

McAfee Security Forensics

Product Overview

The success of your company depends increasingly upon your network and the data it transports. You need to protect that data and ensure it is not misused. And today's networks run faster than ever to support new and more valuable corporate applications, which means you need to protect larger volumes of business-critical traffic.

Traditional security products provide control for a variety of security issues, but they lack the integration to work together and deliver complete network coverage—they only provide “islands of security.” For example, firewalls may not block all malicious traffic. Intrusion detection systems may not contain the latest, frequently required updates to keep abreast of new signature patterns. Some products only sample network traffic looking for patterns, rather than examining every individual byte. Or, if a product performs a deeper data analysis, it may save only the statistical information and not the actual packets.

It is virtually impossible to predict the many ways in which network-based resources can degrade or become compromised. Important security events and network threats must be thoroughly investigated to ensure they do not reoccur. To give you these critical insights, you need McAfee® Security Forensics to deliver high-performance, high-capacity, packet-level data storage that includes an intelligent retrieval mechanism to analyze network-based event data.

Key Features and Benefits

Continuous Capture and Archive

- Captures all the data for a complete packet-level traffic history
- Provides an electronic archive for analysis and investigation
- Supports full-duplex, Gigabit line-rate capture

Three Terabytes of Storage

- Large storage capacity gives you enhanced visibility and network protection. You can access historical data to investigate intermittent anomalies, as well as extended threat activity.

Reconstruction and Replay

- Easy information access to the details behind suspicious events to help you protect network integrity
- Document unacceptable network use such as unauthorized services or facilities access, downloading of offensive material, copyright violations, or data corruption and destruction
- Quickly identify:
 - Who is responsible for a particular network event
 - What a specific user or group sent, said, or saw
 - Where content originated and where it went
 - How data was transferred via the network

Secure, Reliable System

A robust, hardened system providing secure communications between capture engine and console, which ensures that the equipment you install to secure your network doesn't become a security problem itself.

Unsurpassed Functionality

The McAfee Security Forensics solution provides full-time, continuous traffic capture and archival of your Gigabit network traffic. Now you can continuously monitor and save all or a selected part of your network's traffic for active investigation and offline forensic analysis. With an entire day or week of traffic data, you can recreate any user's network transactions for post-mortem inspection. The data capacity you can achieve varies, based on your unique traffic patterns and the way you choose to filter the data. McAfee Security Forensics software allows you to capture and monitor network traffic for all types of infractions simultaneously. Whether you capture all network traffic data or just a specific IP address, you'll have the evidence you need to validate activity such as:

- Computer hacking
- Intellectual property theft
- Software piracy
- Credit card fraud

Gigabit Data Archival

The McAfee Security Forensics solution incorporates a stream-to-disk technology that efficiently captures, indexes, and stores all data packets on the instrumented network, offering you thorough and tangible investigative evidence of network infractions. It provides a complete, packet-level history and retrieval mechanism for all network activity spanning large time periods.

McAfee Security Forensics software captures both incoming and outgoing network traffic data to deliver complete, accurate reconstruction and replay. This two-way data capture is especially important in complex network architectures that often employ techniques such as asymmetric routing or load balancing to improve network performance and integrity. McAfee Security Forensics software also supports full-line rate, full-duplex data capture, so you can record entire conversations.

Reconstruction and Replay

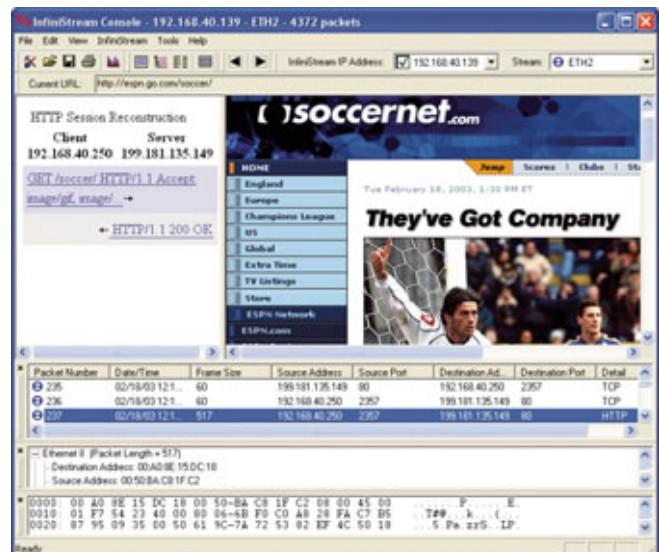
Reconstruction and replay allows you to browse the following types of user sessions:

- HTTP Web pages
- POP3, SMTP, and IMAP4 mail transactions
- Internet Relay Chat (IRC) messaging
- File Transfer Protocol (FTP) downloads
- Voice over IP (VoIP) conversations

Reconstruction and replay converts the data into a flow of application-layer transactions that you can easily step through—just as the user experienced.

