

**The Role of
Network Behavior Analysis & Response Systems
in the Enterprise**

**3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022
P: 770.225.6500
F: 770.225.6501**

**INFO@LANCOPE.COM
WWW.LANCOPE.COM**



ROLE OF NETWORK BEHAVIOR ANALYSIS & RESPONSE SYSTEMS IN THE ENTERPRISE

	1
The Need to Optimize Security and Network Operations	3
More Effective and Efficient Security and Network Operations	4
Detect Unknown and Known Attacks in High-Speed Networks without Signatures	4
Prioritize and Mitigate Threats from Inside and Outside Your Network	4
Reduce Misconfigurations, Enforce Policy and Optimize Network Utilization	4
Streamline Network Management and Planning	5
Insightful Forensic Analysis Facilitates Remediation Efforts	5
Flow-based Architecture Delivers Security through Network Intelligence	6
Flow-based Statistical Anomaly Detection and Correlation	7
Concern Index	7
Behavioral Base-lining and Network Profiling	8
Explicit Zone-based Security and Network Usage Policies	8
Implementing StealthWatch	10
Defense-in-Depth Architecture	10
StealthWatch Management Console Is Your Dashboard	12
Integration with Third Party Signature-based IDS	13
Quarantine Infections with Adaptable Mitigation	13
Quarantine Infections with Adaptable Mitigation	14
Conclusion	16

Legal Notices and Disclaimers: The information contained in this document is proprietary and confidential to Lancope. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the express written permission of Lancope. For information on site licenses and multiple copy discounts, contact Lancope. This document is subject to change without notice. While Lancope has endeavored to provide a high level of accuracy, no complete assurances of accuracy can be provided. If you find any problems with this document, please report them to Lancope in writing.

Lancope is a registered trademark and StealthWatch is a trademark of Lancope, Inc. All other registered or unregistered trademarks are the sole property of their respective owners.

© 2006 Lancope, Inc. All rights reserved.

The Need to Optimize Security and Network Operations

Your business operations and assets are under multiple points of attack from both inside and outside your network. Organizations face escalating security risks and network availability requirements as they open their networks for communications and transactions with key customers, critical business partners and trusted employees. This increasingly ambiguous perimeter along with security policy violations and misconfigured network devices leaves applications, data and systems inside the network vulnerable to rapidly propagating new attacks and insider security breaches. In fact, *Gartner estimates that over 70% of unauthorized access to information systems are committed by insiders.*

Network and security managers face a significant challenge as they attempt to create a delicate balance between open access to enable business and the need to protect and maintain the availability of corporate information assets. Although valuable components of defense-in-depth strategies, firewalls and other perimeter-focused network security devices are largely ineffective against insider threats. Additionally, traditional intrusion detection systems (IDSs) require prior knowledge of attacks, have high false alarm rates, necessitate ongoing maintenance of databases and lose effectiveness in high-speed networks. Many “external” attacks, such as SQL Slammer and M32/Blaster, bypass perimeter defenses to enter a network from the inside as mobile users or business partners with unprotected machines become infected and unsuspectingly introduce attacks on internal network segments. The result is significant network downtime, lost productivity, and an inability to conduct critical business operations.

For many organizations, improperly configured network and security devices and a lack of policies serves to multiply the security risk, introduce business risks and impact network performance. Peer-to-peer file sharing, unnecessary network services and remote-access applications can introduce significant vulnerabilities inside your network. *Gartner estimates that today 65 percent of network risks result from misconfigured devices.* Whether the result of innocent mistakes, user ignorance or malicious intent, unauthorized applications and misconfigured network infrastructure not only pose significant security and financial risks but also waste valuable network resources.

Driven by the need to save costs, integrate acquisitions, and/or drive revenues, businesses are consolidating, migrating, and/or expanding network operations. Organizations need the ability to automatically profile and analyze typical network behavior to understand the impact of such activity from both a network and security operations perspective. This understanding enables effective planning and process to expedite smooth transitions and security policy compliance in order to more quickly realize business objectives.

Securing and managing today’s networks requires scalable, innovative solutions that extend the capabilities of existing network and security products, operate effectively in the core and overcome the challenges of traditional IDSs. Network and security managers need continuous intelligence about the behavior of workstations, servers, and network devices to more efficiently monitor and enhance the security posture and operations of their network.

More Effective and Efficient Security and Network Operations

Defending and managing your enterprise network requires your IT organization to proactively address vulnerabilities and rapidly detect attacks, create and enforce network and security policies and gain insightful network intelligence to optimize your network and security operations. StealthWatch by Lancope is a next-generation network security solution that combines behavior-based threat detection, continuous assessment of risks and security policy compliance, insightful forensic analysis and network management capabilities. With integrated visibility across network security, traffic characteristics and host-level activity, StealthWatch delivers unparalleled network protection and optimization.

Detect Unknown and Known Attacks in High-Speed Networks without Signatures

StealthWatch dynamically detects deviations from typical and allowable behavior, as defined by protocols, automatically tuned baselines and administrator-defined policies. This enables the rapid identification of zero-hour attacks as well as known threats without the burden of maintaining signatures or requiring prior knowledge of attacks. StealthWatch's flow-based behavioral analysis excels at detecting worms, Trojans and Denial of Service (DoS) conditions, low and slow reconnaissance and distributed scanning. Encryption, obfuscation and other traditional IDS evasion techniques do not impact its ability to detect and prioritize attacks, vulnerabilities and network misuse. Operating at gigabit speeds, StealthWatch is particularly effective at securing the core of your network as well as the perimeter.

