

Network Forensics: A Giant Step Toward Real-Time Threat Recovery and Resolution

The InfiniStream Solution's Total Packet Capture, Data Mining, and Visualization Provide a New Level of Insight



Table of Contents

I. Networks Forensics: A Prerequisite for Secure Networks	2
Existing Solutions Provide Only a Partial Picture	2
True Network Security Requires Forensic Capability	3
The Network Associates InfiniStream Security Forensics Solution: Moving Toward Real-Time Threat Recovery and Resolution	3
II. Introduction to the Network Associates InfiniStream Solution	4
A Functional Overview of the InfiniStream Solution	4
Fostering Collaboration Between Network Managers and Security Analysts	5
Adding to the Family of Network Associates Network Defense Solutions	6
Product Highlights: Competitive Comparison	6
III. The InfiniStream Solution in Action: Real-world Applications	6
IV. Summary	7
About Network Associates	8

I. Networks Forensics: A Prerequisite for Secure Networks

In January 2003, the SQLSlammer worm spread around the globe in less than ten minutes, shutting down vital business networks for days and costing untold billions in lost revenues and clean-up costs. Days later, many organizations had still not recovered, suffering everything from inaccessible customer databases to out-of-order automatic teller machines.

Just how severe is the damage that businesses sustain from security attacks? According to the 2002 CSI/FBI Computer Crime and Security Survey:

- Ninety percent of respondents detected security breaches within the last twelve months
- Eighty percent acknowledged financial losses due to security breaches
- Forty-four percent were willing and/or able to quantify their financial losses. These 223 respondents reported losses of \$455,848,000
- The most serious losses occurred through theft of proprietary information and financial fraud

These statistics, and SQLSlammer's incapacitating damage, painfully illustrate how today's networks are undisputedly neither safe nor completely secure. They are under siege, under attack by this blockbuster threat as well as tens of thousands of other worms, viruses, and blended security threats before it. Unfortunately, the prognosis is grim: worms like SQLSlammer exploit software vulnerabilities, the number of which found in 2002 jumped 82 percent over the previous year, while the number of severe software flaws found increased by 85 percent.¹

But security threats that jeopardize network performance and mission-critical operations don't always originate outside the perimeter. Increasingly, their genesis is inside the firewall, as well—up to 80 percent, by some estimates.² Both internal and external threats are being perpetrated on a 24/7 basis, challenging the livelihoods of enterprises that also work around the clock, around the world.

Existing Solutions Provide Only a Partial Picture

Managing and assuring the availability and security of the network is a complex challenge, historically requiring enterprises to employ a patchwork of non-integrated security products that provide incomplete coverage. These problems include:

- **Many individual point products:** Over the past decade, security analysts and network managers have come to rely on a multitude of specialized solutions that address specific points on the network where security can be compromised. These include intrusion detection systems (IDSs) and firewalls at the perimeter, server log files and vulnerability scanners that inspect servers and desktops—all useful products that unfortunately do not present a holistic picture of network activity. Their actions—and interactions with other security products—must be continuously interpreted by security analysts and network managers, causing confusion and management inefficiencies.
- **Limited interoperability between products:** Few standards exist to allow these products to share information, again increasing the burden of human interpretation. This dissonance is compounded by security flaws in SNMP, the traditional network management messaging and communications protocol.
- **"Line speed" analysis only for lower line rates:** Most products that reside directly on the network do not have the capacity to analyze data traveling at high speeds, such as on a Gigabit Ethernet network. As a result, complete packet capture and inspection is impossible; network managers must extrapolate action plans from a limited set of data points.

¹ "Report: Net attacks on businesses down," Robert Lemos, CNET News.com, February 3, 2003.

² Merrill Lynch, "Security Software," January 21, 2003.

- **Sampling limitations:** Products that do sample packets traveling over the network can only capture an extremely limited quantity. This creates a frustrating guessing game for network managers who must interpret these ambiguous “snapshots,” leading to false negatives and positives that can jeopardize mission-critical network operations.

In sum, these products are fundamentally limited in their investigative ability, since they can only capture network events after the fact. They cannot answer an even more important question: “What happened before the network event?”

