Proofpoint Zero-Hour Anti-Virus Module

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. The Proofpoint Zero-Hour Anti-Virus™ module, a component of the Proofpoint Messaging Security Gateway™ and Proofpoint Protection Server®, 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.

features

Global analysis, local protection

To protect large organizations from emerging virus attacks, Proofpoint Zero-Hour Anti-Virus combines global analysis of internet traffic patterns with local containment of suspicious messages and attachments. 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 greater than 95% accuracy.

At the customer's site, 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 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. Proofpoint 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 anti-virus signatures are updated. Proofpoint's solution provides protection from viruses hours before competing "outbreak filters" react.

Precise detection, minimal disruption

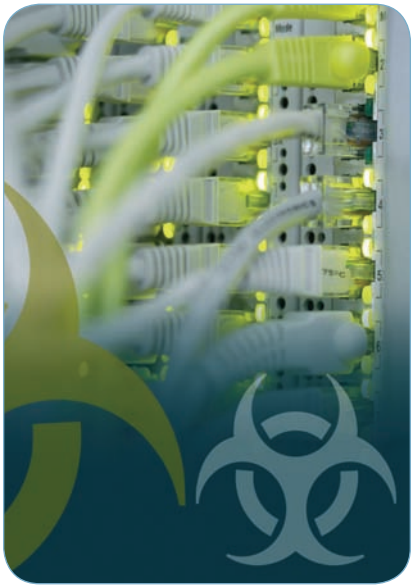
Unlike other virus outbreak solutions, Proofpoint Zero-Hour Anti-Virus accurately detects and quarantines only those messages associated with an emerging virus, without stopping legitimate email. Instead of quarantining all email with attachment types deemed to be dangerous, Proofpoint's solution temporarily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

Customizable policies

Proofpoint customers can easily customize their zero-hour anti-virus policies using the Proofpoint Messaging Security Console™, a convenient graphical user interface to all Proofpoint policy management, system administration and reporting features. Based on these flexible, customer-configurable policies, messages 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 of Proofpoint's modular messaging defenses, 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—allowing you to quickly show ROI for your anti-virus initiatives.



Comprehensive Virus Protection

Proofpoint understands that an effective defense against today's virus threats requires more than just signature-based protection or outbreak filters. Proofpoint provides comprehensive protection from malicious code through a combination of technologies and information services.

Proofpoint Zero-Hour Anti-Virus Module

Provides immediate protection from emerging viruses:

- Early, accurate detection
- Real-time protection
- Fine-grained policy control
- Consolidated, correlated reporting
- Lowest total cost of ownership compared to competing zero day solutions

Proofpoint Virus Protection Module

Provides signature-based protection using leading anti-virus engines from F-Secure or McAfee:

- Continually updated protection against the latest viral threats
- Scan both inbound and outbound "zombie" traffic
- Flexible policy and dispositions

Virus Lifecycle Information

Proofpoint provides up-to-date information on viruses in the wild and the state of virus-related threats affecting your enterprise:

- Alerts and news channels to educate your users
- Centralized reporting for 360 degree view of virus activity affecting your enterprise

Proofpoint Zero-Hour Anti-Virus Module

zero-hour policies and data flow

Flexible policy management and message disposition

Proofpoint Zero-Hour Anti-Virus works in conjunction with the Proofpoint Virus Protection module to provide comprehensive defense against viruses. Together, these modules 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.

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

Customizable rules

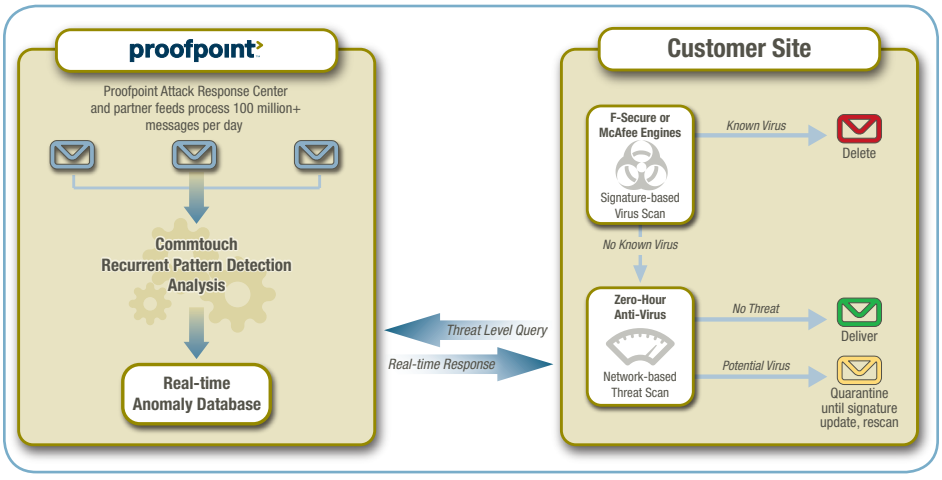
Rules for the handling of suspicious messages can be customized in a variety of ways. Proofpoint Zero-Hour Anti-Virus lets you define any number of policies including:

- **Suspect message policies:** These policies define how to handle messages that contain suspected viruses. 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 of Proofpoint's standard message disposition options (e.g., continue, block, quarantine, etc.) are available. 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. 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 the Proofpoint Zero-Hour Anti-Virus module is installed, quarantine folders can be customized with a "zero hour delay" behavior that holds messages until a certain condition is met and then resubmits the messages for scanning by Proofpoint Virus Protection engines. Folders can be customized in a variety of ways including number of anti-virus signature updates to wait for until resubmission and minimum/maximum quarantine time for suspect messages.

proofpoint zero-hour anti-virus at a glance



Proofpoint Zero-Hour Anti-Virus uses a combination of recurrent pattern detection technology, zero-hour heuristics and message-specific matching to identify new viruses. It works in concert with the signature-based protection offered by Proofpoint Virus Protection to protect against all types of malicious code.

Zero-Hour Anti-Virus in Action

Proofpoint Zero-Hour Anti-Virus works in concert with other Proofpoint defenses to provide nearly impenetrable defense 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 Proofpoint's signature-based anti-virus defenses.

Zero-Hour scanning

Messages that are declared clean by the signature-based anti-virus filters are then passed to the Zero-Hour Anti-Virus module to determine if the message is part of a recent outbreak for which a traditional 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.

Typically, suspect messages will be sent to a Zero-Hour quarantine where they are held for a designated time (e.g., until two anti-virus signature updates are received), then the message is resubmitted to Proofpoint Virus Protection for rescanning.

Learn More about Proofpoint Zero-Hour Anti-Virus

For more information about Proofpoint's advanced protection against emerging virus threats, download our free whitepaper, *Close the Zero-Hour Gap,* by visiting:

http://www.proofpoint.com/zhavwp