Challenges to Network Security

The rise of malicious software and its devastating effects on organizations make the headlines almost daily. As forward-thinking organizations have learned, it is not enough to protect against today's threats. To truly safeguard a network from intruders, organizations must determine whether their current solutions will protect them from tomorrow's more complicated attacks.

According to the FBI, cyber crime is now larger than the worldwide narcotic market.

According to the FBI, cyber crime is now larger than the worldwide narcotic market. Cyber pranks used to be a game to an early group of hackers whose goal was to gain notoriety. Today it has become big business with the rate of attacks doubling every year. To gain access to vital corporate data, cyber criminals are becoming more sophisticated using multi-layered attacks to overwhelm network systems and gain access to information. In many cases, victims don't even realize that their data has been compromised until long after the crime.

Another challenge to network security is the mobile workforce. Maintaining a wireless network and collaborating with outside mobile workers, partners and vendors can increase a company's risk. Yet such collaboration is often critical to a company's ability to respond to market pressures and maintain a competitive advantage. Allowing suppliers, consultants, outsourced resources and remote workers to access the network can put a company's network at the mercy of hackers.

Today's security threats are increasingly capitalizing on the security glitches in these Web applications.

While the earliest versions of malware took advantage of security glitches in the Windows operating system, the proliferation of Web technologies has provided a new window of opportunity for network threats. Today's security threats are increasingly capitalizing on the security glitches in these Web applications. Easy access to netcentric applications lets employees exchange information that may contain malware, making it nearly impossible to secure the endpoints of a network. Furthermore, a frightening number of global websites are infected by malware or are injected with false links to malicious servers. These types of "drive-by" infections are increasing rapidly.

Organizations are challenged by current network security systems that don't meet today's threats.

Finally, organizations are challenged by current network security systems that do not meet today's threats. For example, a single point of entry to the Internet can no longer be classified as secure since any port or protocol can be used to inject malware into the network and circumvent firewall technology.

[1] U.S. Government Accountability Office, Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats, June 2007.

It only takes one infected computer to launch a massive attack on a corporate network. For companies without adequate network security, the question is not if the network will come under attack, but when the attack will occur.

It only takes one infected computer to launch a massive attack on a corporate network.

Shortcomings in Current Network Security Solutions

In light of the increase in malware, many current security solutions are inadequate for today's more sophisticated threats. Here is a list of shortcomings that reduce a network's ability to eliminate malware outbreaks and limit an organization's productivity and efficiency:

In light of the increase in malware, many current security networks are inadequate for today's more sophisticated threats.

Increased latency

Many companies today employ a proxy server as one means of protecting the network. With the proxy server, any data stream entering the LAN is intercepted and scanned before it is passed on to the destination machine. But because the proxy server needs to gather the entire stream before it can be scanned, the data is not passed on to the recipient until the entire stream has been scanned and declared virus-free.

Reduced availability

There are many new tools and services available on the Internet that can improve the operational efficiency of a business. However, due to the security concerns inherent in these tools, many organizations limit their availability or simply disallow them entirely. For example, by using firewall technology, a website or URL can be completely blocked with no alternative to separate the safe portions of a site from the unsafe portions that may contain malware.

Lowered detection capabilities

Intrusion prevention systems and firewall technology can do an adequate job of protecting the network, yet they lack the critical ability to keep up with new forms of malware. With new threats arising every day, organizations must deploy technology that will protect against these vulnerabilities. For example, if a "day zero" threat has no known signature, current security solutions don't recognize it, which puts the network at risk. Just as important as recognizing a "day zero" malware is the ability to provide detailed information about it so IT professionals can fully understand the new threat and protect against it.

Limited protocol protection

Security threats come in many forms and several protocols are utilized for spreading and infection purposes, yet current security solutions leave clear and distinct holes in the perimeter of an organization's network. Many network security solutions support only Internet protocols like HTTP, SMTP, POP3, FTP and IMAP significant amount of malware is spread via CIFS, SMB (Windows traffic) and RPC ports. They protect only against outside traffic coming in rather than inside traffic infecting other machines within the network.

Many network security solutions support only Internet protocols like HTTP, SMTP, POP3, FTP and IMAP significant amount of malware is spread via CIFS, SMB (Windows traffic) and RPC ports.

As network security solutions have evolved to meet new challenges, it has become obvious that they have inherited several weaknesses that limit an organization's ability to fully protect against new and emerging threats coming from a variety of external and internal sources. To overcome these challenges to network security, organizations need a next-generation solution that scans and protects in real time without adding latency.

