



Securing Network-Attached Storage

Protecting NAS from viruses, intrusions, and blended threats

INSIDE

- > Executive Summary
- > Challenges to securing NAS
- > An effective NAS security solution
- > Conclusion

Contents

Executive summary3
Challenges to securing NAS4
Viruses, intrusions, and blended threats4
Compliance with industry regulations6
An effective NAS security solution6
Security at the firewall7
Virus protection8
Intrusion protection9
Conclusion9

> **Executive summary**

Data is one of the most valuable assets of any enterprise and it must be readily available to the authorized employees, suppliers, partners, and customers who depend on it to conduct business. As the need for data storage and access increases every year, the need for dependable, optimized, and scalable storage that can grow with the enterprise has become essential. To create these available sources of data, enterprises have been integrating network-attached storage (NAS) into their networks and consolidating data into these central servers.

The benefits of implementing NAS are shown in increased uptime and disaster recovery by fast backup and mirroring of data. Also, the easy availability of data clearly enables new business initiatives, such as Enterprise Resource Planning and Customer Retention Models. However, this centralized consolidation of data requires a shift in the approach to data security. The increase in data availability and access improves productivity but also increases vulnerability to malicious threats and attacks.

An attack on a NAS system can cause loss of intellectual property, business continuity, liability for compromised customer data, the time and money spent in recovery, and loss of customer confidence. Because of this, enterprises are finding that staying ahead of the savvy attacker is no longer an option but a necessity.

These problems add up to another problem. Inadequately protected data can also result in non-conformity to industry regulations, and this can lead to potential criminal penalties and/or loss of business integrity.

The best defense against compromised data is a full understanding of the risks involved in *not* securing data on a NAS system. With this understanding, you can create a stronger defense against attacks and create a better plan for recovery in the event of an attack. This paper describes how you can effectively mitigate the risks with intelligent security solutions to create a more efficient and cost-effective storage solution.

> Challenges to securing NAS

The consolidation of the various types of data to the NAS environment creates a new set of security concerns for the IT professional that must be carefully addressed. These new security concerns include:

- Storage servers accessed by more users are more susceptible to internal and external attack from hackers and their use of viruses, worms, Trojan horses, and other malicious code.
- Infiltration of the NAS system by malicious code can result in lost, stolen, or corrupted files at great cost and downtime to the enterprise.
- The NAS system might be used as a stepping-stone for intruders to the rest of the network, or as a launch point for attack.
- The NAS system could become the vector for malicious code. Threats can reside on NAS and can compromise the machines and data of users who access the NAS system.
- Through NAS backup, mirroring of data, and archiving, malicious code can be replicated multiple times in multiple locations. Whenever NAS data is restored from these locations, the malicious code can be reintroduced to the NAS system, thereby reinfesting the enterprise network. In essence, the threat is being replicated and reintroduced by the system itself.
- With the possibility of malicious code residing on the NAS system, in multiple backups, on mirrored sites, and on clients and servers, the time and effort involved in effectively removing the entire threat becomes an overwhelming task, causing downtime and costing time and money for data recovery.
- Because the data is at risk, the enterprise is at risk of non-compliance to industry regulations and laws. Many organizations are held legally responsible for keeping financial, medical, personal, and email data from being stolen, altered, or destroyed.

VIRUSES, INTRUSIONS, AND BLENDED THREATS

There are many types of threats that can originate from inside or outside of the enterprise to compromise access to data stored on a NAS system. Threats to network security come in the form of intrusions or attacks by people interested in information theft or destruction. These attacks can come from users of the NAS system inside or outside of the enterprise, such as from disgruntled employees, hackers, or industrial espionage.

A real challenge for network security comes in what is now commonly called a “blended threat.” These sophisticated tactics utilize multiple methods and techniques to transmit and spread an attack, maneuvering around existing defenses. These threats can come from several directions and self-replicate with surprising speed. The threat might come from the Internet, a remote site, a dial-up user, or from several other sources. It ultimately attacks internal clients or devices, creating a number of possible problem scenarios. Though there are numerous others, two high-profile examples of blended threats are Nimda, CodeRed, and Blaster.