High-Volume Storage

Gigabit networks by their very nature have the potential to generate large quantities of traffic. That's why large storage capacity is important. For example, if your Gigabit network typically operates at 10 percent utilization, the three terabytes of storage in the McAfee Security Forensics system can archive over five days of traffic data before recycling the stored data. If you use capture filtering to concentrate on a specific part of the Gigabit data stream, the archive capacity is even greater. This increased storage capacity lets you examine user activity patterns that may span numerous days. Now you can view and access data that would normally be unrecoverable. An extended forensic data window also lets you revisit and examine behavior that occurred without your previous knowledge.



Reconstruction and replay gives you an application-layer view of network activity—just as the user experienced.

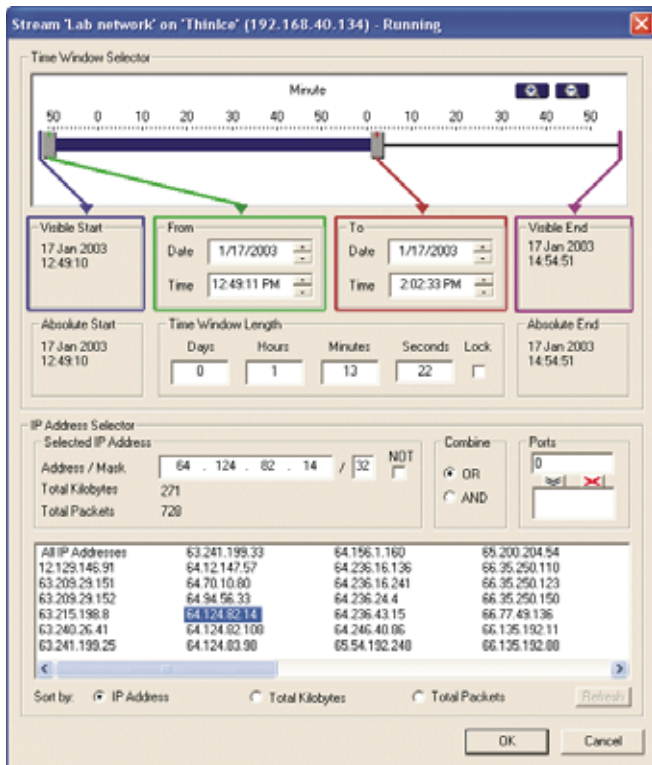
Actionable, Easy-to-Access Data

Collecting large quantities of data doesn't provide much use if you can't access it easily. You need actionable information—not a myriad of bits and bytes. The McAfee Security Forensics data capture, mining, and replay capabilities provides an easy-to-use system that gives you the information quickly—not just the data. Its specially designed file and indexing system reduces the amount of data that must be retrieved and analyzed. This intelligent mining process saves you time by quickly creating a Windows® display that contains a visual representation of the data flow. It allows you to replay the actual content graphically, so you can see the user's actions; for example, view visited Web pages, read sent e-mails, or examine FTP files.

Large enterprise networks may employ multiple Gigabit connections that can benefit substantially from the McAfee Security Forensics data capture and archiving functionality. The Security Forensics console serves as the central access site to all McAfee Security Forensics appliances in your organization. From the console, you can centrally authenticate and manage connectivity to the capture engines. The console also allows you to monitor status, set filters, and view analysis data.

Once the data is saved, post-capture filters by IP address or time frame provide an easy way to find specific information. The analysis results are displayed in a flexible three-pane window of Summary, Detail, and Hex. Multiple simultaneous users can access the Security Forensics appliance, so the data is always

available whenever it is needed. For example, one analyst group can examine yesterday's e-mail traffic for suspected intellectual property theft while a different group investigates a just-reported network intrusion.



