

Rethinking Endpoint Security

Mitchell Ashley, CTO, StillSecure

1/21/05

The next worm to attack your network could come from the most trusted employee in your organization. It might sound strange, but the likelihood of being attacked by end users connected inside the network has increased dramatically. Many of the worm and Trojan attacks today are launched by clicking an innocent looking link in an email or by unknowingly visiting a web site intent on delivering a worm, Trojan or spyware onto an unsuspecting user's computer. It could happen to almost anyone—if proper security measures are not in place to protect the network from these compromised endpoints.

Everyone is familiar with attacks that attempt to gain access and compromise our defenses from outside the network perimeter. Not long ago protecting the perimeter was considered sufficient to meet the security best-practice standards prevailing at that time. Today, our networks are much more porous due to the variety of access methods, such WiFi, full VPN, SSL VPN, and dialup, and the variety of devices that access the network – a growing percentage of which are not secured by the organization's IT department. Unless tightly controlled, devices with peer-to-peer messaging, music, and file-sharing programs installed expose the internal network to outside "virtual" networks whose traffic passes unabated through network defenses. P2P networks can also be the entry point for additional attacks, and the exit point for corporate data being illegally transferred to locations outside the firewall.

The 2005 StillSecure IT Security Adoption Survey shows that anti-virus, firewall, and VPN solutions have already been widely adopted (96 percent, 94 percent, and 78 percent, respectively.) At the same time, most organizations have been negatively impacted in some way by Trojans, viruses, and spyware. Many have suffered financial losses when IT and security staff are redirected to respond to these incidents, and in some cases business downtime has resulted. An Aberdeen Group study shows that revenue losses attributed to Internet-based business disruptions now average \$2 million per incident, with almost one business-disruption incident per organization per year. Mid-sized businesses (revenues of \$500M) experience a loss rate of over \$335,000 per incident. Even small businesses (\$10M in revenue) feel this impact with losses averaging \$6,700 per incident. To combat this, the IT Security Adoption Survey respondents indicated they are implementing newer

technologies such as intrusion detection/prevention, vulnerability management, and endpoint compliance. 67% of the respondents to are implementing endpoint compliance solutions, the most recent and fastest growing addition to the list of new technologies.

Many of the Internet-based business disruptions result from attacks that originate inside the network. It is rapidly becoming a common experience for organizations to have been exploited by attacks launched from inside the network as a result of visitors (contractors, vendors, or business partners), VPN users, dialup users, wireless users, or employee desktop computers. In some cases the attack's point of entry remains unexplained because there is no record of the attack at traditional perimeter points, and there are so many other possible entry points. Frequently these entry points don't have or are not set up to maintain adequate audit trails to aide in tracking down incidents. In other cases, the staff is too busy or isn't trained in the necessary forensic techniques to trace down the actual source and type of attack.

Leveraging the endpoint

Since mid-2003 a fundamental shift has occurred in the way attackers attempt to compromise our networks. MS Blaster was more than just another worm. Its pervasive spread to desktops and laptops highlighted the exposure that endpoint devices pose to the network whether they are inside or outside the firewall. Many of the worms, trojans, and spyware that have been introduced into the wild attest to this shift in the nature of attacks. Network and security administrators are grappling with exploits such as Download.Ject that take advantage of browser deficiencies. At the same time they are deluged by the many variants of MyDoom, Beagle, Sasser, Netsky, Sober, Sobig, Phatbot, Witty, Blaster, and many others.

The 2004 Online Safety Study survey (www.staysafeonline.com) conducted by AOL and the National Cyber Security Alliance (NCSA) showed that end users perception of their computer security doesn't match reality. 85% of the respondents believed they had anti-virus installed yet detailed scanning of their computers revealed that 67 percent either hadn't updated their virus signatures in the past week or had no anti-virus protection at all. The scan also found an average of 93 spyware/adware components on infected computers. The dirty little secret is that not all endpoint devices are secure, and attackers are increasingly taking advantage of them.

