



WormScout Anti-Worm Solution

→ WormScout delivers an enterprise Anti-Worm solution with an innovative approach to one of the costliest and most lethal threats facing enterprises today: Worm Outbreaks.

Automated worms are fast moving, destructive, and an ever-changing threat to networks of all sizes. Because worms propagate without human involvement, they can spread much faster than conventional attacks. Worms such as Nachi, Slammer, Blaster, and Welchia disrupt business operations and are responsible for billions of dollars in damages. And, experts claim the worst is yet to come. Future worms may cause more damage than has been seen to date, potentially corrupting hard disks and disrupting network devices.

Worms are now appearing soon after vulnerabilities are discovered. This leaves enterprises exposed, facing the potential loss of critical electronic assets before proper safeguards and patches can be deployed.

WormScout identifies these worm-infected computers, contains their activity and suppresses them from infecting other network segments. This ensures high network availability and continuous business operations during worm outbreaks, as well as an effective recovery process.

Benefits

- Business Continuity
- High-level of Network Availability
- Low Operational Cost
- Automatic Worm Containment
- Suppression of Worm Propagation
- Real-time Protection Against "Zero-day" Worms

The screenshot displays the WormScout Enterprise Manager interface. The main window shows a hierarchical network tree with nodes for 'Source Network', 'R&D', 'Administrator', 'Bus Development', 'QA', 'Documentation', 'Finance', 'Personnel', 'Int'l Sales', and 'Marketing'. Each node shows the number of Active, Offensive, and Blocked sources. A table at the bottom lists blocked sources with columns for Source, Reason, Blocked Ports, Expires in, Segment, and Scout. The table shows three blocked sources from the Personnel segment.

Source	Reason	Blocked Ports	Expires in	Segment	Scout
10.0.0.40	Domain logon...	None	7:49	Personnel	10.0.4.104
10.0.0.38	Port title	All	8:20	Personnel	10.0.4.104
10.0.0.36	Port title	All	8:34	Personnel	10.0.4.104

The WormScout Enterprise Manager displays where worm-infected computers are contained, ensuring no further propagation within the enterprise

“When the Blaster worm struck, I was absolutely calm. I knew that ForeScout had automatically protected us.”

John Shields, Senior VP E-Business, Patelco Credit Union

“Zero-day” worm identification

Whether the worm is known, a variant of a known worm, or one that’s never been seen, WormScout identifies it accurately, providing suppression and containment where needed.

Worm slow-down mechanism

WormScout engages in a dialog with a worm to accurately identify and confirm its source. As part of this dialog, WormScout plants a slow-down mechanism into the thread, significantly limiting the capability of the worm to spread malicious content into the contained “cell” and improving network availability. This is in addition to blocking infection attempts from spreading beyond the limits of the contained “cell”.

Automatic escalation

Automatic escalation provides three levels of suppression, depending on the severity of worm activity.

The first level of suppression is limiting infected hosts from communicating over the specific ports the worm is infecting – ensuring the remaining ports are available for business operations. The next suppression level is to block the infected hosts from any communications – quarantining them until they are disinfected. The highest level of suppression is to disable the specific ports the worm is infecting across the entire network – ensuring the worm is unable to spread further.

Advanced TCP session reset

WormScout’s TCP reset blocking is activated during the initiation of the TCP session, providing efficient and robust blocking capabilities. In addition to using its own blocking technique, WormScout can dynamically activate any industry standard firewall, to implement additional traffic blocking mechanisms of specific IP addresses.

Alerting & Reporting

WormScout provides flexible, intuitive alerting and reporting options to ensure security managers get the information they need, when they need it.

Graphical network maps

WormScout provides a graphical network map with icons that indicate the location of worm-infected computers. This map can also be displayed for any specific point in time or time range using historical data.

Infected source identification

Pinpoint identification is provided regarding the source of the infection, allowing the administrator to act on the infection and reduce the recovery time.