A class of network events will always exist that cannot be predicted but must be thoroughly investigated in order to prevent their recurrence. Network and security managers both share a common challenge of definitively identifying the root cause, precise methods, or even the existence of such high-impact, network-related events—particularly on high-speed and high packet-volume networks. It is these managers’ charter to clearly understand high-impact network events in order to prevent their recurrence.

True Network Security Requires Forensic Capability

Network forensics analysis is an investigative discipline that combines elements of network management and network security to help organizations maintain maximum uptime of networks that are absolutely mission-critical. In theory, it uses reconstructive traffic analysis to investigate and definitively understand network events, enabling their speedy resolution, and perhaps even more importantly, preventing their recurrence. However, until now, only limited tools have been available that allow the full investigative potential of network forensics analysis to be realized.

The situation is changing with new network forensics solutions that not only allow security analysts and network managers to reconstruct what happened during and after a network event—they also answer the question “What happened before the network event?” Today’s new solutions fulfill the mission of network forensics with three key components. The first layer in the stack is *total data capture at the packet level*, providing irrefutable evidence of the behavior of any network component or user. Raw packet capture entails:

- Full line rate capture and storage—no “sampling” of the packets
- No dropping of packets, which typically occurs during burst intervals
- Capture from both transmission sources of a full duplex path
- Capture for a sufficient window of time, up to several days

The second layer of the network forensics stack is *analysis tools*, to help users quickly sift through volumes of data in order to find the exact information they need. These tools offer intelligent data mining to allow non-experts to quickly locate and extract the information they need.

The final layer of the stack is *visual presentation of information* to the user, to allow fast, accurate interpretation of the selected data. Visual presentation reduces errors and makes network forensics activities accessible to a wider range of users.

Together, these three capabilities ensure that security violations and attempted violations can be fully investigated and handled.

The Network Associates InfiniStream Security Forensics Solution: Moving Toward Real-Time Threat Recovery and Resolution

The Network Associates® InfiniStream™ Security Forensics product is a network forensics tool that offers, for the first time, complete historical archival, retrieval, and analysis of raw packet streams. In turn, these capabilities enable network and security analysts to research and understand if, when, and how any network event occurred. In environments where network-attached resources carry high financial and/or public relations value, the InfiniStream solution lets network and security administrators achieve near real-time, historical certainty that the network is performing in an efficient and secure fashion.



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

The InfiniStream solution is a breakthrough product for two reasons: first, because it picks up where intrusion detection systems and firewalls leave off, enabling network managers and security analysts to see what happened before, during, and after a specific network event. Second, because it moves practitioners further along the “network security continuum,” the InfiniStream solution elevates network and security managers from merely carrying out advance proactive preparation and delayed reactive response, bridging these approaches to near real-time investigation and resolution.

Network Associates believes that in an ideal world, network and security management tools would automatically, proactively predict and detect all network-related events, and prevent them from ever impacting business operations. The InfiniStream product presents a giant step toward this ideal; it's a prerequisite for a network protection strategy that allows enterprises to, for the first time, determine how they need to refine defenses in anticipation of future threats. In effect, the InfiniStream solution is a “safety net”, “black box recorder” for existing security technology.

II. Introduction to the Network Associates InfiniStream Solution

The InfiniStream solution effectively addresses the challenge of real-time recovery in attacked enterprise networks with sustained packet capture and stream-to-disk operation, in even heavily loaded Gigabit Ethernet networks. As a result, data from the InfiniStream solution offers a thorough and tangible form of investigative evidence: a complete packet-level history and retrieval mechanism for all network activity spanning large periods of time.

A Functional Overview of the InfiniStream Solution

The InfiniStream solution comprises three components that provide total data capture at the packet level, comprehensive analysis, and visual presentation of information.