This shift toward exploiting the endpoint is somewhat of a natural progression given the two basic methods of breaking into a computer. The first method exploits operating system or application software that contains vulnerabilities or that is improperly configured and opens up the device to compromise. Many of the commonly deployed security defense systems are directed at preventing such attacks by blocking malicious traffic or reporting known vulnerabilities that need to be repaired.

The second attack approach leverages end-user behavior. Many common—and even desired—end-user activities can be exploited to facilitate an attack. For example, attacks can be facilitated by the end user clicking a link on a web page or within an email that

appears to be legitimate. Successful attacks of this type bypass traditional defenses such as firewalls and IDS/IPS solutions and give direct, immediate access to core network devices and other endpoints. By exploiting end users and their computers, attackers have an almost unlimited number of unsecured corporate and home computers through which to gain access to business and government networks.

How do the new worms and trojans leverage the end user as part of the attack? In the case of MyDoom, malicious payload is delivered when end users open a zip file. Sober.D relies on end users clicking a link to download a security patch contained in a would-be security email bulletin, thereby delivering the worm directly to end users' devices. In January 2005, a new exploit presents emails masquerading as CNN news subscriptions by presenting the latest CNN website headlines (pulled from CNN website content as the worm spreads) in the subject of the message. At first blush this might appear to be an end user training problem. Certainly, end user security training is a necessary element of any security plan but more than good training and safe computing practices are needed.

Mobile and remote users pose as great of a threat. Such users who unknowingly have compromised devices can VPN into the network, dial in, or connect their laptops to the LAN when returning to work and infect or re-infect the network. Visitors and contractors regularly connect to the network with their own endpoint devices and contaminate the network through attacks latent on their computers. In these situations attacks enter behind perimeter defenses and have a wide open network on which to spread. Not only does this make it easier for attacks to enter the network but frequently security administrators must respond to the same attack multiple times. Stiffening the defenses at the network perimeter doesn't necessarily decrease the likelihood of this type of attack from occurring.

Focusing on the endpoint

Until recently it was much more common for attacks directed at end users to be delivered as a virus, arriving in end users' email boxes. Since the new generation of attacks leverage vulnerabilities, web sites, peer-to-peer applications, as well as email, anti-virus software can't adequately defend against them. Certainly it's important to have anti-virus software on endpoint devices, and now it's even more critical that endpoints have the very latest virus definitions. But clearly, this isn't enough.

Is better anti-virus software needed? Are personal firewalls the solution? IT organizations are in a rush to determine what's needed beyond traditional anti-virus and personal firewall solutions. Vendors would have you believe that product upgrades, enterprise-managed versions of the product, even OS upgrades that include anti-virus and personal firewalls are the answer. But it's not just about locking down the endpoint device. Endpoint security solutions must work to protect the network from unsecured and unknown devices. End users often knowingly or unknowingly disable security applications (such as anti-virus or personal firewalls), neglect to install up-to-date security patches, improperly configure security settings, install restricted software (peer-to-peer, file sharing, or instant messaging) or are subject to spyware contamination. The

reality of network security today is such that we cannot assume users can secure their own devices; administrators must protect the network from all endpoints, foreign and domestic. In short, endpoint devices must be considered suspect.

A more comprehensive, holistic approach to endpoint security is required. It's time to revisit the best practices we use to secure the network and ensure that they take into account endpoint devices. Locking down the endpoint isn't the only option to be considered. We must consider the dynamic, and in some respects, uncontrollable nature of endpoint devices and devise security programs and policies that secure the network as well as the endpoint. Many networks, such as those in universities and businesses, don't have the luxury of controlling every endpoint hardware device that connects to the network. Most environments must maintain some level openness to allow outsiders, even employees, to connect with devices beyond the organization's immediate control.