End user notification

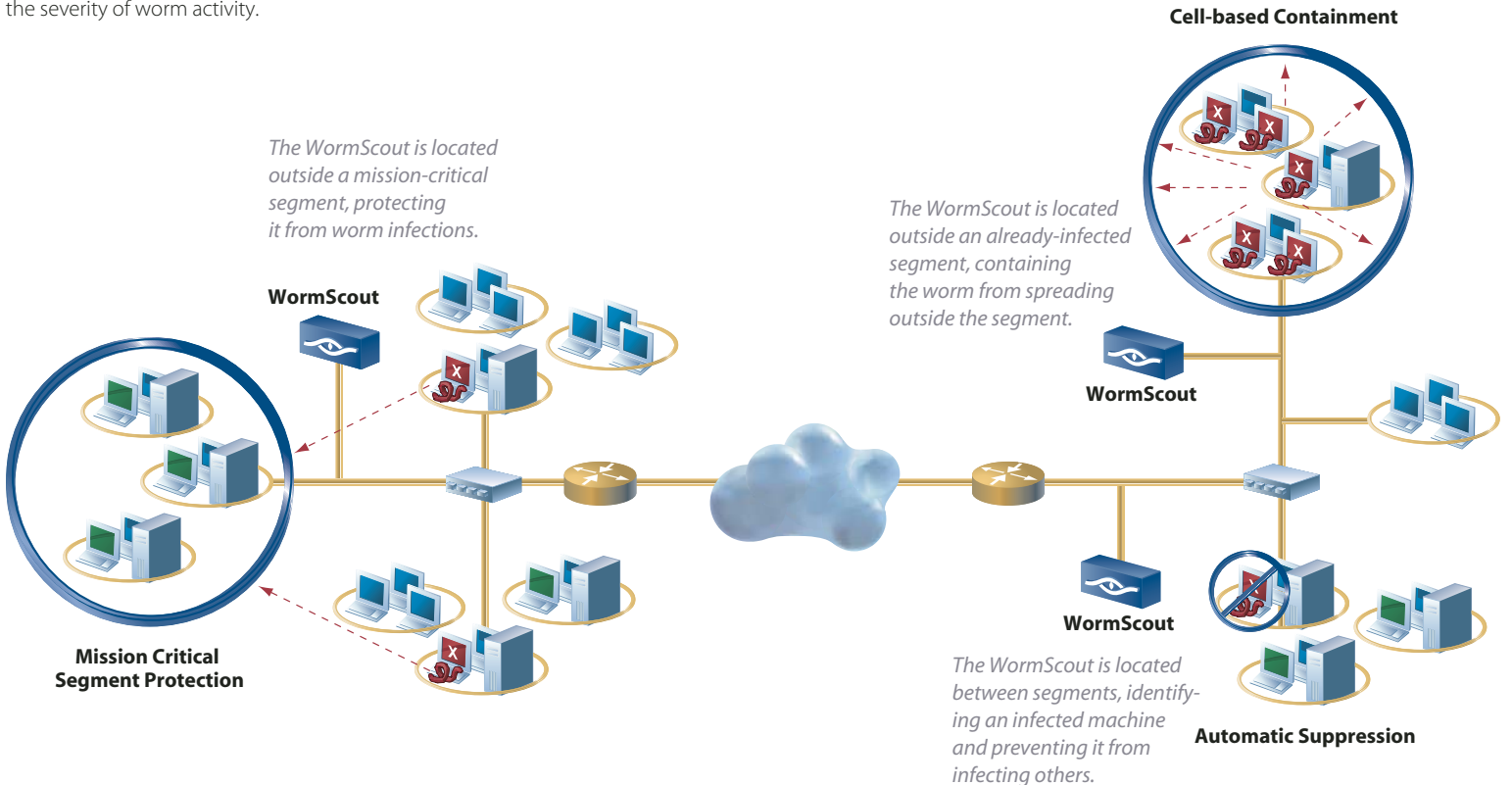
The user of an infected machine can be notified of events that may limit his access to resources on the network, and can be provided instructions on how to proceed or who to contact.

Complete event documentation & reporting

WormScout records all worm-related activity, enabling security managers to thoroughly investigate these incidents. Comprehensive reports are easily generated, presenting up-to-date detailed historical information regarding worm activity and the preventive steps that were taken against them.

Real-time alerts

WormScout can send alerts in real-time via email, SNMP traps, syslog, OPSEC™, or SESA™.



“WormScout immediately addresses known or unknown attacks without constant monitoring, so staff can focus on business operations with confidence that worms will not catch them off guard.”

Robert Henderson, *Manager of Network Engineering Services, University of the Pacific*

Worm Entry Points

Even if your organization has locked down all network perimeters to a minimum and filtered any unnecessary traffic, worms are still a threat to your business. This is because worms penetrate networks through other entry points. Users and business partners can unknowingly infect your network through VPNs and mobile connectivity.

VPNs

Worms can enter networks through infected home and remote computers, which are connected to the network through an encrypted or “trusted” channel. At the same time, these infected computers are also connected to an outside, “non-trusted” network, thus bypassing any perimeter firewall protection.

Mobile Users

Users returning to the network after roaming in other, “non-trusted” networks can bring the worms into the heart of the network, bypassing any security measures in place.

WormScout Components

WormScout provides bi-directional capabilities, which can protect a single network segment from worms infecting it from outside that segment, or protect multiple network segments from each other. WormScout is also able to contain a worm within an already infected segment, preventing it from spreading to other segments.