Prioritize and Mitigate Threats from Inside and Outside Your Network

StealthWatch enhances the efficiency of security teams by prioritizing and mitigating malicious network and host behavior. By continuously correlating signs of suspicious behavior and prioritizing threats through a proprietary Concern Index, StealthWatch improves productivity and effectiveness by enabling the network security team to focus on the real threats, not the flood of false positives. In addition, StealthWatch will soon provide enhanced threat mitigation that protects both the core of the network as well as the perimeter, leveraging your organizations' existing investments in firewalls and routing infrastructure. With StealthWatch, administrators will be able to customize the mitigation response based on a combination of alarm type, IP address, protocol, and/or port number. Through early identification and mitigation of threats, StealthWatch minimizes the impact of attacks on your network in terms of downtime, lost productivity and remediation efforts.

Reduce Misconfigurations, Enforce Policy and Optimize Network Utilization

StealthWatch reaches beyond threat detection to provide powerful tools that proactively eliminate risks and pinpoint inefficient network utilization. By identifying unauthorized applications, nonessential network services and misconfigured network devices, StealthWatch provides more effective security and network operations, while minimizing legal and financial risks to your organization. Early detection and remediation of security policy violations can prevent attackers from taking advantage of network exposures. Regardless of obfuscation techniques, StealthWatch identifies popular peer-to-peer file sharing applications that introduce new vulnerabilities, consume significant bandwidth and create substantial liabilities.

Gathering a timely and complete picture of network services on each host is critical, but nearly impossible to do manually. Traditional network scanning tools are laborious and capture only a static picture while host-based systems are expensive to deploy and maintain. With StealthWatch's behavioral base-lining, administrators can easily view the services running on the network (per host and per zone) to determine which are appropriate and in profile. This illumination of your network efficiently and cost-effectively

provides a baseline from which to establish, audit and enforce network usage policies as well as remediate network exposures.

Streamline Network Management and Planning

As a value-added benefit of StealthWatch's flow-based analysis, network and security teams can analyze network behavior to understand network usage, identify malfunctioning devices, and detect trends. This can help organizations anticipate a need to plan for additional capacity in order to avoid critical applications and/or data from becoming inaccessible. Additionally, StealthWatch can help minimize the impact of network changes, avoid quality of service issues, and accelerate the time to relocate or deploy network and security infrastructure in support of network migration, consolidation, or expansion efforts. StealthWatch is also useful for monitoring network performance and auditing change management process.

Insightful Forensic Analysis Facilitates Remediation Efforts

Despite your best efforts, networks occasionally still come under attack. In these situations, StealthWatch delivers insightful forensic analysis, which security administrators can use to pinpoint root cause, identify affected hosts and perform detailed attack analyses. In addition, the analysis of flow details enables rapid understanding of attacks in order to better assess the impact and facilitate remediation of security events. Operating at gigabit speeds, StealthWatch collects and archives network flow logs for a detailed and easy-to-digest trail of information about network activities that can be summarized through on-demand daily and weekly reports. Armed with this critical information, StealthWatch helps your quickly trace the source of attacks and serves as a crucial time-saving tool when responding to attackers.

Flow-based Architecture Delivers Security through Network Intelligence

As a behavior-based network integrity solution, StealthWatch learns the typical behavior patterns of your systems, networks and applications, creates a profile of what is acceptable on a network and detects deviations from this baseline. Unlike traditional signature-based IDSs which require prior knowledge of all possible “defects” or attacks to recognize potential threats, StealthWatch detects deviations alerting you to possible network attacks, application misuse or other threats. Using these behavior profiles, you can create and enforce powerful security and network usage policies. Additionally, behavior profiles can in turn facilitate network management, planning and analysis.

StealthWatch’s innovative triadic threat detection provides you with early detection and warning of vicious and costly cyber-attacks:

- Flow-based Statistical Anomaly Detection
- Behavioral Base-lining and Network Profiling
- Explicit Zone-based Security Policies

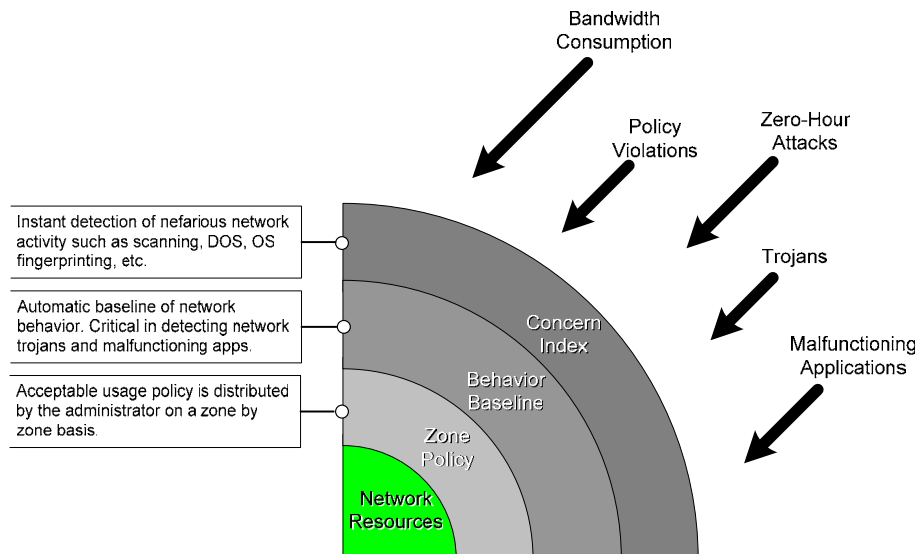


Figure 1: StealthWatch provides three levels of protection against internal and external threats, unauthorized applications, and misconfigured devices.