The case for endpoint compliance

A security strategy that protects the network infrastructure but left the security of endpoint devices up to their users would be pure folly. Organizations must accept that all endpoint devices connecting to the network are untrustworthy and should be considered so until their security state has been validated. It is prudent to define a clear policy for the security requirements of all endpoint devices connecting to the network and then devise mechanisms of enforcement. Our investments in identity management, such as two-factor authentication, must be matched with similar controls around the devices that connect to the network.

Rethinking endpoint security means that we must view the security of endpoint devices from a network perspective. As each endpoint device connects to the network, it is to be tested for compliance with the organization's security policy. Endpoint compliance includes both devices under the control of the organization, such as corporate desktops and laptops, as well as foreign endpoints that are not under the organization's direct control. Foreign endpoints include laptops and desktops that may be brought into the organization by visitors, contractors, or employees. Also, devices that the organization may never physically see such as employees' and contractors' home computers, and devices attaching to the network via WiFi are considered foreign. While most IT shops tend to focus on corporate-owned endpoints, both foreign endpoints and corporate-owned devices must be addressed as part of any organization's endpoint security program. In fact, foreign endpoints pose a greater risk than corporate-owned machines because their security is unknown and likely to be inadequate or non-existent.

Network endpoint compliance must be addressed from both an external and internal perspective. The external perspective entails controlling the access of devices that connect to the network remotely such as through VPN, dialup and WiFi. All external endpoints accessing the network should be tested prior to gaining full access to network resources. Non-compliant devices may only receive limited access through a quarantine policy, or may have no network access until they meet endpoint security requirements. For example, you may not want people updating their home computers through the

corporate VPN. VISA, for example, not only has internal security requirements but security standards for credit card processors. With the financial and brand integrity of so many at stake, the VISA CISP program enforces very specific security standards with their business partners.

The internal perspective pertains to controlling the access of the devices that connect directly to the internal LAN. This includes devices at a central location as well as devices at smaller or remote offices. Similar to external machines, these devices should be cordoned off into a separate quarantine network with only the access necessary to receive virus definitions, update software, or receive updates from a patch management solution.

Endpoint compliance means more than checking for the latest patches and antivirus files. Endpoint compliance requirements should include a wide range of security settings on the device. Examples of security requirements that should be considered for each endpoint include:

- OS updates, hotfixes, and critical updates
- Windows automatic update settings
- Antivirus software installation and up-to-date virus definitions
- Personal firewall and up-to-date firewall rules
- Installed software, programs, or services
- Registry entries
- Prohibited software including peer-to-peer and spyware applications
- Application security settings including macros
- Browser application, version, and security settings
- Storing local credentials, such as user IDs, passwords, and .NET credentials

An example of an endpoint compliance scenario is when the Download.Ject Microsoft Internet Explorer exploit was discovered. The recommended actions were to either disable the execution of javascript by setting the Internet security zone level to high, or require the use of a different browser. An endpoint compliance solution would test for these requirements and then grant or deny network access on a device-by-device basis based on the test results. When patches to security exploits are not available, compliance requirements may enforce other options such as security settings or work-arounds that prevent exploitable devices from entering the network.

Rolling out endpoint compliance

There are three primary considerations when assessing endpoint compliance options:

- Are you seeking protection for just corporate assets or do you also need protection from endpoints not under the control of your organization (i.e., foreign endpoints)?
- Are you willing to take on the burden of installing or downloading agents on each endpoint, or do you need an agent-less solution?
- Do you only want to enforce endpoint requirements for software patches and anti-virus, or do you want to enforce a more comprehensive set of security

requirements? Many organizations need the flexibility to create security requirements beyond those that come out-of-the-box with most solutions.

Although a number of options are available for securing internal endpoints, only a few focus on the foreign endpoint security problem. Almost all of these require the installation of an agent (similar to a personal firewall or VPN client) or are limited to SSL web-page-based applications. It's not realistic, though, to assume you'll have the resources or the level of control needed to install a client on every foreign device. Also, most organizations would prefer not taking on the administrative burden of supporting an agent regardless of whether the device is corporate owned or foreign.

