The Security Benefits of a Flow-based Intrusion Detection System

Flow-Based
Intrusion Detection Technology
from
Lancope

www.lancope.com

Creators of StealthWatch™
www.stealthwatch.com

High-Speed Network Threat Management

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   1

Contents:

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   2

StealthWatch™ is an advanced information security threat management system that monitors, detects and responds to security breaches and internal network misuse on high-speed corporate networks. Unlike traditional intrusion detection systems, StealthWatch's patent-pending flow-based architecture recognizes undocumented attacks and allows for high throughput while reducing the false positives commonly associated with those tools.

The Pros and Cons of Signature-based Systems

Signature-based detection involves identifying known attack methods and creating a set of rules (signatures) to detect such attacks. Such products are effective at detecting known attack methods and some application-level misuse such as "cgi-bin" attacks. However, security analysts have struggled to effectively configure these products to live up to their promises.

Three well-defined weaknesses in signature-based intrusion detection systems are:

- ❑ Inability to detect undocumented, mutated or encrypted attacks
- ❑ High percentage of false positives that limit product usefulness
- ❑ Packet dropping at higher speeds (typically 30 Mbps and higher)

The StealthWatch Advantage

StealthWatch's flow-based anomaly detection architecture was designed to address these three issues. While the product does not look specifically for application-level exploits, its emphasis on detecting abnormal network behaviors provides corporations with the following benefits:

- ❑ **Attack Recognition of Undocumented/Novel Attacks, DoS Attacks and Trojan Horses** – StealthWatch enables recognition of attacks that typically evade intrusion detection systems such as undocumented attacks, encrypted attacks, mutated signatures, internal hacking attempts, DoS attacks and Trojan Horses. Unlike traditional systems, StealthWatch does not rely on signature updates for this advanced attack recognition. Its anomaly-based recognition starts to do its job from the moment you plug it in.

- ❑ **Increased Detection Accuracy** - StealthWatch quickly differentiates between legitimate and suspicious connections (probes). But instead of alarming you on every ping, probe or scan, StealthWatch builds a profile of each suspicious host. When a host's Concern Index surpasses a user-defined threshold, StealthWatch responds with a full array of customizable capabilities including pager, email, SNMP traps and connection disruption.

- ❑ **High-speed Network Scalability** - By not having to search through strings of signature data, StealthWatch's flow-based engine can analyze network traffic at bandwidth requirements up to 1 Gbps.

This paper explains StealthWatch's innovative flow-based architecture and how it enables these benefits. With StealthWatch as the foundation of a layered intrusion detection program, corporations can finally defend themselves against today's advanced hacker.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   3

Understanding Our Flow-based Architecture

StealthWatch is an innovative anomaly-based threat management system. It features a patent-pending flow-based architecture that characterizes and tracks network activities to differentiate abnormal network behavior from normal behavior. StealthWatch should not be confused with signature, or protocol anomaly products as it provides a unique new approach to detecting network misuse.

Data Flow Analysis

StealthWatch characterizes and analyzes the data flow between Internet Protocol (IP) devices. In order to get a complete picture of what is occurring on an IP-based data network, it is best to partition the individual data packets into groups that represent a complete communication transaction between two hosts. These groupings of data packets are called flows.

Restated, a flow is defined as the packets exchanged between two hosts that are associated with a single "service". Examples of a service would include using a Web browser to access a single Web server, or using an e-mail program to access a mail server.

In contrast, other intrusion detection systems piece together the packets in a TCP connection to collect the stream of bytes being transmitted and then look for certain strings of characters in the data, called signatures. These signatures are particular data strings that have been discovered in known hacker "exploits" and documented and added to the signature system's database of known exploits. Even with all this effort, this technique will not recognize a brand new exploit that has not been analyzed for a signature.

Lancope has created two innovative security features built upon data flow analysis to provide advanced attack recognition. These features are called **Concern Index** and **Service Profiler**, and they are explained in detail below.

