NPMD for Network Security Forensics

A critical asset in responding to security breaches

The right Network Performance Monitoring and Diagnostics (NPMD) solution can help IT operations deliver superior performance for users. When incorporated into your IT security initiatives, deep packet inspection can strengthen your existing antivirus software, Intrusion Detection System (IDS), and Data Loss Prevention (DLP) defenses.

The ability to capture and store all activity that traverses your IT infrastructure—like a 24/7 security camera—enables your NPMD tool to serve as the backstop of your business' IT security efforts. This white paper outlines the essential product attributes required to achieve these security objectives.

The ominous headlines are incessant; corporate networks and IT resources are under ever-increasing attacks from those seeking sensitive customer or employee information. Whether from unfriendly governments, criminal organizations, or disgruntled individuals, your critical information system assets are constantly threatened.

But, for every open acknowledgement, there are numerous intrusions and violations that remain unreported, either because of concerns regarding the organization's image or worse, because they have yet to be detected. Once an attacker is within the network, it can be very difficult to identify and eliminate the threat without deep-packet inspection.

Security experts agree that the rapidly changing nature of malware, hack attacks, and government espionage practically guarantees your IT infrastructure will be compromised. The question is not whether your corporate network will be compromised, but what to do when the breach is detected. The best NPMD solutions offer network forensic capabilities with post-event intrusion resolution to track and eliminate intrusions as well as fortify existing defenses to prevent future attacks.

Bitrate (PTY) Ltd
Ground Floor Unit 7, Bedfordview Office Park, 3 Riley Road, Bedfordview
Telephone: +27 (0) 11 450 0481 | Fax: +27 (0) 11 450 0482 | Email: info@bitrate.co.za
www.bitrate.co.za

"IT operations teams must leverage network forensic evidence collected by NPMD solutions to help security operations teams solve difficult security problems"

–Gartner Research

Network Performance Monitoring Tools Can Play a Critical Role in Responding to Security Breaches

Vital NPMD Security Features

An effective solution must offer:

- **High-speed (10 Gb and 40 Gb) data center traffic capture**
  The data center is at the core of today's IT infrastructure. Given the volume and speed of traffic—and therefore increase in potential threats—your NPMD solution must be faster.
- **Expert analytics of network activity**
  To find the specific illicit event among millions of legitimate packets you need analysis tools that offer deep-packet inspection to quickly assist in determining when and where a particular anomaly or unexpected incident has occurred.
- **Filter using custom-defined rules**
  The ability to filter packets against these known threat signatures and alert when detected is critical to resolving many malware events.
- **Event replay and session reconstruction**
  Rooting out emerging threats means being able to rewind a network to view past events, often down to individual network conversations.
- **Capacity to store petabytes of traffic data for post-event analysis**
  Since it is often not until after intrusions occur that breaches are detected, it is critical that network traffic is maintained for a relevant period of time—at least 24 to 48 hours. This enables the NPMD solution to act like a surveillance camera that is always on.

Cyberattack Investigation and Breach Detection

Cyberattacks, malware, and unauthorized IT resource access typically generate a recognizable network signature. Full featured NPMD solutions can use complex pattern-matching filters to detect these events and alert the administrator to their presence at the perimeter or on the network. These filters can be applied forensically against captured traffic, alerting the network and security teams when they are detected.

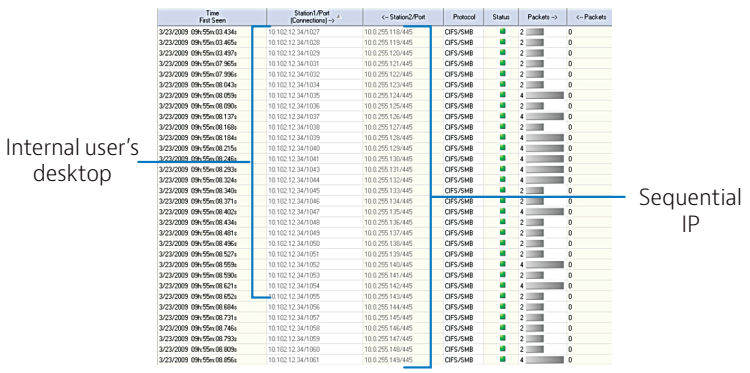
If the security breach includes extraction of critical customer or business data assets whether by an outside malefactor or an "inside job," the subsequent response and investigation can be conducted by forensically viewing captured traffic to fully assess compromised resources. This capability also aids in the case of compliance violations, where regulatory agencies often demand a full accounting of such events.

NPMD solutions such as Observer® GigaStor™ are capable of storing petabytes of packet-level traffic collected from a variety of network topologies; from the core, edge, and branch. Observer Analyzer can then apply advanced filtering to quickly inspect all captured network conversations stored within GigaStor, answering the crucial security questions needed for definitive resolution, "Who, what, when, and where?"

