# The Buyer's Guide for

# Network Behavior Analysis and Response

## Lancope

**Network Performance + Security Monitoring**

Lancope, Inc.
3650 Brookside Pkwy
Suite 400
Alpharetta, GA 30022
Tel: 770.225.6500
Intl: +44 (0)560 344 8075
Fax: 770.225.6501
sales@lancope.com
www.lancope.com

## Abstract

Network perimeter defenses such as firewall, antivirus and intrusion detection/protection systems (IDS/IPS) are inadequate for defending internal networks. These technologies add expensive complexity to internal IT infrastructure, introduce significant performance bottlenecks, and miss most of the threats they are intended to stop. By comparison, Lancope's **StealthWatch** System of network behavior analysis (NBA) and response security appliances represent a far simpler, less expensive and more effective means to protect internal networks against attack or misuse.

## Introduction

Hackers. Viruses. Worms. It's old news. By now most businesses have invested a lot of money in hardware and software to protect their network perimeter. They have dedicated staff that specializes in network security. They know how to respond to attacks. They know how to document the effectiveness of their solutions.

What organizations often do not know, however, is that their own internal networks represent a rich opportunity for attack and misuse. Security technologies designed for the network perimeter are only minimally effective when deployed across internal networks. Even worse, that low level of functionality rapidly becomes very expensive.

The reasons for this lack of performance are simple. Internal networks and network segments run at very high line speeds, or feature highly segmented and/or highly switched topologies. It is possible to deploy large numbers of perimeter defense devices for each segment, but each application or appliance becomes a chokepoint that severely limits network performance – and still fails to stop threats that originate from within that segment. Policy distribution and administration tasks grow exponentially, and the cost of purchasing and managing so many hardware devices and software agents becomes enormous.

Internal networks must now encompass growing numbers of contractors, mobile users, extranet partners and tightly integrated remote offices. Every one of these points of access represents a free pass around network perimeter defenses. If any one of these trusted relationships becomes compromised, it threatens the integrity of all interior network segments.

Perimeter defenses simply do not see these threats. Devices such as firewalls and intrusion detection/intrusion prevention systems (IDS/IPS) cannot analyze encrypted traffic across a virtual private network (VPN) or trusted link, nor are they able to act against attacks that originate from inside the enterprise, such as:

- Rogue wireless devices
- So-called zero-day attacks, for which attack signatures have not been defined
- Unauthorized remote control or peer-to-peer software
- Trojans or worms introduced via laptops, email or flash-based storage devices (e.g., USB drives)
- Known attacks for which signatures have not been activated

It should not be a surprise that internal threats are growing concern for businesses. Consider the following statistics:

- A 2004 survey of 23 insider misuse incidents discovered that 25% of the insiders involved had criminal records
- A 2005 survey conducted by Deloitte Touche Tohmatsu indicated that approximately 33% more respdents reported that attacks had originated from inside their network perimeter than did respodents citing external atacks
- A Yankee Group and Computer Security Institute report determined that over 50% of attack came from internal networks or unidentified sources
- A 2005 FBI and Computer Security Institute survey found that 56% of organizations reported internal security breaches

White Paper: The Buyer's Guide for Network Behavior Analysis and  Response

- An IDC study estimated that 60% of all serious security threats come from internal sources with privileged access to network resources

Ironically, network security's success at the perimeter tends to work against organizations that try to improve their internal security. Firewalls, antivirus and intrusion detection/prevention systems (IDS/IPS) are regularly budgeted items. Security oversight and documentation is part of normal budgetary processes. New investments for protecting internal resources must prove that they deliver the most protection for the least additional cost, while simultaneously helping meet increasing government and industry regulation.

On the surface, it makes sense to apply perimeter defenses to internal security. However, an organization that tries this strategy soon runs into two problems. First, each internal network or network segment requires its own firewall or IDS/IPS. Every one of these devices is a chokepoint that limits performance. Next, separate policies must be developed, distributed and managed for every device. It is an expensive proposition, and very, very difficult to coordinate, let alone operate efficiently.

Businesses need a better, more cost-effective means to secure internal information resources. As defined by an *InformationWeek* Research Report, "To safeguard proprietary information and ensure business continuity, companies in the United States are intensifying their security initiatives, not just preparing for external threats but also monitoring for breaches from within the enterprise" (*US Information Security,* 2005).