Concern Index

After StealthWatch associates each packet with a flow, it analyzes certain statistical data and adds it to the flow data record such as number of bytes, packets, and flag-bit combinations. No string search is made for signatures. The statistical data is examined to determine the type of transaction that took place and the record on each host is updated to reflect this new flow information.

The gathered statistical data allows us to determine if a flow represents a legitimate connection or a suspicious connection (possible probe).
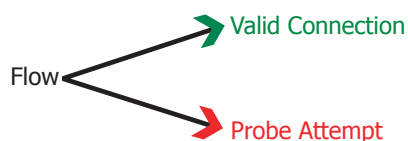
Figure 1. StealthWatch determines whether a flow represents a valid connection or a probe attempt.

StealthWatch identifies and logs probes because they represent the first stage in most external hacking attempts.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   4

Stage 1: A network is probed to determine what types of computers are on the network, their operating systems, their network listener applications (servers), their IP addresses and open port numbers. This is known as network mapping.

Stage 2: Based on the data gathered from step 1, an exploit routine is applied to gain access to a vulnerable computer.

Stage 3: An operation is applied that accomplishes the attacker's objectives (e.g. downloading sensitive data from a financial server).

By documenting probe attempts in **Stage 1,** StealthWatch is gathering critical indicators regarding future attacks. In order to take advantage of this reconnaissance information, StealthWatch logs the suspicious activity and assigns a measurement of concern to the suspicious host. This measurement is called Concern Index.

StealthWatch provides data on the scanning host that can be obtained from techniques such as a DNS name lookup and a traceroute back to the scanning host. Some scanners have software that alerts them when they have been tracerouted and they stop immediately, so StealthWatch watches and logs data prior to launching the traceroute. Thus, an up-to-date list of suspicious hosts and their IP addresses is maintained.

Then StealthWatch watches closely to detect whenever a local host responds to one of these suspicious hosts with anything more than a TCP Reset or an ICMP "No Listener". When this occurs it indicates that a hacker has successfully found a vulnerable host and is communicating with that host. StealthWatch alerts the network administrator immediately with what is referred to as a **"Touched Host Alarm"**.

Service Profiling

In addition to the Concern Index, StealthWatch has another major characterization feature that enables it to catch undocumented or altered attacks. It is called **Service Profiling** and it is used to confirm that network connections appearing to be legitimate (those that are not considered possible probes) are, in fact, considered appropriate in the eyes of the organization.

For example, a hacking technique that is seen with increasing frequency is the installation of a Trojan Horse program by an innocent looking program, such as an email or network news attachment. When a Trojan Horse is introduced onto a network, **Stage 1** and **2** of the attack process are bypassed and **Stage 3** becomes the first stage to show in network activity. In order to recognize these attacks, StealthWatch does not rely on building a measurement of concern, but instead turns to its Service Profiler.
With this feature, StealthWatch keeps a database of what Services each local host is allowed to offer (as a server) or access (as a client). If a flow does not fit this **Host Service Profile**, the discrepancy is reported. StealthWatch automatically builds the Host Service Profiles while operating in several progressive modes.

Mode 1: Local hosts and Host Service Profile points are detected and profiles are characterized.

Mode 2: Service profiles continue to build up, but every day the new Out-of-profile (OoP) points are reported on a Web page. At the end of the day, the new points are added to the relevant Host Service

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   5

Profile.

Mode 3: The profiles are locked. New points are not automatically added to the Host Service Profiles. Network managers can inspect this list of Out-of-profile services on the Web and manually add applicable services to the Host Service Profiles, or delete services from a Host Service Profile if they feel the service should not be allowed. (a personal Web server with vacation photos, for instance)

Mode 4: Service Profile Lockdown. As soon as an Out-of-profile service is detected, an alarm is sent to the network manager.

Service Profiling is extremely effective in detecting back doors/Trojan Horses, but it is also helpful in locating other areas of network misuse and abuse.