The following figure illustrates the state of an unprotected NAS device and the network it supports. This example shows a blended threat originating outside the corporate network. The dotted line indicates the path of the threat.

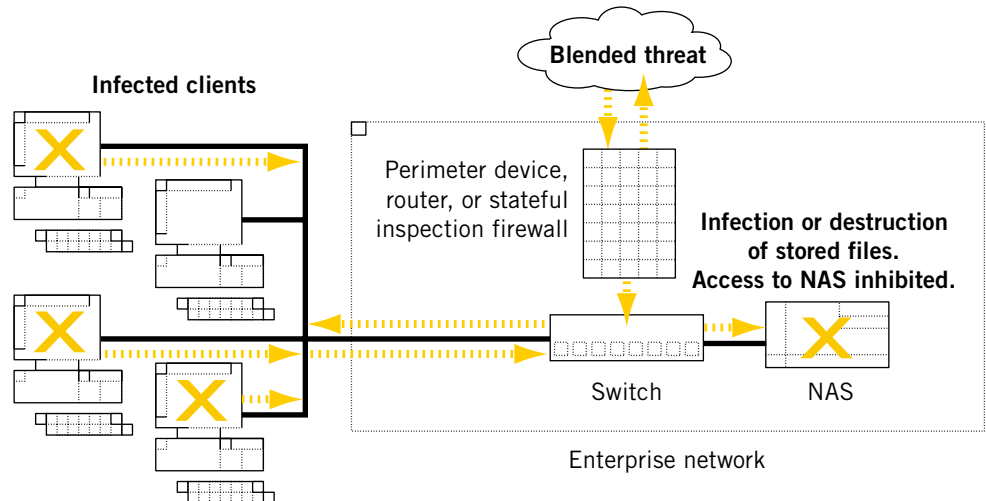


Figure 1: A blended threat compromises data integrity on an unprotected network.

Once data on a client computer is compromised, clients can infect files on network shares causing the destruction or corruption of stored data. Compromised clients can unintentionally transfer confidential data to the attacker, exposing personal, financial, or medical records to unauthorized users. Infected files on a storage device can live on in hibernation, through backups and mirroring, being replicated to multiple sites and potentially infecting other clients when they are reintroduced using disaster recovery methods. Without direct access to virus scanning, storage devices will continue to be a safe haven for these compromised files. Without proactive virus protection at the NAS level, it's difficult to eliminate data loss or compromise from a multi-terabyte storage subsystem.

In a large corporate environment, compromised clients with high available bandwidth could be utilized as "zombies," attacking the storage device in a distributed Denial of Service (DoS) attack. This attack could be directed at the NAS head, denying access to mission critical data by legitimate users. DoS attacks can interrupt or adversely impact business activities for an indefinite period of time.

A hacker can also perform network mapping, continuing to threaten valuable storage resources and potentially opening the door to future attacks on the entire network.

COMPLIANCE WITH INDUSTRY REGULATIONS

A final challenge faced by an enterprise is to comply with the myriad of standards and industry regulations imposed by Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), the Basel Accords, Securities and Exchange Commission (SEC), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and others. Ensuring that sensitive data is secured in accordance with the regulations that apply to your enterprise can help to avoid criminal penalties.

Enterprises are now being held to a higher degree of accountability for security than ever before, not only by the regulatory commissions, but also by their business partners, shareholders, and customers. And they are often challenged to provide proof that they have created the security policies and implementations necessary to satisfy requirements. Some enterprises are required to demonstrate that they can ensure the accuracy and safety of their data, securely back up and archive the data, and notify affected parties if the data has been compromised. Other requirements might be to provide full audit trails for email archiving, applications infrastructure, and data replications.

> **An effective NAS security solution**

To effectively protect NAS systems, it's critical to not only protect the NAS system, but also to protect the rest of the network infrastructure from intrusion and attack. If any parts of the network are open or vulnerable, they can be leveraged for a DoS attack or a blended threat. Since a NAS system is accessed through the network, it's just as vulnerable as the rest of the network devices to being taken off-line by these types of attacks.