Flow-based Statistical Anomaly Detection and Correlation

Immediately upon installation, StealthWatch begins observing bi-directional host communications—or “flows”—and bandwidth consumption into and out of the internal network. Each flow is defined as a set of data that characterizes communication between two hosts.

StealthWatch categorizes the traffic into flows to profile network activity and identify nefarious behavior. After StealthWatch associates each packet or Netflow record with a StealthWatch flow, it analyzes certain statistical data and adds it to the flow data record, including the number of bytes, packets, and flag-bit combinations. StealthWatch uses this gathered statistical data to determine if a flow represents a legitimate connection or a suspicious connection, such as a possible probe.

StealthWatch identifies and logs probes as they represent the first stage in most external hacking attempts. In a process known as network mapping, an attacker probes the network to determine what types of computers are on the network, their operating systems, network listener applications (servers), IP addresses and open port numbers. Based on the data gathered from network mapping, the attacker applies an exploit routine to gain access to a vulnerable computer – and then applies an operation that accomplishes the attacker’s objectives, such as downloading sensitive data from a financial server.

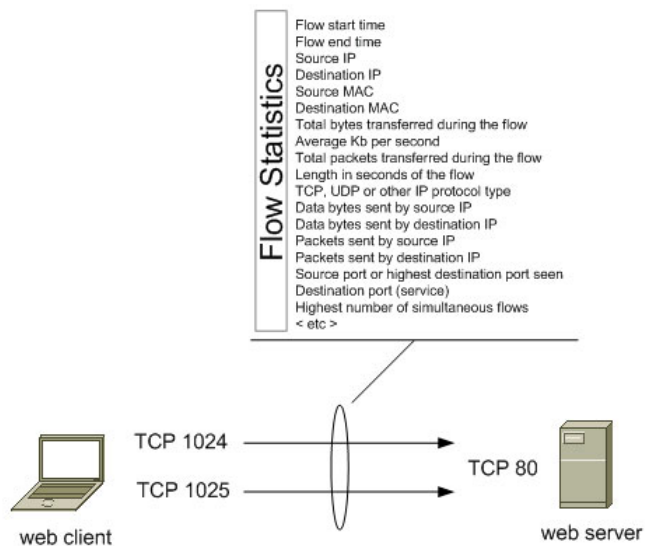


Figure 2: StealthWatch observes “flows” - the communications between host and networks.

Concern Index

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 behavior would be sufficiently concerning that calling the police would be an appropriate action. For a hacker, that action may be an IP address scan. The same is true if the stranger rattled numerous doors and windows on the same house – or a potential attacker scanned TCP or UDP ports.

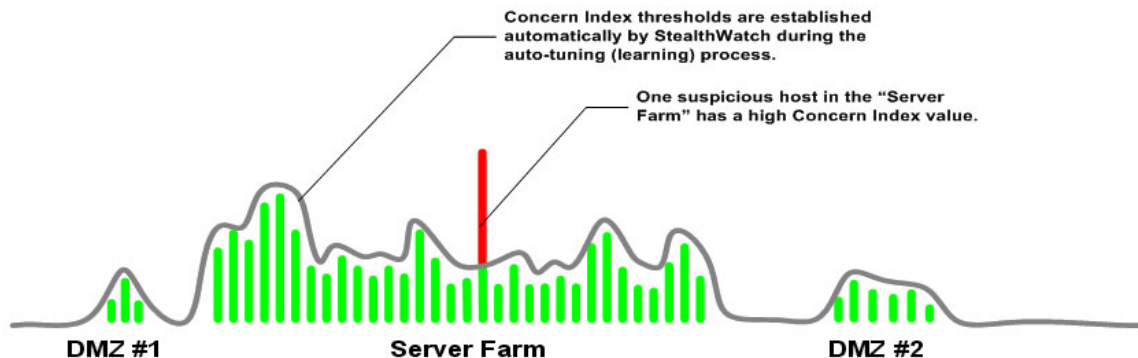


Figure 3: Network hosts are grouped into like “zones” and then profiled by the StealthWatch system until a n understanding of “normal network usage” is developed. Once established, the behavioral profile is used to find non-conforming hosts.

By continuously correlating signs of nefarious behavior, such as probes, and prioritizing threats through the Concern Index, StealthWatch improves IT's operational effectiveness by allowing the security team to focus on the real threats, not the flood of false positives. StealthWatch does not alarm on every ping, scan and probe. Instead, using a non-linear algorithm, it builds concern for suspicious hosts by correlating activities on the network, and only triggers an alarm when those hosts cause enough concern to cross a pre-determined threshold. The result is a sensitive detection system that identifies all suspicious activity without the resulting false positives associated with overly sensitive signature-based intrusion detection systems.

Behavioral Base-lining and Network Profiling

Based upon observing and analyzing the communications between hosts and networks, StealthWatch creates host and network-level profiles that describe who is talking to whom, which services are being used, and how much bandwidth is being consumed. These profiles, which are automatically and continuously refined, define the baseline of typical activity that StealthWatch utilizes to detect undocumented attacks and network misuse.

StealthWatch's behavioral base-lining dramatically simplifies the creation and refinement of security policy for administrators. StealthWatch helps easily identify unexpected network activity in addition to validating that servers, workstations and network devices are acting as expected.