- **The capture engine** is a self-contained network appliance, purpose-built for the InfiniStream application. It features a hardened operating system derived from Linux, with a proprietary file system. The appliance provides exceptionally high levels of security and performance, and it is the first product of its kind to offer complete packet capture for high-speed Gigabit Ethernet networks. The device's extensive 2.9 terabytes of storage is up to three times larger than similar solutions³, enabling up to several days' data to be stored³—on a 5 percent utilized Gigabit Ethernet network, the InfiniStream solution can capture over 2.5 days' total traffic. This allows security analysts to quickly seize the opportunity to diagnose and resolve a network anomaly the first time it occurs—instead of waiting and hoping, for a second occurrence—and also allows post facto analysis. For example, the data capture engine's capacity allows a security analyst to investigate on Monday morning, an event that occurred on Friday night, alleviating the need for 24/7 network monitoring.

Uniquely, the InfiniStream solution can capture packets at or near the network core. This is increasingly important because more and more attacks are being launched from within. According to a recent Merrill Lynch report, “Enterprises have largely succeeded in securing the perimeter of corporate networks against external attacks. However, according to security data, 80 percent of technology is deployed to keep bad actors out while 80 percent

³ Duration of storage period will vary with trafficload and capture filters used.

of attacks occur from within. The problem is compounded as rogue employees, clients, trading partners, temporary employees, and others with network access seek to do harm.”⁴

- **The InfiniStream data mining console** is a client software application that resides on a PC workstation. The easy-to-use console software securely accesses the capture engine to quickly parse the high volumes of collected data, using embedded filters and intelligence to find the proverbial “needle in a haystack.” Data mining is performed on the InfiniStream data store of network, transport, and application information. The user can specify the timeframe of activity and the endpoints in the network session to find and retrieve the appropriate data.
- **Packet reconstruction and replay** is the final component, and is presented on the same PC workstation used for data mining. Extremely easy to use, the InfiniStream console’s visual user interface is an extension of the interface familiar to thousands of Sniffer® Technologies software users. While Sniffer Technologies software shows the user specific packets, decodes the protocol layers, and provides an Expert analysis view of the packet, the InfiniStream solution takes the replay concept one step further. It collects and displays an entire “conversation” between a client and server, and it can reconstruct the entire session.

By working on a session level between a user and an end point, the InfiniStream solution can reconstruct detailed network events—such as a database that was compromised, the opening of a suspicious attachment that turned out to carry a virus, a conversation between a client and a server that resulted in missing log files on the server, and limitless other possibilities.

While other products are available that deliver portions of what the InfiniStream solution offers, only Network Associates delivers robust functionality for all three functions—total data capture at the packet level of all network data from layers one to seven, comprehensive analysis, and visual presentation of information—integrated into one product.

Fostering Collaboration Between Network Managers and Security Analysts

With the InfiniStream solution, network managers and security analysts can better collaborate to quickly manage security threats or policy breaches and get networks back up and running. Security analysts can immediately turn to indisputable, tangible evidence reconstructed from raw packets to confirm and document suspected network-based exploits or policy violations. Likewise, network managers can use the InfiniStream solution to isolate any network reliability issue the first time it occurs, rather than suffering multiple iterations of the problem before its cause can be understood.

With the InfiniStream solution’s comprehensive packet data store and sophisticated retrieval and analysis tools, network managers and security analysts no longer need to operate in a vacuum, implementing technology based only on known or predictable events. With the InfiniStream solution they can now immediately perform rigorous analysis of any existing or potential high impact incident that takes place across the networks they manage.

For security analysts, additional InfiniStream solution benefits include:

- A vast improvement in high packet-volume environments where severe limitations exist—such as dropped packets and failed detection—in existing network forensics tools
- A conclusive investigative tool to help in comprehensive security incident response
- A means to better understand and document when and why incidents slip through your security defenses and how you can prevent their recurrence
- A playback capability of Internet protocol-based application activities just as they were experienced by the application user

Network managers can become more productive with the InfiniStream solution for high-speed networks because it can:

- Reduce greatly the pressure on network support personnel to perform the predictive configuration of an analyzer, often required in high-speed Ethernet networks

⁴ Merrill Lynch, “Security Software,” January 21, 2003.

