Cisco Virus Outbreak Filters

Overview

A proven preventive solution, **Cisco Virus Outbreak Filters™** provide a critical first layer of defense against new outbreaks hours before signatures used by traditional anti-virus solutions are in place. Real world results show an average lead time over reactive anti-virus solutions of 13 hours, along with an extremely high catch rate and near zero misclassifications.

Integrated into Cisco's email security appliances, **outbreak filters** perform a threat assessment of inbound and outbound messages, and quarantine suspicious messages temporarily. Messages are automatically released once signatures from traditional anti-virus vendors are deployed.

By detecting new outbreaks in real time and dynamically responding to prevent suspicious traffic from entering the network, Cisco **Virus Outbreak Filters** ensure customer uptime and business continuity for hundreds of Fortune 500 companies, ISPs, small and medium-sized companies, and universities worldwide.

Features

IronPort Virus Outbreak Filters are a proven high-performance solution that offers unmatched detection, immediate and accurate protection, coupled with easy setup and zero ongoing administration.

Fast, Accurate Detection

Real-time detection powered by SenderBase®—the world's largest email and web traffic monitoring network. Cisco's's SenderBase Network captures data from over 100,000 contributing organizations around the world, and has a view into a remarkable 35 percent of the world's enterprise email traffic, providing unparalleled capabilities in accurately identifying anomalies that are proven predictors of an outbreak.

The 24x7 Cisco Collective Security Intelligence (CSI) provides human oversight to ensure speed and accuracy. Experienced analysts use sophisticated tools to verify anomalies and approve automatically generated outbreak rules. A customer-facing website is also continuously updated with data on current outbreaks.

Automated Protection

Cisco's exclusive Context Adaptive Scanning Engine™ (CASE) scans messages against both "real-time" outbreak rules and "always on" adaptive rules to accurately identify and quarantine viral messages. Suspicious messages are temporarily quarantined.

Cisco's unique dynamic quarantine allows Cisco **Virus Outbreak Filters** to immediately quarantine viral messages based on limited information, without cost. Quarantined messages are continuously re-evaluated against the latest, increasingly fine-grained rules, and released if they do not match.

Comprehensive Management

An integrated web-based user interface makes it easy to setup and configure the solution to meet corporate-specific requirements. Administrators can easily configure policy parameters, select the forms of protection that are enabled, and more. The solution also contains powerful tools that let administrators examine messages, address exceptions, and change status of certain users.

A full suite of alerts and reports, plus a detailed support website, ensure complete visibility into global and local outbreak activity.

Unmatched efficacy plus automated quarantine and release translates into zero ongoing administration. Minimal misclassifications eliminate administrator intervention and customer support overhead. In addition, the dynamic quarantine enables automated release, based on updated signature availability.

Over 100,000 organizations participate in the SenderBase Network, enabling the world's largest email traffic monitoring system.

Benefits

Proven results Cisco Virus Outbreak Filters are the industry's only proven preventive solution for catching new outbreaks. For over a year, **Cisco Virus Outbreak Filters** have been preventing virus outbreaks from infecting top ISPs, Fortune 500 and Global 2000 companies, as well as major universities. The solution has a track record of providing protection up to 48 hours ahead of traditional anti-virus solutions, along with a high catch rate and minimal misclassifications.

Massive cost savings by detecting new outbreaks in real time, and dynamically responding to stop infected messages (hours prior to traditional virus signatures), **IronPort Virus Outbreak Filters** protect companies of all sizes against significant network damage.

Easily measurable ROI: The exact cost of a virus attack can be difficult to determine. If there is data destruction, where backup has been inadequately carried out, the costs can be immense. On average, **Cisco Virus Outbreak Filters** in use at a typical Global 2000 company will block more than 5,000 infected messages per outbreak. Stopping this many infected messages allows the solution to pay for itself in a single outbreak.

Easy Setup, Zero Ongoing Administration Cisco Virus Outbreak Filters are easy to setup and configure to meet corporate-specific requirements. Once installed, the solution is fully automated and requires no ongoing management. Administrators can be "hands-on" or they can leave the system alone and let the automatic Dynamic Quarantine take care of blocking, scanning, and releasing messages—saving valuable bandwidth and system resources. Administrators have complete visibility to outbreak activity.

Summary

Preventive Security

As email viruses evolve to become faster spreading and more destructive, corporations will need to expand anti-virus defenses to include solutions that proactively detect and dynamically respond to new outbreaks.

Today, most corporations implement a layered anti-virus defense using reactive anti-virus solutions at the desktop, mail server and gateway. However, the unavoidable window of time between when an outbreak starts and when updated signatures are deployed emphasizes the importance of including solutions that can prevent new virus outbreaks and dynamically trigger policies to protect networks immediately.

Cisco Virus Outbreak Filters offer protection that overcomes the time-to-response limitations inherent in traditional anti-virus solutions. **Cisco Virus Outbreak Filters** recognize email virus outbreaks faster than traditional anti-virus solutions, allowing corporations to defend against new outbreaks before they escalate into damaging and costly incidents.

Contact us

How to get started with Cisco Email Security

Cisco® sales representatives, channel partners, and support engineers are ready to help you evaluate how Cisco email security products can make your email infrastructure secure, reliable, and easier to manage. If you believe that your organization could benefit from Cisco's industry leading products, please visit us on the Web at http://www.cisco.com/go/emailsecurity

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C78-734826-00 05/15