❑ What about the story in the local paper that describes how to download software and listen to your favorite background music or your hometown radio station on your PC? Many office workers will do this without having a thought about tying up limited Internet connection capacity. Fifty Web radios will completely use up the capacity of a T1 connection.

❑ There are an increasing number of "spyware" programs out on the Web today that collect personal information and send it back to a hacker without telling the user. Without the Service Profiler feature, there is nothing to prevent "spyware" applications from collecting company proprietary information.

❑ Another problem is presented when users install software like Napster or Gnutella, which may present security problems as well as consume network bandwidth. StealthWatch will report these activities as Out-of-Profile services. Signature-based systems do nothing to detect these unauthorized services.

Signature-based systems have signatures for some backdoors/Trojan horses. However, most of these are tied to specific ports. It is a trivial task for a hacker to change the port used in order to escape detection by a signature system. When using StealthWatch, mutated and encrypted Trojan Horses are still detected as Out-of-Profile.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   6

Benefits of a Flow-based Architecture

1. Attack Recognition of Undocumented Attacks and Altered Signatures

As demonstrated above, once a suspicious host has begun communicating with an internal host, a major alarm is sent to the security team. In addition, a major alarm is triggered when an unauthorized service is run on your internal hosts (if in Host Profile mode 4). Thus, undocumented attacks in the form of suspicious network behavior, altered signatures, DoS attacks and Trojan Horses are detected. StealthWatch also provides traffic analysis information and alerts you to internal security policy violations before they compromise your network.

Put in perspective, once the Concern Index and Service Profiler characterize activities on a network, StealthWatch can detect **Stages 1** and **3**, and sometimes **Stage 2** of the attack process as abnormal or Out-of-Profile activities.

In contrast, the exploit routine often seen in **Stage 2** can be detected by a signature-based intrusion detection system, but only if it has been seen before, captured and analyzed by that vendor. In addition, the slightest alteration to a known attack can enable hackers to bypass a signature-based system altogether *(see Section 4 - Encrypted Back Orifice case study).*

StealthWatch Architecture

APPLICATION			
Intrusion Detection	Security Policy Management	DoS Monitoring & Response	Forensics

BENEFITS		
Anomaly Detection	Intelligent Alarming	High Throughput

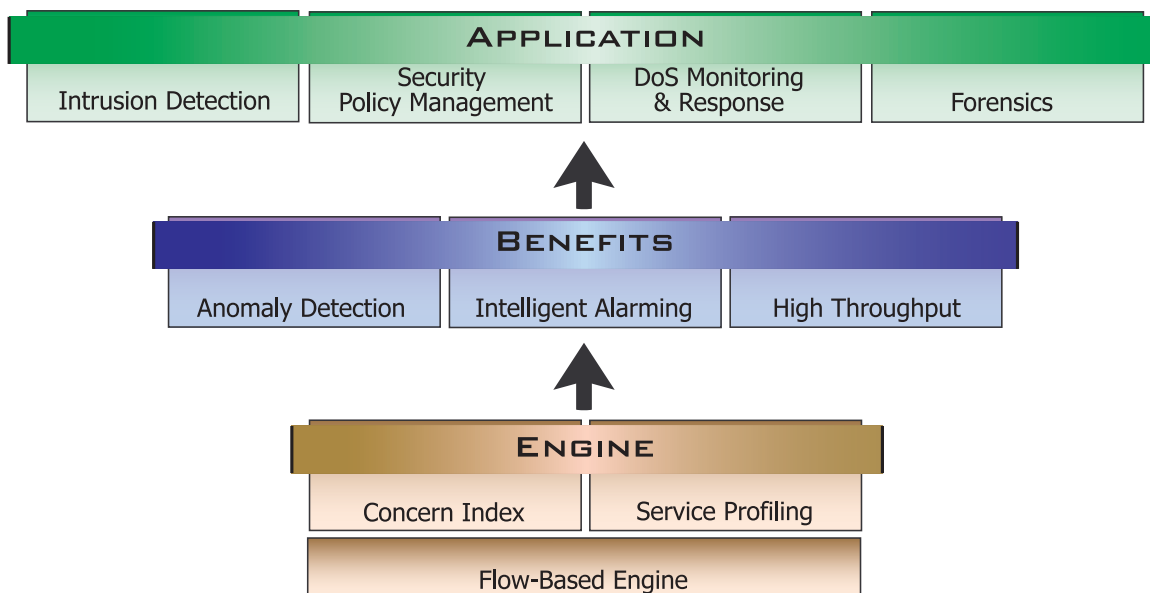| ENGINE	
Concern Index	Service Profiling
Flow-Based Engine	