- Expedite the isolation of the root cause of network-based events because analysts can immediately investigate the first instance of the event. They need not wait for the event's recurrence with the properly filtered traditional analyzer

Adding to the Family of Network Associates Network Defense Solutions

The InfiniStream solution is the newest offering from Network Associates, which for more than fifteen years has provided packet-level analysis tools with its Sniffer Technologies family of products. The InfiniStream solution extends this legacy with new security capabilities to create network defense solutions for our customers.

Network Associates also recognizes that the distributed management system model holds the greatest potential for managing complex, widespread enterprise networks. Sniffer Technologies supports this model through its Sniffer Enterprise Management Architecture, a scalable, distributed management system that helps assure the security, availability, and performance of the network. It encompasses a suite of integrated enterprise application and performance management products.

III. The InfiniStream Solution in Action: Real-world Applications

Invaluable to companies that are highly dependent on their networks to do business—such as financial services organizations, airlines, government institutions, and others—the InfiniStream solution provides an unprecedented level of network forensics capability, helping to maintain the utmost security and performance of high-speed networks. Organizations with large networks connected to thousands of nodes can deploy multiple InfiniStream appliances around the network. Common installation points include:

- **Behind the firewall**, to detect potential security breaches, or inappropriate use of internal network resources
- **In the Service Network** and/or DMZ, including extranets
- **Departmentally**, typically on network trunks that connect the core network to sensitive departmental environments such as human resources, engineering, or finance

Once deployed, the InfiniStream solution is ideal for detecting and quickly resolving a wide range of issues that threaten the viability of network operations, including

- **Malicious code attacks:** Many malicious code attacks—especially viruses—often arrive innocuously in an e-mail attachment. With InfiniStream Security Forensics, network managers who are apprised of an odd file type arriving via e-mail and causing strange behaviors on the network can take immediate action. They can then play back the arrival of the message and see the impact of the file being opened on the network. They can capture the file, put it on a secure drive and send it to McAfee® AVERT™ for detailed analysis. In doing so, malicious code attacks can be resolved in hours, instead of spurring a protracted outbreak and remediation over a period of days. This capability is

Product Highlights: Competitive Comparison

Compared to other similar data capture and network forensics analysis tools, the InfiniStream solution offers:

- Exceptional data capture capabilities—2.9 TB storage, more than three times the average competitor's
- Extremely robust performance on the high-speed Gigabit Ethernet networks that are ubiquitous in today's enterprise environment
- Ease of use in reconstruction and replay functionality; the totality of information that can be replayed is extremely granular
- High levels of security in a purpose-built device with hardened OS and file system
- Superior price performance

particularly useful in detecting cookie-based viruses or new e-mail viruses that are discovered via heuristic analysis in McAfee anti-virus solutions, but for which there is not yet a specific signature file.

- **Hacker attacks:** A security analyst can use the InfiniStream solution to see how a hacker, operating from single or multiple IP addresses, is probing multiple points on an enterprise network via http, ftp, Internet relay chat (IRC), e-mail, and voice over IP (VoIP). Minutes or hours afterward, the InfiniStream visualization console can show how the hacker moved through and attacked the network, replaying the experience and views packet-by-packet.

This capability not only applies to external parties, but internal users, as well. For example, a corporate user with malicious intent could use a laptop with a remote connection or a wireless connection to access the network, downloading files via ftp and probing servers around the company. With InfiniStream software security analysts can look at network traffic originating from a specific IP address and recreate the user's experience, thus analyzing activity that would not be detected by perimeter defense methods.

- **Inappropriate use of resources:** Activities such as downloading large video or streaming audio files, or playing network games, can jeopardize the performance of enterprise networks—networks that are required to conduct business activities. Network Associates Network Performance Orchestrator™ (nPO™) solution, a network optimization platform that improves the manageability of enterprise infrastructure by improving visibility into network performance, can graphically display the problem to the network manager. The administrator can then use InfiniStream functionality to determine exactly what occurred on the network.

Additionally, the InfiniStream solution can be used to gauge intent for viewing inappropriate materials. Its application playback feature can be used to see if a user went directly to an inappropriate site—signaling probable intent to go there—or was diverted by means of a nebulous e-mail or innocuous banner ad, both of which would suggest no intent.