A more recent development is agent-less, also called client-less, endpoint security solutions that are network-based and do not require the download or installation of any software on the endpoint device. Agent-less solutions are network-based and "connect" to the endpoint device to perform a series of compliance tests. The device is tested prior to allowing it full access to the network and then can be retested during its session on the network. Multiple policies can be applied to the device falling under that policy. Traveling laptops may have different compliance requirements than engineering workstations, or the typical desktop device. Agent-less solutions are also effective at "pre-rolling policies"; testing new compliance policies prior to their being enforced. This can provide great insight to the organizations readiness prior to an endpoint compliance policy being rolled out.

Agent-less solutions offer significant advantages over the agent-centric approach. Since no software runs on the endpoint, agent-less options do not suffer the deployment problems or the increased administration that arises when software has to be installed and supported on each device. Software compatibility issues, upgrade deployment and support issues, and increased helpdesk calls are all avoided. Clearly, the agent-less approach offers a compelling answer to the problem of foreign endpoints as well.

To truly ensure that endpoints are secure, a solution should meet the following three requirements:

1) Deliver a full suite of testing capabilities. Most endpoint security solutions check endpoints for the latest software patches and for the presence of up-to-date anti-virus signatures, but as discussed in the previous section, much more is required to truly ensure endpoints are secure. Endpoint compliance means testing for a broader range of security and configuration compliance requirements.

In addition to testing for patch levels and anti-virus, authorized and unauthorized software should be examined. Your policy may be to restrict applications such as file sharing and peer-to-peer software, or limit instant message software to a particular provider. Software and security settings on the device should be tested, such as automatic software update frequency, patch installation, browser version and security zone settings, and executing macros.

These tests may be applied differently depending on the user or device that is connecting to the network. The laptops of visitors may be required to have all the current patch levels and one of a number of up-to-date anti-virus software programs where as a traveling corporate laptop user must also have the authorized company personal firewall, desktop management software (such as SMS), and very specific browser and application macro security settings.

2) Verify that harmful software does not reside on the device. Endpoint security solutions should proactively check endpoint devices to determine if they have been compromised by any worms, Trojans or spyware – which ultimately is what endpoint security is all about.

While it may not be practical to wait for full virus and spyware scans to run before an endpoint device is connected to the network, testing to make sure the device has not already been compromised by one of the most agreeous and pervasive malware can greatly reduce the risk of infection. Testing for worms and Trojans such as Beagle, Blaster, MyDoom, Netsky, Sasser, Welchia, etc., in addition to making sure the device has the necessary security software and settings is a very effective means of protecting the network from suspect or untrusted devices.

3) Provide the ability to create custom tests. More advanced solutions have the capability to add user-created sets of endpoint tests, allowing you to check for requirements that may be unique to your organization.

A common practice is to use certificates or key entries in the device's registry to recognize validate the device is an asset owned by the organization. Additionally, MD5 tests can verify software has not been tampered with. Custom tests can also be used to collect information about the endpoint device, such as an inventory of all software installed, or could be used to start programs or services such as the patch management distribution agent. Custom tests can check for these as well as other unique compliance requirements.

Conclusion

Blaster was a wakeup call for security organizations; it was more than just another attack. The speed at which it and subsequent worms spread through networks are cause for concern. Of greater concern is the entry point of such worm and Trojan attacks. Taking a network perspective to endpoint security is a fundamental requirement if any organization is to defend itself from attacks delivered by endpoint devices.

About the author

Mitchell Ashley is CTO and VP of Customer Experience at StillSecure where he is responsible for the product strategy and development of the StillSecure suite of network security products. Mr. Ashley has more than 20 years of industry experience holding

leading positions in data networking, network security, and software product and services development. Mr. Ashley can be reached at mashley@stillsecure.com or 303-381-3830.