The new breed of threats demands a more integrated, proactive, and layered approach to security that will protect every part of the enterprise network—from gateway, to client, to server, to storage. Despite all of the various parts of the network that need protection, the solution needn't be complicated. Symantec's NAS security solution employs multiple levels of defense and response to strengthen the security posture of the enterprise, protect against blended threats, reduce downtime, and reduce the administrative burden.

To accomplish this, Symantec's security solution uses a specialized virus protection scan engine at the NAS systems, combinations of integrated virus protection, content filtering, intrusion detection, firewall/VPN security at the client, server, and gateway, and intrusion protection at the switch. Since complex threats such as blended threats cannot be addressed by using a single product, each product addresses specific aspects of a blended threat. By using a layered approach at different points on the network, more effective protection can be achieved.

The following figure shows a network with Symantec's security solution implemented and how it responds to a blended threat.

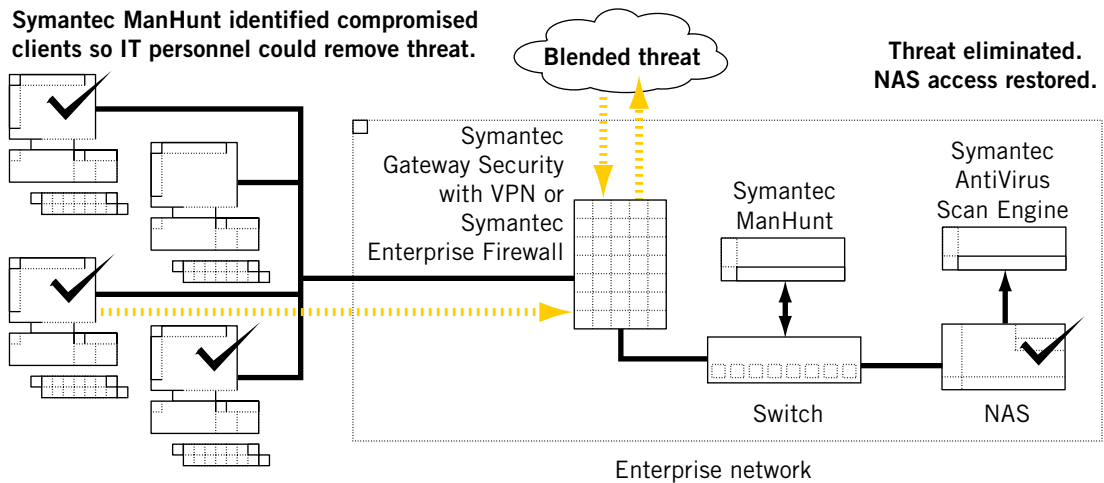


Figure 2: NAS is more secure from threats when the entire network is protected.

SECURITY AT THE FIREWALL

By placing full inspection firewalls between your clients and your storage subsystems, authentication (and encryption via VPN) can take place, ensuring data is not read or stolen while traveling across the network to and from the storage system. This can also ensure that only authorized clients can read the data without fear of an internal hacker sniffing the content of important documents from the network itself.

Starting at the firewall, the implementation of Symantec Gateway Security with VPN or Symantec Enterprise Firewall will provide a barrier to network threats by combining the best of packet filtering, stateful inspection, and application layer inspection. In essence, by implementing a Symantec Firewall solution you are creating a demilitarized zone (DMZ) or stopgap for an attack.

Symantec™ Gateway Security is an ICSA certified and IPsec-compliant firewall appliance that integrates full inspection firewall technology, protocol anomaly based intrusion prevention and intrusion detection engines, virus protection, URL-based content filtering, antispam, and IPsec-compliant VPN technology with hardware-assisted high-speed encryption.

Symantec™ Enterprise Firewall protects enterprise assets and business transactions by ensuring fast and secure connections with the Internet or between networks. As a comprehensive hybrid firewall, it enables controlled connectivity, providing protection against intrusion without slowing the flow of approved traffic. Since most threats are carried out using non-standard packets, Symantec Enterprise Firewall inspects all packets entering or leaving the NAS system to make sure they are RFC standard compliant. Some network attacks, like Nimda and CodeRed, put illegal commands or buffer lengths in packets to open up holes in the targeted application. Symantec Enterprise Firewall prevents these attacks by examining each packet to verify that it contains the correct information formatting.