This white paper is a guide for choosing an internal network security solution. First, we take a brief look at what is wrong with using network perimeter technology against internal threats. Then we compare network perimeter systems such as IDS/IPS with Lancope's StealthWatch System of network behavior analysis (NBA) and response appliances to see why StealthWatch is a significantly better, more costeffective alternative.

## Eight Security Questions Every Organization Needs to Ask

### Question #1: Are you satisfied with you IDS/IPS deployments?

*FACT: Most organizations are concerned with the cost and complexity of widespread deployments of IDS/IPS technology.*

Any organization that has tried to apply IDS/IPS to internal security has quickly realized that this technology is very limited when it comes to internal threats. Each internal network or network segment requires its own IDS/IPS gateway. Maintenance, tuning and updates quickly become major challenges.

Threat prioritization and false positives routinely plague IDS/IPS devices. Therefore, IDS/IPS requires large amounts of human intervention to identify truly significant security events that require immediate intervention. This time could be spent on more productive tasks if a more automated technology was in place.

IDS/IPS also suffers from its inability to handle high line speeds – precisely the type of load most likely to be found in a highly switched internal network environment. Limited forensics capabilities and difficulties coordinating IDS/IPS with broader network management services introduce delays between detection and resolution – exactly when and where a delay can cause the greatest amount of damage.

### Question #2: How effective is your IPS deployment when configured for blocking mode?

*FACT: When an IPS blocks access to a port in response to a threat, it also prevents good traffic from getting through.*

IPS technology is at its most effective when it is used to respond to a threat by blocking access to ports or services, or to drop suspicious network packets. Unfortunately, the high level of false positives inherent in an IPS means that good traffic will be blocked along with the bad. Dropped packets create network management challenges. It becomes very difficult to separate security issues from network performance issues, and overall online business operations suffer.

Many organizations try to balance blocking with performance by limiting the thoroughness with which the IPS examines network traffic. Greater throughput, however, means an attack is more likely to sneak through. IPS is also very expensive to deploy as a high-coverage solution for internal networks. The CVE threat database contains more than 15,000 known vulnerabilities, as of January, 2006. Most IPS systems rapidly lose their efficiency if asked to detect and block more than 200 attack signatures. In other words, a typical IPS covers less than 2% of the possible threats in its most useful configuration. That leaves the other 98% completely undetected.

## Question #3: Have you secured your entire internal network?

*FACT: Agent-based solutions are expensive to deploy on an enterprise basis, and the complexity inherent in deploying, updating and managing hundreds or thousands of devices is a major obstacle to* widespread use.

Very few IPS technologies operate at the high line speeds or across the highly segmented architectures common to internal enterprise networks. The reason is simple – it takes too many IPS devices to cover each individual network or segment, and coordinating all of these devices is a logistical nightmare.

There is no simple, cost-effective means to process this huge amount of security information to develop a true, real-time overview of internal security policy violations and overall security performance. Therefore, large parts of internal networks are often left unprotected.

## Question #4: Is your internal enterprise network prepared to handle zeroday attacks that bypass network perimeter defenses?

*FACT: Many successful attacks are designed specifically to evade network perimeter defenses, and can only be detected after they propagate across internal networks and segments.*

The technological limitations of perimeter network security technologies can quickly combine with policy failures, device misconfiguration and misjudgments of the likelihood of a successful attach to create a significant risk to internal networks. Encrypted traffic hides threats from firewalls and IDS/IPS. Trusted connections from contractors, mobile workers, remote offices and extranet partners punch directly through the network perimeter.

It gets worse. Walk-in devices such as USB drives, portable music players, laptops and "smart" phones represent devices that directly connect to internal networks after having been exposed to outside threats. File sharing software, rogue wireless networks and unauthorized devices or applications are another avenue for threats to bypass the network perimeter. Finally, if antivirus or IDS/IPS signatures for a threat have not been activated for any reason, then these attacks, too, will quickly slip through to internal resources.

It is very difficult to identify and isolate any of the issues in real-time, when an attack can be contained most easily. Patching, likewise, does not represent a realistic solution. It takes time to identify vulnerable systems, and each delay means another internal resource remains unprotected.