- **Content security:** The news media frequently report on corporate networks being compromised and sensitive information, such as credit card numbers being stolen. If such an event occurred on a network monitored by the InfiniStream solution, security analysts and network managers could reconstruct the hacker's session and see exactly which information had been stolen. The credit card company could then avert public relations and financial disasters by proactively canceling the card numbers, notifying their respective cardholders and replacing the old credit cards with new ones. In today's highly security-conscious environment, this capability can be invaluable to a wide range of organizations such as state, local and federal government institutions, airlines, and many others.

IV. Summary

As network and content security threats escalate in frequency, sophistication, and malice advanced proactive preparation and delayed reactive response are insufficient—today's viruses, worms, and blended threats move swiftly and with utter destruction. Network forensics analysis presents a significant step toward real-time diagnosis and remediation of compromised networks. This emerging discipline combines elements of network management and network security to help organizations maintain maximum uptime of networks that are absolutely mission-critical.

Although network forensics analysis concepts are well established, until recently they have been inadequately realized with underpowered tools. The Network Associates InfiniStream solution presents a dramatic improvement in the network forensics field; it uses reconstructive traffic analysis to investigate security and network events, enable their fast resolution, and prevent their recurrence. For the first time, InfiniStream Security Forensics can answer the heretofore-unanswerable question, "What happened before the network event?" It is the first solution that provides high levels of performance and security through three capabilities:

- Total data capture at the packet level with a high-performance network appliance that offers several unique capabilities:
 - Large storage (2.9 terabytes), allowing up to several days data to be captured and stored for immediate or later analysis
 - Data capture at or near the network core, to better resolve attacks that originated from within the organization

- Analysis of network data with easy-to-use tools
- Visual presentation of information to allow fast, accurate interpretation of the selected data

Together, these three capabilities ensure that security violations and attempted violations can be fully investigated and handled.

The InfiniStream solution is a strong complement to a wide range of other Network Associates products, helping customers extend the return they receive from investment in:

- **McAfee Security anti-virus products:** A wide range of McAfee products—including VirusScan®, WebShield®, NetShield®, GroupShield™, and others—as well as the McAfee Security heuristic analytic engine that can detect new viruses; InfiniStream allows them to quickly be isolated and removed for further investigation, dramatically reducing the possibility of widespread infection.
- **Sniffer Technologies products and Network Performance Orchestrator™:** Sniffer Technologies products' alarm capabilities can notify administrators of suspicious security-related traffic or network performance issues, respectively—which can then be fully examined with the InfiniStream solution.
- **Magic Solutions®:** Many companies use the Network Associates Magic Solutions platform to ensure that the steps required to enforce a security policy are executed. After the InfiniStream solution is used to determine a remedy, Magic Solutions' workflow capabilities can ensure that policies are enforced with steps such as shutting down a port, taking a server offline, or reinstalling a desktop operating system.

These and a wide range of other Network Associates products can be installed and optimized by the Network Associates Expert Services, a group of seasoned professionals that understands the realities of maintaining security and network performance. Expert Services addresses all phases of the network and security management cycle with its assessment, design, deployment, and emergency response services, as well as hands-on training courses to develop the skills of existing staff.

For more information about the Network Associates InfiniStream solution, please visit www.nai.com.

About Network Associates

With headquarters in Santa Clara, Calif., Network Associates, Inc. is a leading supplier of network security and availability solutions. Network Associates is comprised of three product groups: McAfee Security, delivering world-class anti-virus and security products; Sniffer Technologies, a leader in network availability and system security; and Magic Solutions a leader in innovative service management solutions.

For more information, Network Associates can be reached at 972-308-9960 or on the Internet at <http://www.networkassociates.com>.

All Network Associates® products are backed by our PrimeSupport® program and Network Associates Laboratories. Tailored to fit your company's needs, PrimeSupport service offers essential product knowledge and rapid, reliable technical solutions to keep you up and running. Network Associates Laboratories, a world leader in information systems and security, is your guarantee of the ongoing development and refinement of all our technologies.