Symantec Enterprise Firewall's support for a broad selection of user authentication methods such as Defender, Radius, Digital Certificates, LDAP, and NT domain authentication, offers administrators the flexibility to use existing security databases in the users' environment. EAL-4 and ICSA certification guarantees compliance with industry-leading security requirements.

VIRUS PROTECTION

Though many enterprises already have virus protection software set up at key locations in the corporate network, virus protection for firewalls, email gateways, and desktops is not enough to protect data on NAS servers. Because of the increased number of users accessing a NAS system, and the size and number of files being accessed, these systems need very fast, scalable, and dedicated virus protection scanning services to keep from creating latency or delay access to the business critical data. Only virus protection software tailored specifically for NAS can adequately protect these systems. Without this layer of protection, viruses can be stored on your NAS devices where they will be backed up into multiple locations through the mirroring and archiving processes, and reintroduced to the NAS when the infected data is restored.

Symantec AntiVirus™ Scan Engine was designed specifically for NAS devices. It scans, detects, removes and/or quarantines viruses before they can cause damage or be transferred to clients. It can easily accommodate growing traffic volumes with automatic load balancing across multiple servers while supporting multiple NAS devices. Implementing a virus protection solution along with a NAS system dramatically reduces the risk to the contents of the storage device and its users.

Data that is moving in and out of production on the NAS devices should be scanned, but it's also important to scan and clean data that is being moved into and out of *archives*. Malicious code can reside in archives and be reintroduced to the network and to users if it isn't scanned. Data should be scanned before it's archived, and old data from archives should be scanned in the event that it was stored before the implementation of the scan engine.

However, you still need to eliminate the other risks to the storage system and address more aggressive blended threats. The storage subsystem continues to be vulnerable to DoS attacks, network probing/mapping activity, and other unknown threats.

INTRUSION PROTECTION

Another element that can be used to protect the NAS system is a network-based intrusion protection system. Since NAS systems are high bandwidth devices and can span multiple segments of a network, a flexible, high performance product is required for this portion of the solution.

NSS approved Symantec ManHunt™ provides multi-gigabit intrusion detection with the ability to see traffic over multiple virtual LANs. Symantec ManHunt utilizes protocol anomaly detection to detect threats that utilize non-standard implementations of a given protocol. It can also utilize Snort signatures to search for signature-based detection of a specific threat.

Symantec ManHunt provides the ability to track a threat to a known internal source. During setup of the solution, detailed information is provided to allow it to track an intrusion to the source on an internal network. This allows the administrator to determine from which clients an attack originated providing the ability to repair the problem at the source.

> **Conclusion**

Obviously, with all of the threats that exist to the NAS system and the network in general, and with the various regulations now in effect that enforce specific security practices, enterprises must establish and follow a security policy for business continuance and compliance. The security policy should describe the use of effective security solutions that include intrusion protection, virus protection scanning, security management, and plans for disaster recovery.

The selected security products should work together to effectively protect the enterprise, the various parts of the network infrastructure, and data assets without significantly impacting system performance. An effective security policy and security product implementation will detect and prevent problems in a timely manner, as well as report situational status, risks, and problems. This security solution will ensure data security, business continuance, and industry regulatory compliance, while minimizing costly system downtime.

For more information on Symantec enterprise security solutions, go to:

<http://enterprisesecurity.symantec.com>.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF CLIENT, GATEWAY AND SERVER SECURITY SOLUTIONS FOR VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

**SYMANTEC CORPORATION
WORLD HEADQUARTERS**

**20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.**

800 441 7234

408 517 8000

www.symantec.com

**For Product Information
In the U.S., call toll-free
800 745 6054**

**Symantec has worldwide
operations in 38 countries.
For specific country
offices and contact numbers,
please visit our Web site.**