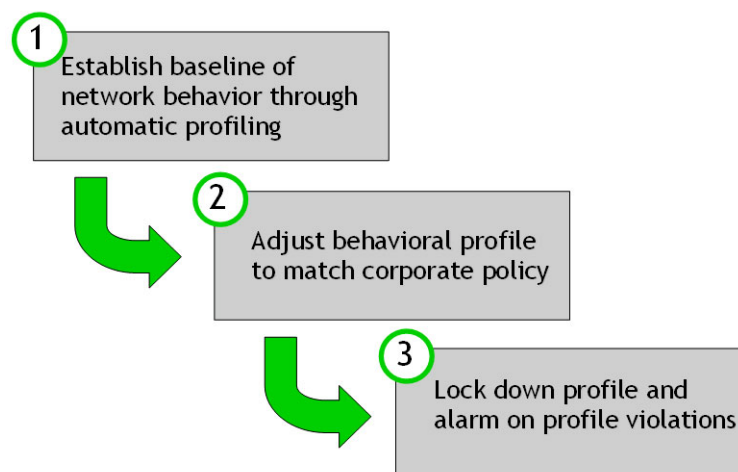


Figure 4: Behavioral profiling consists of three distinct stages: 1) Learning the behavior of the network 2) Auditing and adjusting the profile 3) Alerting on violations to the established behavior.

With StealthWatch's behavioral base-lining, you can view the services running on the network per host to determine which are appropriate and in profile. For instance, you can specify peer-to-peer file sharing, streaming media or spyware programs as inappropriate, and the right system administrator will be notified whenever an out-of-profile service is run within his area of responsibility. The continuous collection, categorization, and analysis of network activity helps establish, further tighten and enforce security policies over time.

Explicit Zone-based Security and Network Usage Policies

StealthWatch's network profiles are an easy starting point to implement zone-based security policies. Virtual Security Zones dramatically enhance your ability to create, assess and enforce security policies across the enterprise, while significantly reducing complexity in managing host-level security. In addition to greater control and manageability, zone-based security policies improve the detection of malicious activity and policy violations that pose security risks.

Security policies are enforced by Virtual Security Zones, which represent different groups of hosts with similar network and application behaviors. During deployment, IT managers conveniently classify hosts and networks into hierarchical security zones, which can be functional groupings, such as marketing, engineering or the DMZ, or zones may be physical or organizational. IT configures these groups by IP address, address range or subnet. Zones are hierarchical, making it simple to enforce a security policy across the global enterprise or down to an individual host.

Ownership of Virtual Security Zones can be assigned to different IT groups. For instance, the Information Security group may take ownership of the internal network, while Network Operations assumes control of the network devices, Systems Administration is responsible for Floor 1, and the Help Desk is responsible for Floor 2.

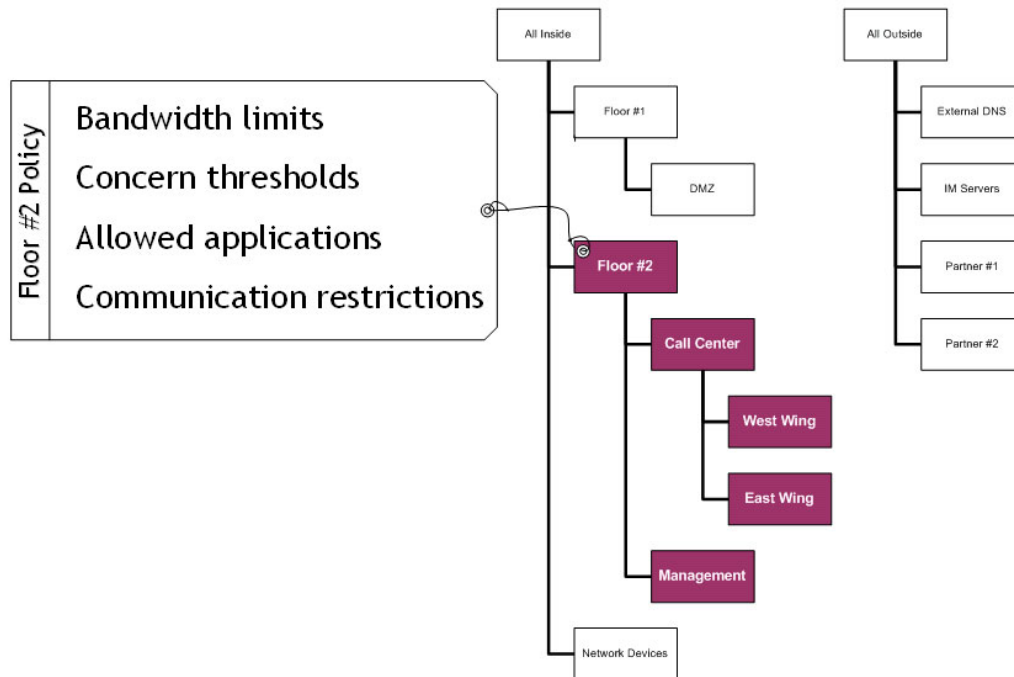


Figure 5: Virtual Security Zones enhance IT managers' ability to create, assess and enforce security policy that can be tailored by functional group, region or IP address.