White Paper: The Buyer's Guide for Network Behavior Analysis and  Response

## Question #5: Can your security systems detect insider misuse, misconfigured devices and unauthorized attempts to access internal network resources in real-time?

*FACT: Insider misuse, misconfigured devices and unauthorized attempts to access internal network resources take significant amounts of time to recognize using network perimeter technologies – if they can be recognized at all.*

The hard truth is that perimeter security cannot detect or mitigate internal misuse. These threats never cross the perimeter. Therefore, internal threats require an internal solution. As discussed above, firewall and IDS/IPS are poor choices for internal security due to expense, complexity and an inability to operate efficiently without crippling normal network operations.

Internal security presents another challenge. Multiple locations, multiple departments with security or IT responsibilities, and multiple network access points combine to make it very difficult to monitor or control internal usage. Without real-time insight into current network security performance, administrators cannot see and react to what is happening now, let alone quickly coordinate an enterprise-wide response.
ntion to identify truly significant security events that require immediate
intervention. This time could be spent on more productive tasks if a more automated technology was in place.

## Question #6: Do you have complete network and host visibility across the breadth of your enterprise network?

*FACT: Hundreds and thousands of devices connect to, and detach from, your networks every day – which greatly complicates maintaining an accurate picture of network usage at any given point in time.*

It is a simple but deadly accurate truism – network security cannot stop what it cannot see. Firewalls and IDS/IPS by definition create a time lag between data collection, data analysis, alerting and response. The larger the organization, the longer the time lag between attack detection on one network segment and true containment across the rest of the company.

Many perimeter-style network security systems reduce this time lag by sampling data or restricting the number of attack signatures in use. Neither option delivers truly comprehensive protection, and gaps in security datasets make it extremely difficult to gauge overall security performance by measuring hostlevel activity over time.

## Question #7: Do you use existing routers and switches as automated surveillance points across your internal networks?

*FACT: Existing IT infrastructure including routers and switches often has the capability to capture flow data that details critical security information. These devices represent a missed opportunity to improve security performance at little additional expense.*

Many routers and switches from major vendors such as Cisco, Juniper and Foundry Networks generate rich point-to-point communications records for every session or transaction crossing an internal network. These same data flows also provide at least partial coverage for communications that bridge the network perimeter.

Existing infrastructure is rarely tapped as an internal security surveillance resource. This inability to use what is already in place often leads to unnecessary duplication of function and a waste of limited security budgets.

## Question #8: Do you use, or plan to use, MPLS as part of your wide area network management solution?

*FACT: MPLS makes it much easier for network administrators to route network traffic around link failures, congestion and performance bottlenecks. However, MPLS also grants full connectivity from any remote site to any other remote site or central office – without the traditional hub-and-spoke gateways that limit access from one subnet to another.*

MPLS – multiprotocol label switching –integrates Layer 2 information on network links with Layer 3 IP information within a single system (e.g., an Internet service provider) to simplify and improve packet exchange. In terms of quality of service, MPLS helps ISPs manage different kinds of data streams more efficiently based on priority and service plan. Customers benefit directly from MPLS through minimal latency and packet loss across their network connections.

However, MPLS carries serious security implications that are often not fully taken into consideration. Since the traditional hub-and-spoke network model dissolves into an enterprise-wide MPLS cloud, security administrators must decide which new equipment to deploy to capture inter-site communications and detect active threats. IDS/IPS technology requires fixed network gateways in order to work, which makes IDS/IPS less than suitable for MPLS environments. A much better alternative is a security solution that uses network flow information (native capture, NetFlow or sFlow) to recognize and mitigate improper behavior within an MPLS deployment.