With NNP SandBox technology, the complexity, speed and infrastructure needed to analyze files have been dramatically reduced, providing a quick return on investment.

SOLUTION

Norman Network Protection

Proactive, Real-time Defense for the Entire Network

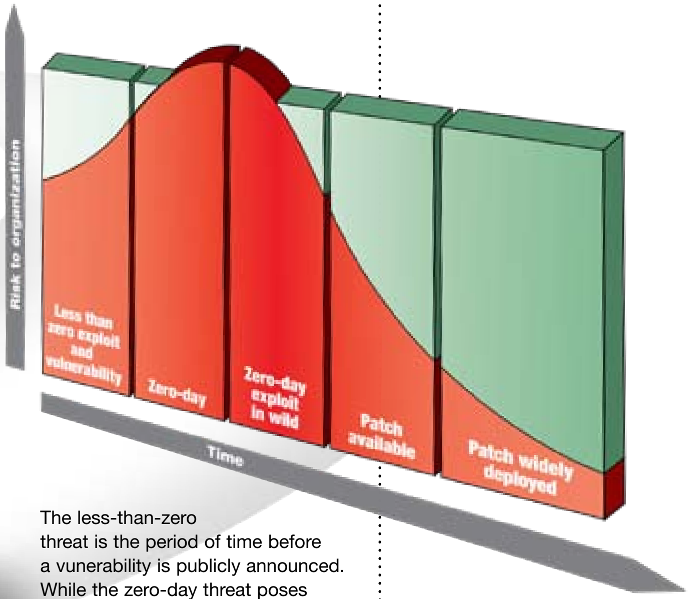
Organizations looking to implement a proactive network security solution that meets their current and future needs can now turn to Norman. Norman Network Protection (NNP) utilizes leading malware detection and analysis technology to provide a realtime protection solution. Multiple protocols are scanned to stop malicious code, keeping the network clean and allowing safe traffic to pass through quickly and efficiently.

Multiple protocols are scanned to stop malicious code, keeping the network clean and allowing safe traffic to pass through quickly and efficiently.

NNP combines signature-based security with innovative technology to proactively stop new and existing malware and provides the following advantages over traditional network security products:

Protects against "day zero" threats with SandBox™ technology

Ensuring protection against "day zero" threats, NNP uses Norman's SandBox technology, which stops new and undiscovered malicious code even before the detection signature has been distributed. It analyzes what the code would do if it were allowed to run on a real machine, all from the safe confines of a virtual environment. It emulates the computer, hard drive, memory, operating system, network and even the Internet to determine how the code will adversely affect a organization. If the SandBox regards the code as malicious, the program is stopped - effectively preventing the spread of the malware.



The less-than-zero threat is the period of time before a vunerability is publicly announced. While the zero-day threat poses a servere level of risk, the less-than-zero threat can pose a serious danger as well.

In addition to stopping malware in its tracks, SandBox technology accelerates the analysis of threats to save time and costs. Without NNP, analyzing malware can be a cumbersome and time-consuming task, involving multiple applications for code analysis as well as a network of computers. With NNP SandBox technology, the complexity, speed and infrastructure needed to analyze files have been dramatically reduced, providing a quick return on investment. What used to take days and even weeks, can now be done in seconds with Norman's SandBox technology.

Isolates and analyzes threats for increased Internet availability

Traditionally, firewall technology blocks entire IP's that are deemed risky to the organization. NNP addresses this by identifying and isolating only the URL's that are malicious. As an added measure, NNP implements a "clean" cache so when content changes, this is reanalyzed.

Eliminates latency for rapid operations

In addition to protecting against new threats while allowing undisturbed Internet access, a key component of NNP is its ability to overcome the latency effect created by traditional proxy server approaches. Rather than inspecting packets of data and holding onto them before allowing them to pass through the network, NNP scans for malware on the fly and forwards the data immediately to the receiver. This eliminates any latency effect and allows the organization to operate with rapid efficiency.

> Rather than inspecting packets of data and holding onto them before allowing them to pass through the network, NNP scans for malware on the fly and forwards the data immediately to the receiver.

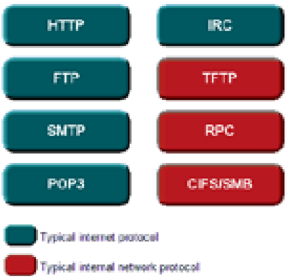
Provides complete transparency for easy deployment and interoperability

Despite this powerful and innovative malware-scanning technology, NNP is easy to implement. NNP is independent of network topology and other network units, meaning that it is effectively transparent to all other entities in the network, allowing them to operate efficiently without interruption from NNP. This is a critical advantage over proxy server solutions where significant maintenance and configuration are required for the solution to run.

