Virus

Protection for Emerging Virus Threats

As email-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. Proofpoint Zero-Hour Anti-Virus™, included in the Proofpoint Enterprise Protection™ Suite, protects enterprises against new viruses and other forms of malicious code during the critical first minutes and hours after new viruses are released and before anti-virus signatures have been updated. It also adds an additional layer of anti-virus protection to an organization's gateway defenses.

Proofpoint Enterprise Protection Suite Components

The following comprehensive protection components are offered through the Proofpoint Enterprise Protection Suite:

- **Proofpoint Dynamic Reputation™**
Connection management for powerful spam protection
- **Proofpoint Email Firewall™**
Detects sensitive information in message content and subject line
- **Proofpoint Spam Detection**
Detects and eliminates spam and phishing attacks in any language
- **Proofpoint Zero-Hour Anti-Virus**
Protects enterprises against new viruses and malicious code moments after their release
- **Proofpoint Virus Protection™**
A wide variety of enterprise-class virus solutions

Multi-layered, defense-in-depth virus protection

When combined with Proofpoint Virus Protection, Proofpoint's Zero-Hour Anti-Virus provides an organization with a multi-layered defense-in-depth protection against viruses. Email is scanned for viruses using various technologies (signature-based and non-signature-based) to cover all virus protection bases.

Proofpoint Zero-Hour Anti-Virus

Feature	Benefit
Defense-in-depth	Proofpoint Zero-Hour Anti-Virus provides in-depth defense when combined with signature-based Proofpoint Virus Protection.
Precise detection	Precise detection, as a result of global analysis of traffic patterns, provides local containment and protection of suspicious messages.
Complete protection from malicious attacks	Proofpoint Zero-Hour Anti-Virus provides complete protection from malicious attacks during the initial minutes and hours after viruses are released.
Minimized administrative overhead and reduced overall risk	Proofpoint Zero-Hour Anti-Virus delays, rather than blocks, messages in the quarantine containing potential viruses. They are automatically rescanned using the virus engine, minimizing administrative overhead and reducing overall risk from zero day attacks.
Flexible policies	Flexible policies allow administrators to customize the handling of suspicious messages.

Global analysis, local protection

Proofpoint 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 high accuracy.

At each Proofpoint Enterprise Protection deployment, Proofpoint 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 email gateway where they can be held until the availability of a production-ready virus signature.

Proofpoint Zero-Hour Anti-Virus

Closing the zero-hour gap

Proofpoint Zero-Hour Anti-Virus identifies new virus activity and takes preventive action at the earliest stages of a virus outbreak, keeping messaging systems safe until new anti-virus signatures are updated. The solution provides protection from viruses hours before competing "outbreak filters" react.

Precise detection, minimal disruption

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

Customizable policies

Organizations can easily customize their Zero-Hour Anti-Virus policies using a convenient graphical user interface. Based on these customer-configurable policies, messages that have been identified as part of a virus outbreak can be automatically re-scanned and cleaned, deleted, released or otherwise disposed of based on the availability of updated virus signatures and other conditions.

Comprehensive reporting

Like all Proofpoint email defense solutions, Proofpoint Zero-Hour Anti-Virus includes integrated reports that provide a complete view into the operation of your Zero-Hour defenses 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.

Flexible policy management and message disposition

Proofpoint Zero-Hour Anti-Virus works in conjunction with Proofpoint Virus Protection to provide comprehensive, multi-layered defense against viruses. Together, these technologies provide a proactive virus protection layer (that does not depend on signatures), and a fast and effective signature/heuristics engine to efficiently verify malicious code.

Customizable rules

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

- **Suspect message policies:** These policies define how to handle messages that contain suspected viruses. Unique policies can be defined based on message route (inbound, outbound, etc.), threat classification level (medium or high probability of virus contamination), document type and/or MIME type. All standard message disposition options (e.g. continue, block, quarantine, etc.) are available. Typically, suspect messages are sent to a 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. Policies can be based on all of the previously described conditions. Typically, these messages are sent to a "probable virus" quarantine where they can be held for some period of time before permanent deletion.

Customizable quarantine folders

When Proofpoint Zero-Hour Anti-Virus is activated, quarantine folders can be customized with "Zero-Hour delay" behavior that holds messages until a certain condition is met and then resubmits the messages for scanning by Proofpoint Virus Protection. Folders can be customized in a variety of ways, including a number of anti-virus signature updates to wait for until resubmission and minimum/maximum quarantine time for suspect messages.

About Proofpoint

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.

Proofpoint, Inc.
892 Ross Drive
Sunnyvale, CA
94089

1.877.647.6488