Implementing StealthWatch

The best approach to network security is a defense-in-depth strategy that employs StealthWatch as a critical component of the network security infrastructure. Easily installed in minutes without disruption to your network, StealthWatch is a hardened, optimized and battle-tested appliance that provides advanced threat detection and network intelligence. Requiring minimal configuration during implementation, StealthWatch's intuitive and effective user interface allows administrators to quickly determine the likelihood of possible malicious activity. As a passive monitoring device operating in span mode or as a Cisco Netflow collector, StealthWatch introduces zero latency to your network and captures network conversations even on high-speed networks.

StealthWatch should be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, on the perimeter or in the DMZ:

- **Outside the firewall:** You may deploy StealthWatch outside the firewall to monitor the IP traffic flow and analyze who is attacking the firewall.
- **Inside the firewall:** You may deploy StealthWatch inside the firewall to monitor traffic and determine if someone has breached the firewall.
- **At key network segments:** You may want to protect sensitive segments of the enterprise networks from disgruntled or indifferent employees or hackers who have gained root access.
- **On the financial network:** You may deploy StealthWatch for protocol use management on the business network, so for instance, you can detect if a hacker is running Telnet or ftp and compromising confidential financial data.
- **At remote offices:** StealthWatch XE extends the coverage to remote offices without the need to deploy a sensor. Netflow messages from Cisco or other Netflow capable devices provide are sent to a centralized collector.

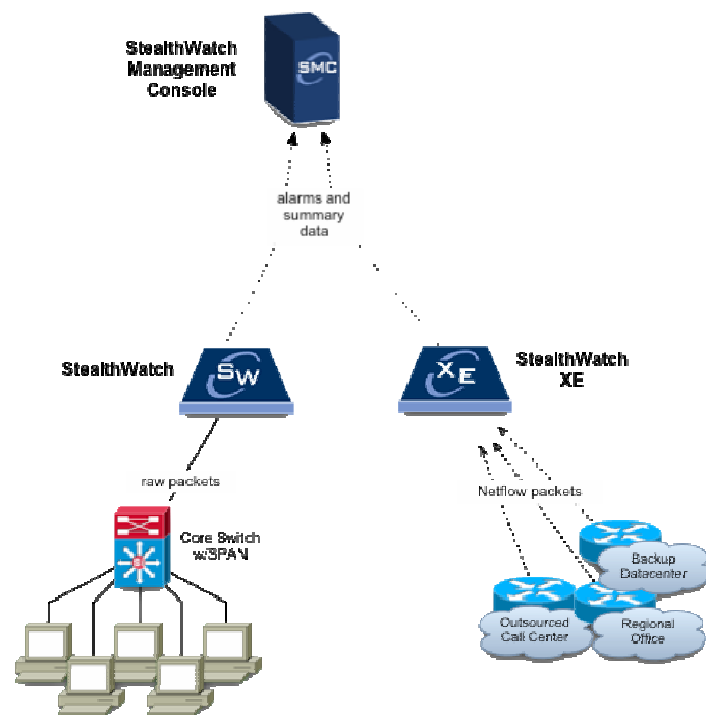


Figure 6: StealthWatch supports both Netflow collection as well as packet capture / packet sniffing.

Defense-in-Depth Architecture

Given the unique nature of the information provided by each system, a deployment strategy involving Inline IPS, Host-based IDS/IPS, and StealthWatch is recommended. Each of these three system types provides a layer of protection unique to its own technology.

Inline IPS: Well-suited for filtering well-known, well-defined attacks at the perimeter defense yet very costly and challenging to deploy in switched core network.

Inline intrusion prevention systems use signatures and rudimentary anomaly detection techniques to recognize and block “low hanging fruit” attacks such as well-known worms and older attack methodologies. IPS technologies are often deployed at perimeter locations where they act as a first line of active defense. Unfortunately IPS systems are often lacking in advanced analysis, policy, and forensics capabilities. Requiring inline deployment limits the scope of their deployment to a relatively small subset of the network.

Host-based IDS/IPS: Appropriate defense for critical hosts yet difficult to manage and deploy enterprise-wide.

Host-based systems have evolved tremendously over the last 3 years. They offer the ability to monitor process activity on the actual host. They are immune to encrypted attacks and allow for extremely detailed logging and information gathering at the OS and user level. Host-based systems are ideal for critical assets such as databases, web servers, and collaborative infrastructure. Unfortunately, their power at the host level is also the primary limiting factor in enterprise-wide deployments. For a host-based system to work, it has to be 1) installed 2) properly configured and 3) operational. All three of these conditions are difficult to maintain on end user desktops and transient hosts such as VPN clients and laptops.

Behavior-based Systems (StealthWatch): Excellent internal monitoring capabilities. Capable of detecting attacks without signatures.

Behavior-based systems close the loop on network security and advanced monitoring. Picking up where host-based systems and inline IPS leave off, StealthWatch provides insight into internal communications without impacting the operation of the network. Since StealthWatch is network-based, there is no need for an agent or any interaction with the OS or user.