## How to Determine If You Need a Different Internal Security Solution

The following grid is based on the questions discussed above. Fill out the grid using "yes" or "no" answers. If two or more answers are "no," then you may want to reconsider your internal security solution.

| | Yes | No |
|---|---|---|
| Are you satisfied with your IDS/IPS deployments? | | |
| Is your IPS deployment operating efficiently when configured for blocking mode? | | |
| Have you secured your entire internal network? | | |
| Is your internal enterprise network prepared to handle zero-day attacks that bypass network perimeter defenses? | | |
| Can your security systems detect insider misuse, misconfigured devices and unauthorized attempts to access internal network resources in real-time? | | |
| Do you have complete network and host visibility across the breadth of your enterprise network? | | |
| Do you use existing routers and switches as automated surveillance points across your internal networks? | | |
| Do you use, or plan to use, MPLS as part of your wide area network management solution? | | |

## A Better Way to Secure Internal Networks

In fact, there is a better, lower cost, more effective way to secure internal networks. Lancope's **StealthWatch** System of network behavior analysis (NBA) and response security appliances represent a different approach, one that improves overall security posture without requiring additional complexity or massive investments in infrastructure or staff.

Consider the following. StealthWatch:

White Paper: The Buyer's Guide for Network Behavior Analysis and Response

## Is easy to install, manage and update

StealthWatch is a self-tuning security solution that is ready within hours of installation – plus automatically learns what it needs to improve protection over time. Unlike antivirus and IDS/IPS, StealthWatch does not require attack signatures, so it is never out of date, and protects against threats for which attack signatures do not yet exist.

StealthWatch's efficient design delivers rich forensic data for compliance documentation and investigation of security events. This level of detail is available in real-time, and does not require data sampling or reduced network performance. In addition, a small number of StealthWatch appliances can provide comprehensive coverage for large numbers of hosts across massive internal enterprise network environments.

## Works without dropping packets or blocking services

StealthWatch works by baselining normal network behavior. Any variance from expected patterns of use triggers an alert. StealthWatch then automatically prioritizes the severity of the threat, balances relative risk against the value of the affected network assets, notifies appropriate staff, and optionally takes direct action to isolate and minimize the attack.

This behavior-based design protects against any threat, not just a small subset for which an attack signature has been created, deployed and activated. As a result, StealthWatch instantly pinpoints and contains zero-day attacks and unknown threats. At the same time, StealthWatch's passive operation means that this exceptional level of protection works without dropping packets or blocking services. There are very few false positives, and little or no effect on network performance or trust relationships.

## Covers all internal network infrastructure-even on high speed, highly switched or highly segmented internal networks

StealthWatch does not use software agents, so it can protect both networks and hosts at very reasonable cost. Each appliance can support over 400,000 hosts, and detects and mitigates all threats, including internal mis-use, device and application misconfiguration, and security policy violations.

Better yet, StealthWatch operates at very high line speeds, even on highly switched or highly segmented internal networks. Just a few StealthWatch appliances can cover the full breadth of an enterprise's internal network infrastructure.

## Responds in real-time to threats that evade perimeter defenses

StealthWatch instantly detects threats that originate inside the network perimeter, attacks waged from within encrypted network traffic, and the presence of unauthorized internal network connections and applications. As such, it represents a much more efficient use of security budget than internal deployments of firewalls and IDS/IPS. Add in StealthWatch's ability to immediately recognize internal misuse and misconfigured devices, and it becomes clear how StealthWatch can reduce the time and cost associated with recognizing and stop-ping zero-day attacks by as much as 80%.

## Instantly recognizes unexpected network traffic - and the reason behind that traffic

StealthWatch operates transparently to detect access policy violations across departments and security zones. This ability to deliver enterprise-wide security insight connects policy violations with specific devices, anywhere inside the network perimeter – then instantly transmits this information to appropriate staff. As a result, StealthWatch helps organizations coordinate threat response across multiple departments and locations for faster, more effective mitigation.

White Paper: The Buyer's Guide for Network Behavior Analysis and Response

## Provides a true, enterprise-wide overview of overall security performance in real-time

StealthWatch monitors all connected devices within an enterprise organization's internal networks. Each appliance delivers end-point intelligence on up to 512,000 individual network devices. In addition, StealthWatch enables "virtual security zones" that simplify protection for complex coverage requirements. Administrators gain the ability to efficiently manage complex multiple security structures without requiring significant amounts of additional hardware and software.

## Leverages existing IT infrastructure to maximize the utility of each security budget dollar

Flow-based routers and switches can transparently capture detailed data that can be applied directly to network security. However, relatively few enterprise organizations take advantage of the hardware and software already in place in order to improve their security operations. This oversight is particularly acute for organizations using MPLS to facilitate more efficient network management operations.