You can selectively analyze archived data by time frame and IP address to focus on specific events.

Robust, Secure, and Reliable

Your main goal is securing your network. You demand a security forensics system that is just as secure and reliable. McAfee Security Forensics appliances are built on a proprietary-hardened, Linux-based operating system. They use secure protocols for all communications between the capture engine and consoles. The capture engine chassis delivers high-speed performance and reliability with features such as triple-redundant power supplies and multiple RAID hard drives that can be configured to support hot-swapping to eliminate data loss and downtime.

World-Class Training, Consulting, and Support

McAfee Security University is a Network Associates® Educational Services institution that delivers cutting-edge anti-virus and security management training. The McAfee Security University curriculum helps students understand effective strategies to battle today's evolving threats. Through hands-on training with McAfee Security anti-virus and security management products,

combined with expert instruction, students gain the real-world skills required to combat and minimize the impact of computer viruses and blended threats.

Network Associates Expert Services can assist you during all network growth stages—from planning, design, and implementation—through ongoing management. Our consultants provide expert resources and an independent perspective to meet your specific needs.

Network Associates PrimeSupport® Services offer essential product knowledge and rapid, reliable technical solutions. Over 80 percent of our technical staff hold industry certifications and/or technical degrees and possess over five years of experience in the IT industry. You can engage this high level of expertise through our extensive support portfolio, which consists of PrimeSupport KnowledgeCenter Service Portal, Connect, Priority, and Enterprise. PrimeSupport is your key to maximizing processing uptime, revenue generation, and customer satisfaction.

Appliance Specifications

Platform

- Custom 4U chassis
- Ball-bearing, rack mount slide rails included
- Weight: 110lbs.

Dimensions

- Width: 17 inches (43.2 centimeters)—19 inches (48.3 centimeters) with rack mount brackets
- Depth: 27.25 inches (69.2 centimeters)
- Height: 7 inches (17.8 centimeters)

Storage

- 2.1 terabytes when configured for RAID 5
- 2.9 terabytes when configured for RAID 0
- Continuous capture

Interfaces/Topologies

- Dual Gigabit Ethernet SX

Capture Performance

- 1,200Mb/s sustained capture
- Five second, full-line rate burst tolerance
- IP address and port filters

Data Mining

- Five simultaneous mining sessions during capture
- Time and IP address mining filters

Application Replay**Protocol Support**

- HTTP
- POP3, IMAP4, SMTP
- IRC
- FTP
- VoIP

File Format Support

- .cap (export/import)
- .caz (export/import)
- .dmp (import)

Operating Input Voltage Range

- AC: 100 to 240V 60–50Hz AC (auto-sensing power supply)

Power Consumption

- 460 Watts (max), 400 Watts typical
- Redundant power

Environmental Specifications

- Operating Temperature: + 5°C to + 35°C
- Storage Temperature: - 25°C to + 60°C
- Storage Humidity: 10–90 percent (noncondensing)
- Operating Humidity: 20–80 percent (noncondensing)
- Storage Altitude: 0m to 3,000m
- Operating Altitude: 0m to 3,000m

McAfee Console Platform Specifications**Minimum Requirements**

- Intel Pentium III-class 700MHz processor
- 256MB RAM
- 500MB free hard drive space (for installing software)
- Microsoft® Windows XP Professional, Windows 2000 (Professional or Advanced Server), Windows NT Workstation 4.0 or NT Server 4.0 with Service Pack 3, or Windows 98
- VGA color monitor with 1024x768 resolution or higher
- Mouse (or similar pointing device)
- Network adapter card configured with an IP address and a network connection
- Microsoft Internet Explorer v5.0 or later, with all Service Packs and other updates

Recommended for Optimized Performance

- 512MB to 1GB RAM
- Gigabit network connection
- Intel Pentium IV 2GHz processor

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 888.VIRUSNO (888.847.8766), www.mcafeesecurity.com

Network Associates® products denote years of experience and commitment to customer satisfaction. The PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects—all with service levels to meet the needs of every customer organization. McAfee® Research, a world leader in information systems and security, continues to spearhead innovation in the development and refinement of all our technologies.

Network Associates, McAfee, and PrimeSupport are either registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other trademarks used herein are the property of their respective owners. ©2004 Networks Associates Technology, Inc. All Rights Reserved. 1-nps-msf-001-0404