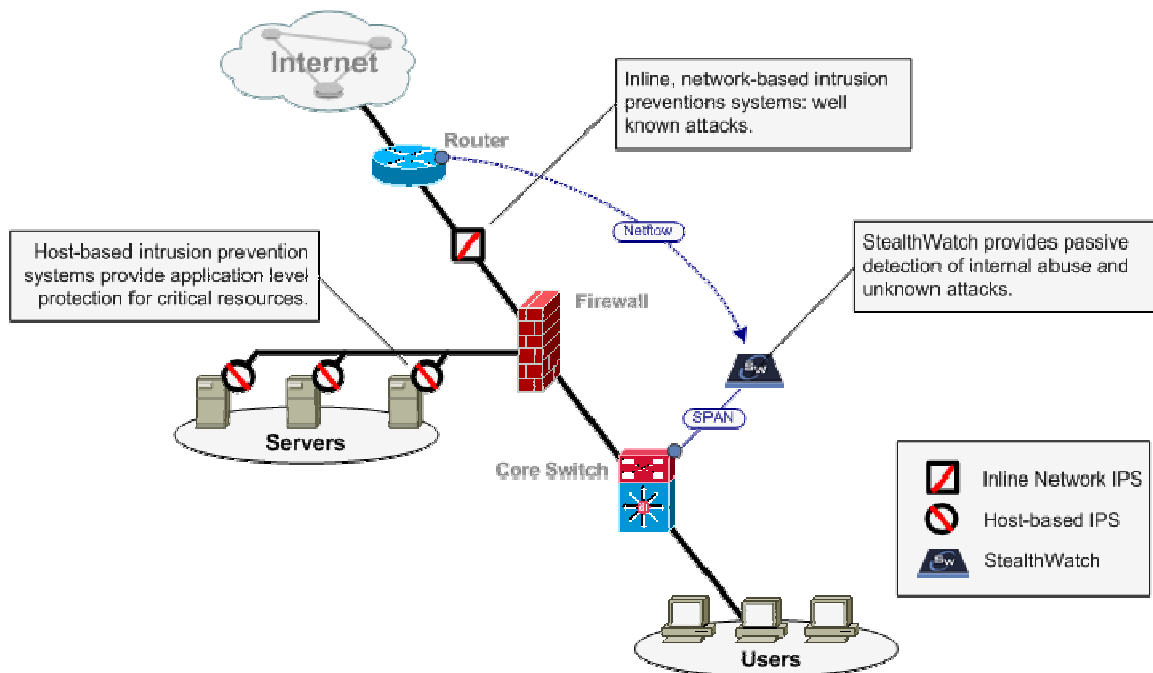


Figure 7: StealthWatch plays a central role in a multi-layered enterprise security architecture.

StealthWatch Management Console Is Your Dashboard

StealthWatch provides the intelligence and tools to bridge the information gap between network and security priorities. StealthWatch's distributed architecture greatly facilitates data collection, analysis, and reporting. The StealthWatch Management Console provides a single view of the data collected from the distributed appliances, so an administrator can easily drill down to investigate statistics from an individual appliance or gain a complete system-wide view.

The StealthWatch Management Console makes it easy for users to quickly get to the information they need by providing both task-oriented and system-oriented views of network intelligence. Each IT group can customize the StealthWatch Management Desktops to their tasks and operational requirements. The StealthWatch system provides a function-agnostic environment in which IT personnel can configure the StealthWatch Collection Network to provide the information they need to do their job more efficiently.

The StealthWatch Management Console is a separate appliance that manages up to 20

StealthWatch appliances. In addition, each StealthWatch appliance comes with its own integrated web server and lightweight web dashboard. The SSL-based web dashboard can be used to administer a single appliance or can be used should the appliance lose contact with the StealthWatch Management Console.

The StealthWatch system enables an organization to overcome significant challenges often present in distributed enterprise environments:

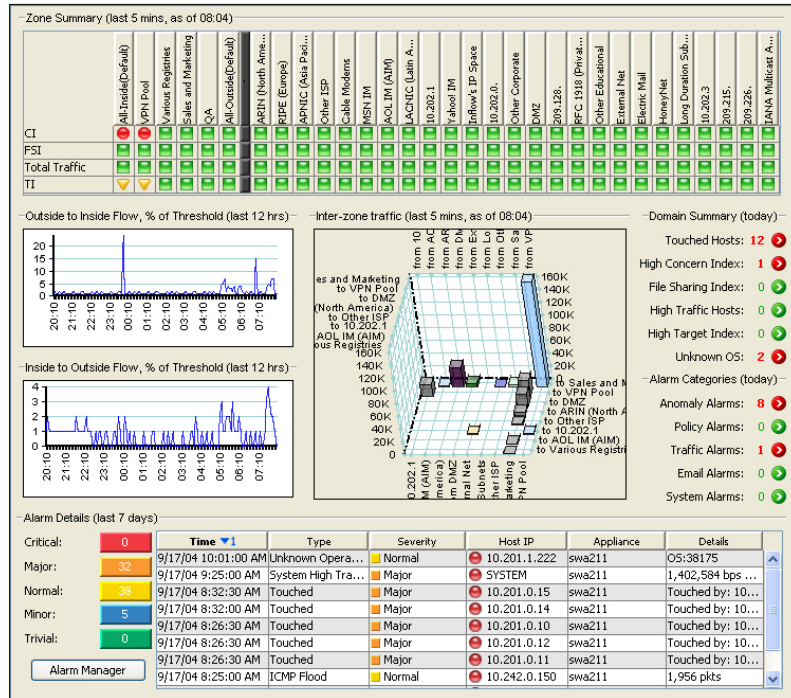


Figure 8: The StealthWatch Management Console domain status view combines custom 3D graphical rendering with useful security and network focused data points on the health of the enterprise as a whole.