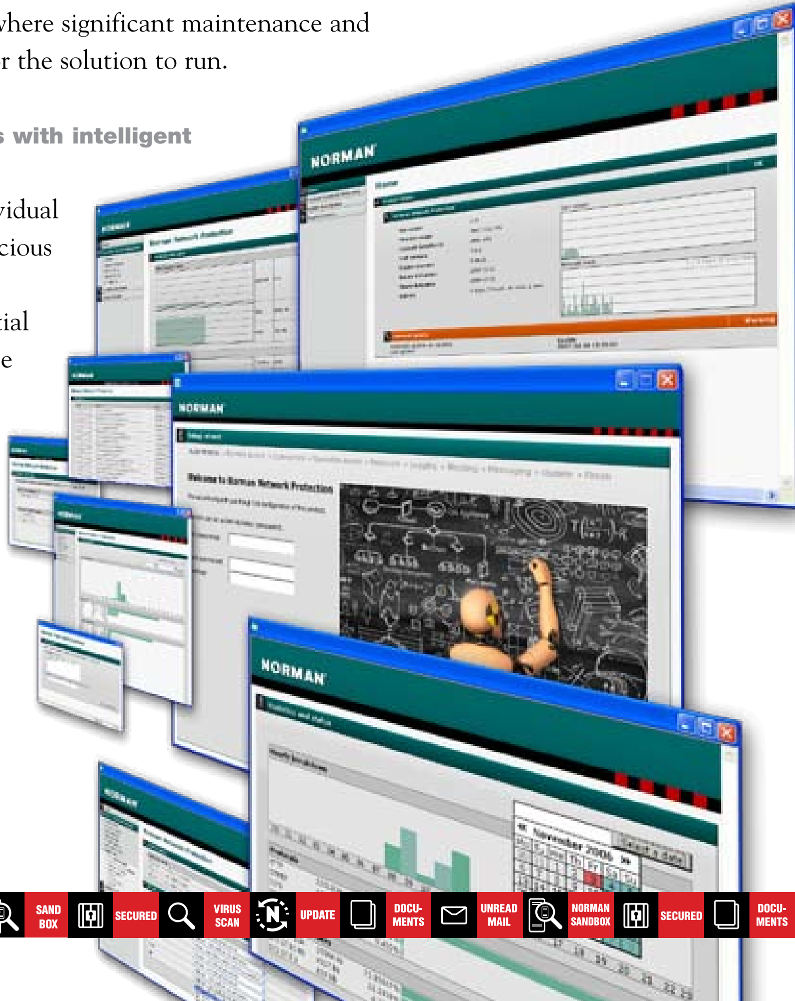
Instantly identifies threats with intelligent malware scanning

Rather than inspecting individual packets, NNP scans for malicious code on the fly, intelligently identifying the threat potential in a particular pattern or type of network traffic.

The number of supported network protocols is unique, including FTP, HTTP, SMTP, POP3, RPC, TFTP, IRC and CIFS/SMB.



The number of supported network protocols is unique, FTP, HTTP, SMTP, POP3, RPC, TFTP, IRC and CIFS/SMB.



Real World Applications of NNP

NNP provides proactive network protection in all environments from the SMB's to global enterprises. Regardless of the network size, any situation where malware is introduced to a network, threats are addressed and eliminated by NNP.

NNP provides proactive network protection in all environments from the SMB's to global enterprises

Public access network protection

There are many organizations, such as libraries, airports, cafes, and hotels that offer public access to their network to guests and customers. Such public access, however, can open the organization to malware.

In the hospitality industry for example, an infected guest computer could spread malware through a hotel's access point. From the outside, it looks like the hotel itself is spreading the malware. Seeing this, the ISP shuts down the hotel's access to the Internet, effectively blocking access for all guests. The hotel is now blacklisted by the ISPs.

To resolve this problem, airports, hotels and other organizations offering public access can install NNP at the network perimeter. NNP stops malware before it leaves the site. Only malicious content is blocked, allowing all users to access clean content and preventing the site from being blacklisted by ISPs.

Drive-by infection prevention

While public access protection is vital to organizations that serve the public, drive-by infections are a real-world threat to any organization that allows access to the Internet. In the drive-by infection situation, an employee visiting a legitimate, yet contaminated, website can pick up an infection from a portion of that site. The malicious code from a newly infected computer logs onto other sites to pick up additional malware. With no network security solution in place, the infected computer passes the malware to other computers on the network. Such widespread infection can be devastating to a organization.