StealthWatch uses native flow capture, NetFlow or sFlow data to generate detailed session and transaction information without requiring additional native capture devices. StealthWatch then applies powerful correlation and analysis to organize this information for alerting and response.

These flow-based solutions deliver exceptional levels of internal network security performance at equally exceptional levels of value. In addition, StealthWatch's network behavior analysis technology protects seamlessly within enterprise-wide MPLS deployments.

## Conclusion

Lancope's *StealthWatch* System represents a faster, more efficient, more cost-effective means to protect internal network resources. For example, consider the following examples of why StealthWatch outperforms IDS/IPS:

|  | StealthWatch | IDS/IPS |
|---|---|---|
| **Threat Detection** | Detects zero-day attacks, worms, viruses and other malware | Only if signatures available and active |
| **Policy Compliance** | Discovers unauthorized applications and prevents network misuse by internal users | No |
| **Prioritization** | Helps staff focus immediately on most significant events | Data must be collected and analyzed before alerting and response |
| **End-Point Intelligence** | Maintains host integrity and identifies rogue devices and applications | Only recognizes threats contained within network packets |
| **Network Integrity** | Maintains network health through network-wide visibility and flow analysis | Improper tuning and configuration can degrade network integrity by dropping good packets and blocking necessary services and applications |
| **Automated Mitigation** | Quarantines compromised hosts to limit additional exposure | Can only drop packets and block access to services and applications |
| **Logging and Analysis** | Automatically investigates and diagnoses internal security events | Can only provide raw information – relies on additional levels of hardware and software for forensic capabilities |
| **Traffic Accounting** | Monitors network performance and usage as well as security data | Security-only focus hinders rather than helps security-IT integration |
| **MPLS Compatibility** | Provides full, transparent protection across remote sites and central offices using MPLS | Requires discrete gateways in order to monitor network traffic – very difficult to integrate with MPLS |

## Conclusion

StealthWatch's advanced application of network behavior analysis and response delivers internal protection that firewalls, antivirus and IDS/IPS cannot match. In addition, StealthWatch can leverage existing IT infrastructure to eliminate up to 80% of the time, cost and complexity associated with internal threat detection and response. There is a better way to maintain host integrity, prevent internal attacks and misuse, and improve overall network health at one-third the cost of alternative systems such as IDS/IPS. That solution is Stealth-Watch.

## About Lancope®

Lancope®, Inc. is the provider of the StealthWatch™ System, the most widely used network behaviour analysis (NBA) and response solution that unifies flow-based anomaly detection and network performance monitoring to protect critical information assets and ensure availability by preventing costly downtime, repair and loss of reputation. StealthWatch streamlines security and network operations into one process, reduces time and resources, and eliminates the costs and complexity associated with non-integrated point products. Both OPSEC and Common Criteria-certified, StealthWatch received the 2008 and 2007 Global Excellence Award in NBA and was named Best of Show at Interop2006. Defending the networks of Global 2000 organizations, academic institutions and government entities, StealthWatch protects hundreds of enterprise customers worldwide, more than all direct competitors combined. A contributing member of the Trusted Computing Group, Lancope also partners with fellow best-of-breed solution providers through its Technology Alliance Program, which includes Cisco Systems, Foundry Networks, IBM Tivoli, Check Point, TippingPoint, ArcSight and A10 Networks. Lancope is a privately held, venture-backed company headquartered in Atlanta, Georgia. For more information, visit www.lancope.com.

## Get StealthWatch for the Unified Visibility You Need

Discover how StealthWatch provides you with a comprehensive view of application delivery, network operations, and security across the entire enterprise, including physical and virtual environments – all from a single, integrated platform.

**Request a demonstration of StealthWatch at www.lancope.com**

### About Lancope, Inc.

Lancope®, Inc. is a leading provider of flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. Enterprises rely on Lancope to make better network decisions, respond faster to network problem areas and avoid costly outages and downtime — at a fraction of the cost of conventional network monitoring solutions.

### Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

U.S. Sales
+1.770.225.6500
888.419.1462

International Sales
+44 (0)560 344 8075

Website: www.lancope.com
E-mail: sales@lancope.com

WP07192010