Challenge: Initial configuration and deployment pains	Solution: StealthWatch is an auto-tuning appliance that can be set up in minutes
Challenge: High-speed core and links between central buildings and data centers	Solution: StealthWatch supports the demands of gigabit network environments
Challenge: Limited bandwidth across WAN links	Solution: Intelligent preprocessing and correlation of data by each appliance delivers predictable, low-bandwidth transmission between sensors and the management console.
Challenge: Encryption used between offices	Solution: Encrypted network environments have no effect on StealthWatch's threat detection capabilities
Challenge: Data overload from distributed sensors	Solution: The StealthWatch Management Console collects and correlates information from multiple sensors into a centralized network and security view

Integration with Third Party Signature-based IDS

Given the complimentary nature of the StealthWatch technology to signature-based IDS and IPS, the StealthWatch Management Console offers a low cost solution for merging alerts from signature-based system such as Snort and ISS Realsecure with StealthWatch behavior-based alarms and alerts. The StealthWatch Management Console provides a single “pane of glass” through which the security analyst can observe enterprise events.

Combining signature-based data points with behavior-based events allows for a new level of “context” which:

- Speeds root cause determination in times of crisis
- Streamlines workflow and increases the efficiency of the security analyst
- Reduces false positives by providing different views of an event
- Maximizes the return on investment for both the signature-based and behavior-based system.
- Exposes those attacks that the signature-based system missed (these are often the most important events as they represent mutated or zero-day anomalies)

The diagram below provides a logical representation of the combination of ISS, Snort and StealthWatch events. The security analyst is shown the correlated and non-correlated events.

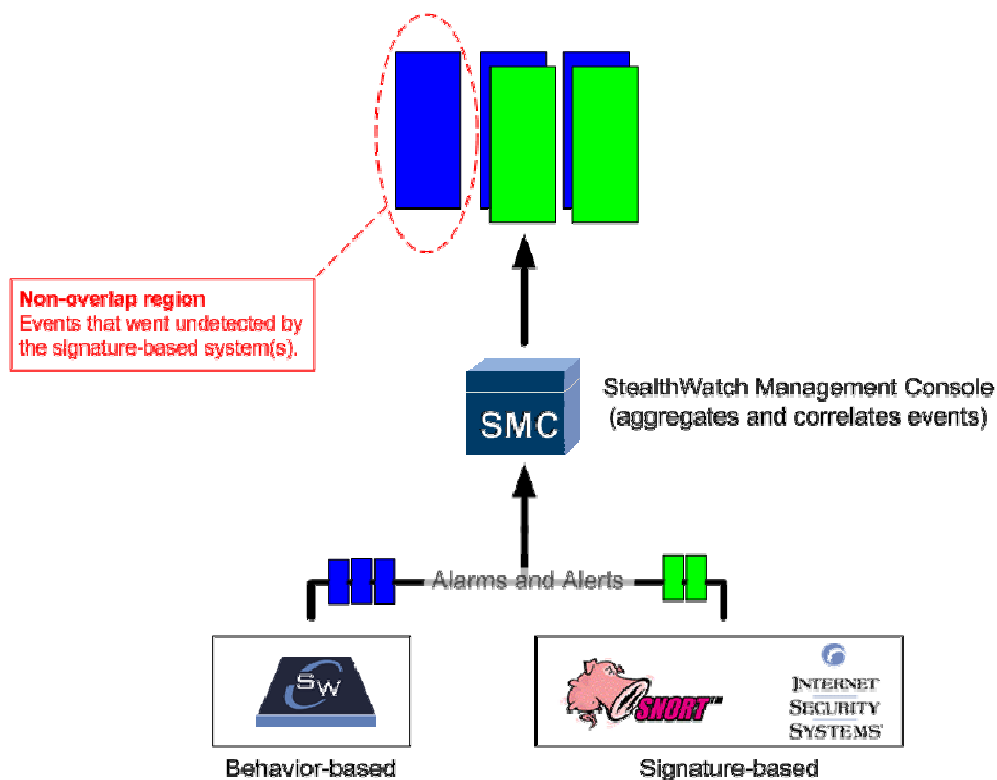


Figure 9: The StealthWatch Management Console brings together “classic” signature-based systems and the behavior-based StealthWatch technology to improve context, prioritization, and accuracy of security and network related alarms and alerts.

Quarantine Infections with Adaptable Mitigation

Lancope customers can direct the StealthWatch appliance to automatically respond to alarms generated by worms, viruses, and internal policy violations. The StealthWatch appliance is deployed as a passive network monitoring device (non-inline). Mitigation actions provided by the StealthWatch appliance leverage existing network infrastructure, such as firewalls and routers.

The StealthWatch automated mitigation system was designed with the following key concepts in mind:

Concept #1 Automate common actions taken by a StealthWatch operator

Lancope studied its existing customer base and developed a list of the most common manual actions taken users of the StealthWatch technology when an alarm is seen. From this list of manual actions, automated actions were created. The following blocking actions are supported by StealthWatch:

StealthWatch Automated Responses	
Cisco router Null0 route injection	Cisco routers dominate many modern networks. Anywhere a Cisco router exists, StealthWatch can be configured to “black hole” traffic traveling to a suspect host using a special routing technique called “Null0”. This technique is especially useful in high speed environments where ACLs create too much of a performance impact on the router.
Checkpoint Firewall-1 OPSEC Compliance	StealthWatch is OPSEC compliant. As alarms are raised, StealthWatch is capable of installing temporary firewall rules in any OPSEC compliant Checkpoint firewall.
Cisco PIX “shun” capability	If PIX is your firewall of choice, StealthWatch can be configured to use the special “shun” command to temporary block traffic traveling to or from a suspect host.