In a drive by infection situation, an employee visiting a legitimate, yet contaminated, website can pick up an infection from a portion of that site.

Enterprise outbreak prevention

The size and complexity of an enterprise often makes proactive network protection difficult. NNP solves the problem by providing the scalability necessary to secure large networks, protecting all network segments and stopping malware before it spreads between segments in an enterprise's operation.

Imagine a typical enterprise environment with 500 branch offices and a centralized IT operation. Each user at a branch has administrative rights to his or her computer which allows extensive rights to file and print sharing. If one computer in a branch office gets infected, the “day zero” malware spreads through file sharing protocols (CIFS and SMB), infecting the entire centralized network.

Because many of these production networks now have Internet access, they are exposed to threats that can literally stop production.

In addition, many enterprises include manufacturing facilities that are integrated with enterprise resource planning (ERP) systems. Because many of these production networks now have Internet access, they are exposed to threats that can literally stop production. In cases such as these, a single attack could result in significant revenue loss.

To prevent such wide-scale enterprise outbreaks, NNP devices are placed at critical sites including branch offices, IT operations and production facilities. By placing NNP devices on gateways, the enterprise stops malware before it can damage the network.

Arla implemented NNP as an enterprise outbreak prevention solution.

A case in point is Arla Foods, a company dependent on its production operations. Arla implemented NNP as an enterprise outbreak prevention solution. With production connected to the company’s network, NNP ensures that traffic between the independent production networks and the administration network (where the ERP system is in control) is scanned and protected. As a result, NNP makes it possible to integrate production and administrative networks without the fear of infections, providing Arla with significant time and cost savings.

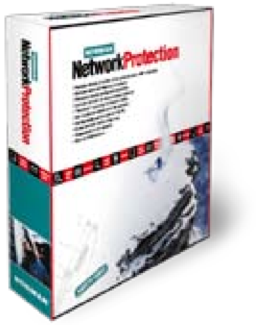
”What was especially interesting for Arla Foods was that the system could be implemented without requiring major changes to the existing equipment.”

Jens Roed Andersen,
Chief Information Security Officer at Arla

NNP protect organizations from outside threats, but it also protects a organization from itself

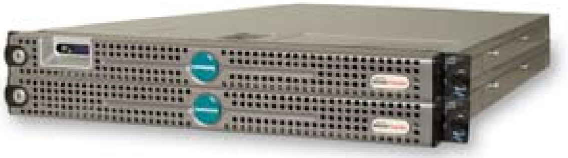
While these cases clearly illustrate the benefits of NNP, they are not the only ways that NNP can be implemented. Many types of environments and businesses can benefit from the network security provided by NNP. And not only does NNP protect organizations from outside threats, but it also protects a company from itself. For example, malware detected on a computer in the accounting department is isolated from the rest of the organization, allowing business operations to continue as normal.

By providing real-time protection for public access networks, drive-by infections and large enterprise environments, NNP effectively eliminates the threat of network attacks and allows organizations to focus on their core business strengths.



CONCLUSION

With new threats arising daily and cyber attacks on corporate networks becoming more costly, today's organizations must address challenges to network security in order to remain competitive. Traditional proxy servers and firewall network security solutions are insufficient to protect an organization from new and evolving malware that can enter the network from a growing number of mobile and external sources. Organization that want to gain a competitive advantage must be able to access the tools and services that are used to improve operations without security risks.



Norman Network Protection meets and exceeds the shortcomings of traditional network security products with a proactive solution that eliminates the risk of cyber attacks by defending against known and undiscovered threats.

Norman Network Protection meets and exceeds the shortcomings of traditional network security products with a proactive solution that eliminates the risk of cyber attacks by defending against known and undiscovered threats. This allows organizations to continue high-performance network operations with total transparency and without any regard to potential malicious software infections. In addition, and perhaps more important, managers and IT professionals can conduct business as usual with complete peace of mind.

http://www.norman.com.

About Norman

Norman ASA, founded in Norway in 1984, is a world leader and pioneer in proactive security solutions and forensics tools for malware analysis. Norman offers analyzers, network security and endpoint protection solutions for organizations' and end-users' security needs. Norman solutions are available through Norman's subsidiaries and partners around the world.

For more information about Norman Network Protection, please visit http://www.norman.com/nnp

NORMAN®

Headquarter: Norman ASA P.O. Box 43 N-1324 Lysaker, Norway
Visiting address: Strandveien 37, Lysaker • Tel: +47-67-10-97-00 • Fax: +47-67-58-99-40 • norman@norman.com