Figure 2. StealthWatch's architecture as viewed by layer. StealthWatch contains a patent-pending flow-based engine on top of a secure appliance solution. The engine enables two unique security features called Concern Index and Service Profiler that provide improved network monitoring capabilities. Your enterprise benefits by having a solution that provides advanced intrusion detection as well as security policy management, DoS monitoring and response and forensics.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   7

2. Increased Detection Accuracy

In addition to advanced attack recognition of undocumented and altered attacks, StealthWatch's flow-based architecture allows for improved decision-making and fewer false positives. As described above, the analysis of data by flow allows StealthWatch to distinguish normal connections - usually between a client and server - from incomplete or rejected transactions (potential probes). A misleading picture of network activity would result if the probes generated by a hacker for scanning or exploitation, or even common connection errors, were treated as actual network connections.

For example, some probe attempts appear like unnatural network activities and they are immediately recognizable. But other times, probes resemble erroneous or unsuccessful connections that are seen frequently in normal network operations. Only by correlation with other events can these be recognized as part of a probing activity. StealthWatch does correlate these events, and each time a host is responsible for a potential probe, its Concern Index is increased and documented.

As an analogy, if a stranger rattled your front door and then said he had the wrong address, you would have no basis to call the police. If he continued down the street doing the same thing, his Concern Index would increase to the point that calling the police would be appropriate (an IP address scan). The same would be true if he rattled numerous doors and windows on the same house (a TCP or UDP port scan).

The following example highlights the importance of flow correlation for accurate detection:

Host Trudy sends three packets to host Bob with a source port number fixed at 64,000 and destination port numbers of 23, 25, 111. Treated as one Flow, this is quickly determined to be a port scan since the source port number did not vary.

Without this step, the probe above would lead to the erroneous conclusion that host Bob was running server programs on ports 23, 25, and 111 (Telnet, SMTP, and Sun RPC). Since Bob responded with TCP reset packets, he should not be credited with operating these server applications.

If the data were collected as three different TCP connections, each connection could be due to a common type of error seen on networks. A further correlation step for all TCP connections would be necessary before the important conclusion – made quickly from the single Flow data record – could be made. Since there can be many simultaneous TCP connection in progress or recently ended, a good bit of CPU time would be required to continually search for such a correlation by a product or person that was not using the Flow-based correlation method.

StealthWatch does not alarm on every ping, scan and probe. It builds concern for suspicious hosts by correlating activities on the network, and only triggers an alarm when those hosts build enough concern to cross the network administrator's pre-determined threshold. The result is a sensitive product that gathers and correlates all suspicious activity without the resulting false positives associated with overly sensitive signature-based intrusion detection systems.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   8

3. High Speed Network Scalability

The third benefit of StealthWatch's flow-based architecture is high-speed network scalability. Intrusion detection systems piece together the packets in a TCP connection to collect the stream of bytes and then look for certain strings of characters in the data, called signatures. These signatures are particular data strings that have been discovered in known hacker "exploits". The more signatures in the intrusion detection system's collection, the longer it takes to do an exhaustive search on each data stream.