Concept #2 Provide multiple “blocking strategies”

Lancope understands the hesitation many network and security engineers have with automated responses and has gone through great lengths in research and development to create a system that is both operationally manageable and safe. Network and security personnel can choose from three blocking strategies:

StealthWatch Blocking Strategies	
No Blocking	The default action for any alarm is to block nothing when an alarm is raised.
Authorize Blocking	No automatic action is taken. A “big red button” is provided for the user which allows the StealthWatch operator to decide when a blocking action should be taken (see Figure 6 below).
Automatic Blocking	Once the StealthWatch operator is comfortable with Authorized Blocking, the next step is Automatic Blocking. In this mode, StealthWatch will take action in a completely automated fashion. No user interaction is necessary.

Concept #3 Allow for deep configuration of blocking actions

Each zone can be independently configured to respond in a different way to different alarm types. For instance, a critical server farm may be configured to as “semi-automatic” blocking (authorize mode) while a VPN DHCP scope zone would provide “automatic” blocking of suspect traffic.

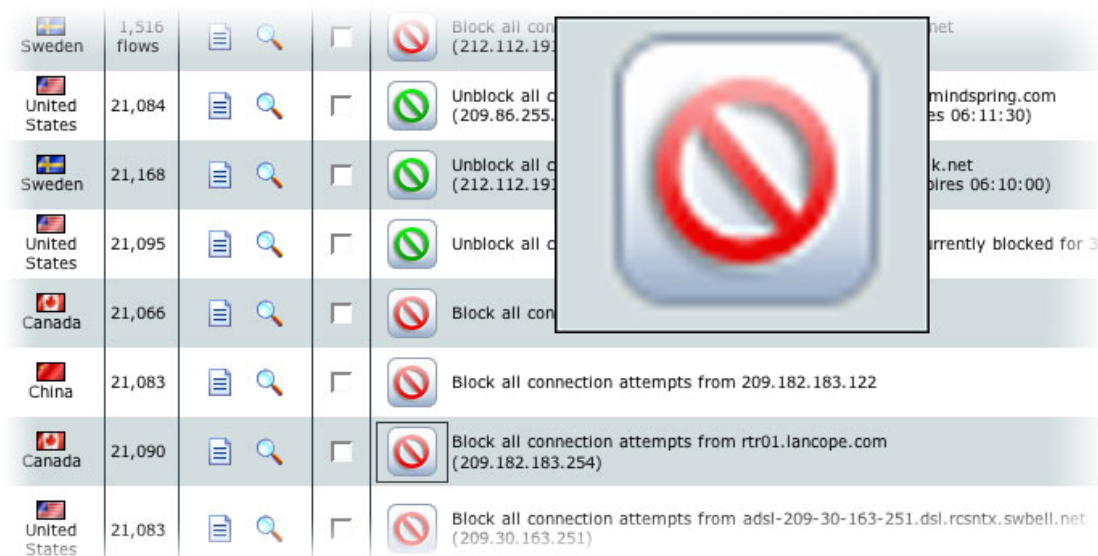


Figure 10: StealthWatch provides three unique “blocking strategies” for automated mitigation: no blocking, authorize blocking, and fully automated blocking. The screenshot above shows an enlarged “authorize blocking” button found in the StealthWatch Alarm Manager view.

Conclusion

In today's environment where threats evolve at Internet speeds, detection alone is not sufficient. StealthWatch not only protects networks against the fastest growing threats: application misuse, information theft and misconfigured devices, but also it provides real-time, continuous network intelligence that security managers, network managers and systems managers alike will find invaluable for strategic and everyday use.

StealthWatch bridges the gap between network and security operations by creating a single point of reference that facilitates collaboration among IT departments throughout the organization. For network and security teams, StealthWatch enables analysis of network behavior to better understand network usage, discover assets, identify malfunctioning devices and detect trends. StealthWatch also helps IT teams minimize the impact of network changes, avoid quality of service issues and perform firewall and capacity planning, which can

accelerate the time to migrate or expand network infrastructure. For system administrators, StealthWatch provides insightful network intelligence for detailed application usage reporting, host-level audit trails or network activity, spam detection and application failure notification. Whether performing trend analysis for a single zone or across the enterprise, StealthWatch gives the operational and management teams the necessary network

and security intelligence. Retaining the flexibility of delivering a view customized to each group's needs. As a result, StealthWatch increases your IT organization's operational effectiveness while managing the conflicting needs of more open access with increased security.

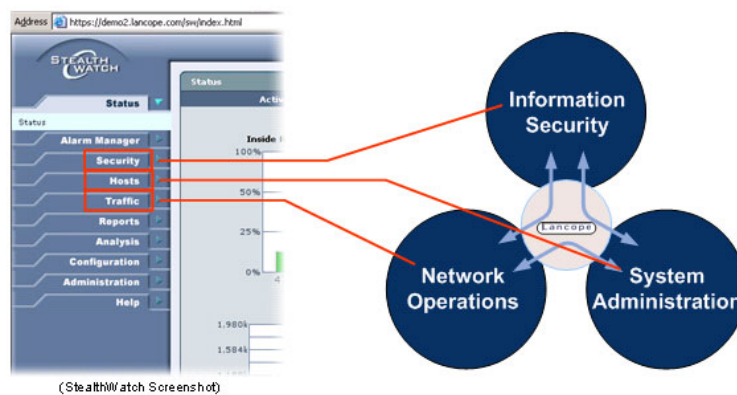


Figure 11: StealthWatch bridges the gap between network and security operations by creating a single point of reference that facilitates collaboration among IT departments throughout the organization.