The WormScout solution consists of Scouts, the Management Server, and the WormScout Enterprise Manager. The Scouts are distributed to protect multiple segments throughout the network, the Management Server is an aggregation device that communicates with multiple Scouts, and the WormScout Enterprise Manager provides centralized management capabilities for any number of Scout servers.

WormScout

WormScout monitors traffic entering and exiting the protected network segment. Once a worm has been accurately identified, WormScout can automatically suppress its propagation. Multiple WormScouts can be distributed across an enterprise and can share worm threat alerts, creating an effective, uniform layer of security at all protected network segments.

Management Server

The Management Server is an aggregation device that communicates with multiple WormScouts distributed across the enterprise. It manages their activity and policy and collects worm activity information. The Management Server also serves as an alert hub, distributing alerts between multiple WormScouts, enabling enterprise-wide suppression of worms.

WormScout Enterprise Manager

WormScout is managed by a Java-based application that provides extensive management capabilities, from policy configurations to comprehensive reports that track worm attempts, identification, and containment action. The WormScout Enterprise Manager also provides a visual overview of WormScout's protection activity—including a graphic network map displaying the location of worm-infected computers, their IP addresses, their propagation attempts, and the preventive steps taken to suppress them.

WormScout Features

Suppression & Containment

WormScout provides real-time protection of network segments against worms. Its automated and instantaneous suppression and containment features limit the replication capabilities of worms and allow additional time for patching of infected systems, making the recovery process fast and simple.

Customized suppression

The suppression mechanisms of WormScout can be selectively activated depending on corporate security policies. Suppression can be activated for specific worm infection categories with configurable action duration and alert options. This method is effective whether suppressing single or multiple infected machines, providing continued network availability during worm outbreaks and ensuring the time needed to deploy necessary patches.

Cell-based containment

WormScout protects the network from worm infections by creating a protected “cell”. Installing multiple WormScouts divides the network into a number of protected “cells” and ensures that worms are contained within their “cells”, isolating them from other network resources. WormScout also provides bi-directional protection, containing worms on both sides of the network connectivity point where they are located.

Management

WormScout Enterprise Manager provides all the management and administrative capabilities necessary to ensure suppression and containment of worm-infected computers.

Enterprise lockdown

Enterprise Lockdown enables the instantaneous sharing of alerts among all WormScouts. When a worm is identi-

fied, Enterprise Lockdown immediately shares the alert with all or some of the WormScouts in the enterprise, ensuring a consistent and superior level of network protection.

Aggregated threat information

Worm outbreak information from all of the enterprise's dispersed WormScouts is consolidated into a single view on the WormScout Enterprise Manager. Detailed information such as the worm-infected computers' IP

addresses, worm propagation activities, and the exact time and date of infection attempts is readily available.

Centralized administration

WormScout Enterprise Manager can manage multiple WormScouts from a centralized location, allowing the administrator to perform configuration changes and apply policies across multiple WormScouts from a single console.

System Requirements (minimum)*

WormScout

Dedicated Intel machine Pentium III-600 or higher
OS – ForeScout hardened Linux OS (shipped with WormScout) or Nokia's IPSO
Memory – 256 MB RAM
Disk Space – 10 GB
NICs – 1 (10Mbps, 100Mbps, or 1Gbps Ethernet interfaces)
Network Connection – must allow full visibility to all incoming and outgoing traffic

WormScout Management Server

Dedicated Intel machine Pentium III-600 or higher
OS – ForeScout hardened Linux OS (shipped with WormScout) or Nokia's IPSO
Memory – 256 MB RAM
Disk Space – 10 GB
NICs – 1

WormScout Console/Enterprise Manager

OS – Microsoft Windows 98/NT/2000, Linux or Sun Solaris
Memory – 128 MB RAM
Disk Space – 100 MB

*Check with your ForeScout representative to determine the hardware requirements for your specific environment.



ForeScout Technologies, Inc.
2755 Campus Drive, Suite 115
San Mateo, CA 94403
USA

T 650.358.5580
F 650.358.5581

About ForeScout Technologies

ForeScout Technologies' enterprise network security solutions focus on providing real-time, automated protection against fast-spreading worms and malicious hacker attacks. ForeScout offers two families of patented products, which ensure network availability and business continuity: WormScout, which suppresses and contains worms at key points inside the network and ActiveScout, which dynamically blocks hackers at the perimeter. **For more information, please visit us at www.forescout.com.**

© 2004 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, the ForeScout logo, and WormScout are trademarks of ForeScout Technologies, Inc. All other trademarks are the property of their respective owners.
WSDS0104