In contrast, StealthWatch need not rely on signature matching to determine suspicious activity, so there is no latency introduced as the signature database grows larger. Additionally, building flows rather than piecing together the packets in a TCP connection is far more effective. On one network monitored by StealthWatch, one flow equaled an average of 5 TCP or UDP connections, or 160 packets, or 50,000 bytes. While these numbers vary from network to network and from day to day, the number of data records to analyze is much smaller when collected on a flow basis.

These efficiencies enable StealthWatch to analyze all the data on high-speed networks running up to 1 Gbps.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   9
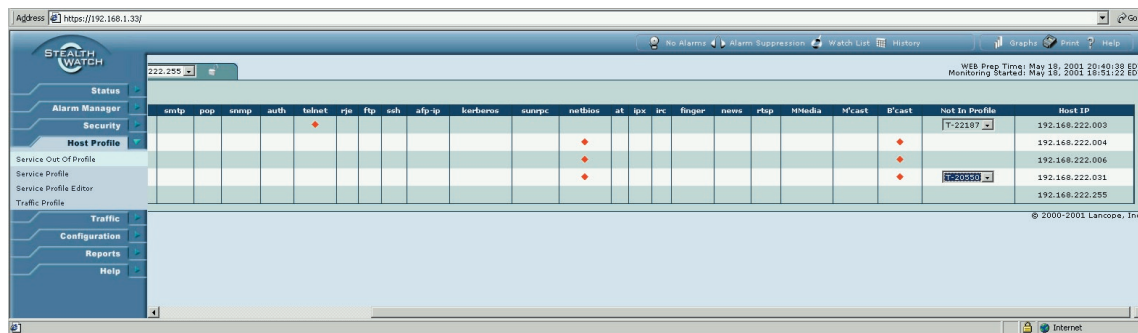
Case Study – Encrypted Back Orifice

In order to demonstrate how StealthWatch catches altered attack methods, Lancope created a test environment in which an altered attack was run against both StealthWatch and an industry-leading signature-based system. Lancope found a plug-in written for Back Orifice on a Script Kiddie Web site, which is well publicized and highly trafficked.

The plug-in creates a new communications module that the author calls Stealthy TCPIO. The Stealthy TCP module for Back Orifice (STCPIO) is readily available on the Internet. Its stated "raison d'être" is to provide a remote administrative tool that will not continually cause alarms on network monitoring equipment. It changes the format of the packet header and encrypts it, so that the packet no longer looks like a Back Orifice packet.

We configured a Back Orifice server to communicate solely with this STCPIO module on port 20550. The encryption used was a fairly weak method called XOR. The server was installed and a corresponding client was created/installed.

The system was instructed to perform a number of actions on the BO server system such as registry editing, keyboard capture and file listings. During this session, StealthWatch noted that the TCP traffic on the high port was Out-of-Profile for that particular host and sent an alarm. *(see Figure 3 – Screenshot of Host Profile interface)*

The signature-based system did not detect this new Back Orifice traffic, presumably because the traffic did not match the included Back Orifice signatures.

Figure 3.   StealthWatch screen shot of Host Profile. Indicating Out-of-Profile Services being run on internal hosts

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   10

StealthWatch Applications

StealthWatch expands the definition of intrusion detection by providing the following four applications:

1. Advanced Attack Recognition, Alert and Response

As discussed in detail in this White Paper, StealthWatch enables recognition of attacks that typically evade intrusion detection systems such as undocumented attacks, encrypted attacks, mutated signatures, internal hacking attempts, DoS attacks and Trojan Horses. Unlike traditional systems, Stealth-Watch does not rely on signature updates for this advanced attack recognition. Its anomaly-based recognition starts to do its job from the moment you plug it in.

In addition, StealthWatch reduces the number of false positives that hound security teams on a daily basis. Instead of alarming on every ping and scan, StealthWatch correlates this information, building a complete picture of the reconnaissance activity on your network, but only alarming you when this activity builds enough concern to indicate a legitimate threat.

StealthWatch provides security teams with a number of response methods to combat attackers that include email, pager and SNMP alerts as well as session disruption. In addition, StealthWatch can quickly trace the source of attacks, a crucial time-saving tool when responding to attackers.