Network Security Forensics in Practice

Consider this customer example: A world-wide Internet marketplace, with over 15 million unique website visits per month and more than 2,000 employees, needed an NPMD solution to better manage and monitor their IT service delivery. Spanning multiple production centers and a large corporate campus, the IT resources incorporated in excess of 500 network devices and 5,000 servers. The multi-tiered and real-time nature of their mission-critical applications called for a solution that would quickly isolate service anomalies in order to avoid any negative revenue impact.

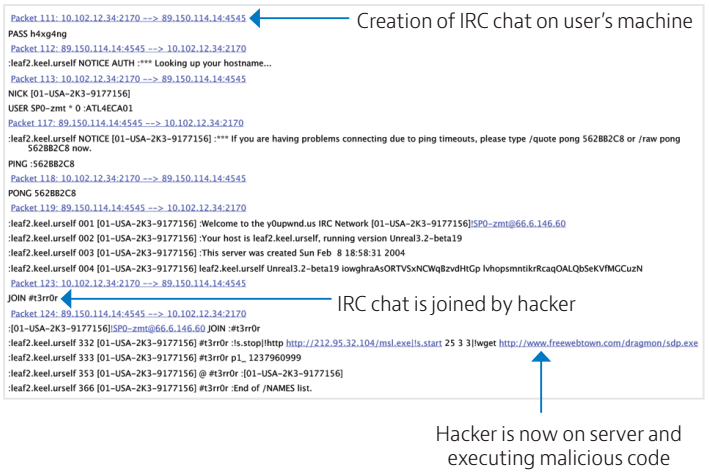
What began as three seemingly benign user complaints regarding slow network and application response time quickly escalated into a potentially serious threat to security. The network engineer used a GigaStor to perform deep-packet network forensic analysis of traffic generated by one of the user's workstations. She discovered it was sending requests to every device on the network; each of these destinations responded in a similar fashion. This activity quickly saturated the network. Desktop support and the security team were notified because an ongoing attack compromising nearly 100 users' machines appeared to be underway.



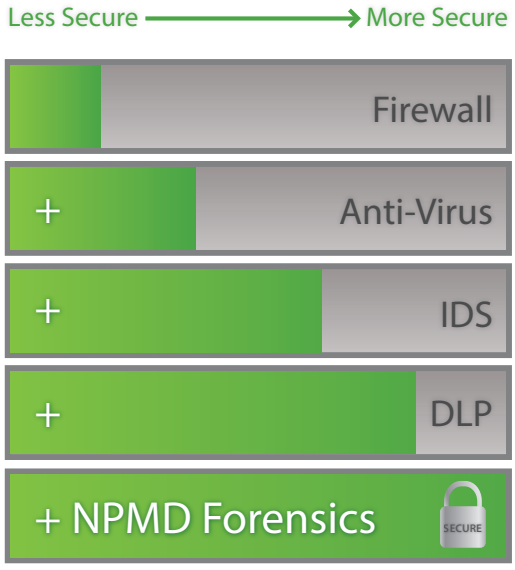
www.bitrate.co.za

Bitrate (PTY) Ltd
Ground Floor Unit 7, Bedfordview Office Park, 3 Riley Road, Bedfordview
Telephone: +27 (0) 11 450 0481 | Fax: +27 (0) 11 450 0482 | Email: info@bitrate.co.za

Once the situation was seemingly under control, the episode repeated with the network again quickly becoming fully saturated. This caused the network manager to infer that one of the users' PCs was infected with a backdoor trojan. GigaStor was used to examine network activity, this time capturing suspicious activity at off-hours on a suspect laptop. With the Observer Platform's in-depth Expert Analysis, it was determined a hacker had created an IRC chat room on the laptop which enabled the network to be re-infected.



"We had implemented a robust, best-in-class, enterprise level IDS and DLP solution," the network manager summarized. "Unfortunately, none of these products identified this attack. Only GigaStor with built-in security forensics was able to detect and determine the root cause."



Conclusion: NPMD Network Forensics – The Backstop to Your Security Efforts

Firewalls, anti-virus software, IDS and DLP systems are necessary but no longer sufficient to achieve the most robust protection or obtain detailed evidence necessary for complete resolution and documentation of cyberattacks and IT breaches. With the capabilities to act like a 24/7 security camera by storing network traffic for extended periods of time and perform deep packet inspection, NPMD solutions enable administrators and security personnel to efficiently detect and root out intrusions, malware, and other unauthorized activities within the IT infrastructure. In a world of ever-increasing cyberattacks, malware, and internal espionage threats, the right NPMD solution can act as the final defense and provide the quickest path to recovery.

VIAVI

BITRATE

Bitrate (PTY) Ltd
Ground Floor Unit 7, Bedfordview Office Park,
3 Riley Road, Bedfordview
Telephone: +27 (0) 11 450 0481
Fax: +27 (0) 11 450 0482
Email: info@bitrate.co.za