2. Security Policy Management and Enforcement

A critical component in the network security equation is the ability to monitor services that are run on a daily basis within your network. Maintaining a timely and complete picture of network services on each host is almost impossible to do using manual techniques, and traditional network management tools are laborious at best. But StealthWatch provides a unique and necessary component in this arena, allowing your security team to set policies and enforce them.

Our service profiler allows you to view the services running on your network per host and to determine which are appropriate and in profile. You will be notified whenever an out-of-profile service is run. This unique type of data visualization provides both knowledge and control.

3. Denial-of-Service Monitoring and Response

A Denial-of-Service attack, which altogether shuts down your network capabilities, is the most feared and most talked about network attack in the cyber world today. While prevention of distributed DoS attacks has proven elusive to network administrators, StealthWatch provides unparalleled detection, notification, trace-back and forensics features to help you fight back.

4. Forensics

StealthWatch's patent-pending technology, called data flow analysis, provides a valuable new forensics tool – the network flow log. By characterizing each flow that occurs on your network, StealthWatch can maintain a detailed and easy-to-digest trail of information. This log is maintained for 60 days and can be archived for later use. In addition, StealthWatch's provides on-demand, daily and weekly reports of network activity.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   11

The Appliance Approach

StealthWatch is an easy-to-install and easy-to-manage appliance solution. It can be installed and con-figured in minutes and is monitored centrally and remotely using its web-based interface. In addition, unlike insecure software-only solutions, StealthWatch is hardened, optimized and battle-tested to pro-vide you with a secure intrusion detection solution.

StealthWatch is available in two models:

G1 – Same advanced functionality in an optical gigabit solution that handles throughput up to 1 Gbps. Allows high-volume data centers to achieve real-time monitoring of performance and mis-sion-critical security.

M100 – Provides advanced threat management capabilities to high-speed corporate networks. Handles full duplex 100 Mbps Ethernet traffic.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   12

Conclusion

The universe of network attack methods is growing exponentially. Today's corporation is combating more advanced attackers with more advanced attack methods. In addition, the automated versions of these attack methods are widely distributed throughout the hacking community, arming even the most amateur Script Kiddie with highly dangerous tools. This scenario puts tremendous strain on security professionals who have limited products and tools with which to do battle. StealthWatch raises the bar in automated intrusion detection by providing:

- ❑ **Attack recognition of undocumented attacks (e.g. altered signatures, encrypted attacks) and Trojan Horses**
- ❑ **Increased detection accuracy**
- ❑ **High-speed Network scalability**

Signature-Based IDS	Flow-Based IDS
Detects application-level exploits	*(Does not look at packet payload)*
(Dependant upon signature updates)	Detects encrypted attacks, encrypted signatures, Trojan Horse, and internal policy misuses
(Alerts on every unique ping and scan)	Correlation provides increased detection and reduced false positives
(Drops packets at higher speeds – allwing attacks to go by unnoticed)	Scales to run on full duplex 100 Mbps Ethernet to One Gbps.

Figure 4. Benefits comparison of Signature-based Solutions vs. StealthWatch

In addition, Stealthwatch expands current definitions of intrusion detection providing a unique tool for managing the increasing threats to your network.

1. StealthWatch's service profiler provides a unique and easy –o-use solution for network policy management and enforcement.
2. StealthWatch provides state of the art Denial of Service monitoring and response.
3. StealthWatch's patent-pending technology, data flow analysis, provides a valuable new forensics tool – the network flow log. By characterizing each flow that occurs on your network, StealthWatch can maintain a detailed and easy-to-digest trail of information.

With StealthWatch as the foundation of a layered intrusion detection program, corporations finally stand a chance against today's advanced hacker.

Lancope, Inc. - 3155 Royal Drive - Building 100 - Alpharetta, GA 30022 - P: 678.566.4750 - F: 678.566.4891 - info@lancope.com

www.StealthWatch.com   13