

Hazardous Endpoints

Protecting Your Network From Its Own Devices

Abstract

The increasing number and types of attacks launched from endpoint devices can no longer be ignored, and organizations must shift and expand their protection. While it is important to secure endpoints with up-to-date anti-virus software and personal firewalls, it is more important to protect the network from endpoints that may be compromised. Extreme Networks® SentiAnt™ AG secures the network from this threat. It protects the network by requiring that endpoints comply with security policy before they are allowed access. SentiAnt AG defends against attacks delivered by endpoint devices.



Summary

A new breed of network attack leverages the endpoint and takes advantage of ‘normal’ user behavior to execute and spread. Traditional endpoint security solutions such as personal firewalls and anti-virus software are insufficient to stop them. Endpoint security is no longer a matter of protecting the endpoint itself; it is now about protecting the entire network from the attacks that can be introduced through compromised endpoints.

Extreme Networks® Sentriant® AG helps secure the network from this threat. It protects the network by requiring that endpoints comply with security policy before they are allowed access. Sentriant AG defends against attacks delivered by endpoint devices.

Introduction: The Rise of Internally Launched Attacks

The next worm to attack your network could come from your CIO, the VP of Operations or even a member of the board. That is not to say that such an attack would be intentional, or that the individual would even be aware of what was happening. The point is that the likelihood of being attacked from inside the network has increased dramatically. Many organizations have already experienced this problem.

We are all familiar with attacks that originate from outside the network perimeter. Previously, protecting the perimeter was considered sufficient to conform to security best-practices. Today, our networks are much more porous as a result of wireless, VPN, and dialup access. Peer-to-Peer messaging and file-sharing programs connect individual desktop computers to virtual networks that pass unabated through perimeter defenses, including firewalls, Intrusion Prevention System/Intrusion Detection System (IPS/IDS) and good patching practices.

Most businesses have suffered financial losses from worms, Trojans, viruses, and spyware. An Aberdeen Group study¹ shows that revenue losses attributed to large 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. Many of these Internet-based business disruptions result from attacks that originate inside the network. It is becoming common for organizations to fall victim to internal attacks launched from visitor laptops (contractors, vendors or business partners), machines connecting through VPN or modems, wireless devices or employee desktop computers. These are referred to as endpoints, and unfortunately, endpoint devices are not really secure.

Attackers are increasingly taking advantage of these unsecured endpoints. 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.

Attacks Leveraging User Behavior

This shift toward exploiting the endpoint is a natural progression in the evolution of attack strategy. Historically, attackers have sought to exploit operating system or application software that contains vulnerabilities or is improperly configured. 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. More recently attacks are increasingly leveraging end-user behavior. Many common, and even desired, end-user activities can be exploited to facilitate an attack. For example, attacks can be launched when the end user clicks 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 leveraging end users, attackers have an almost unlimited number of unsecured corporate and home computers by 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 what seems to be a security email bulletin, thereby delivering the worm directly to end users’ devices.

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 spread contamination through attacks residing 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. Beefing up the defenses at the network perimeter does not necessarily decrease the likelihood of this type of attack from occurring.

1. Aberdeen Group, White Paper: “Open Source Databases: All Dressed Up and So Many Places To Go” March 2004, pp 7-10.

Anti-Virus Software and Firewalls are Not Enough

Until recently, it was common for attacks directed at end users to be delivered as a virus within an email. The new generation of attacks leverage vulnerabilities, web sites and Peer-to-Peer applications as well. Even devices with up-to-date anti-virus software are not protected from these attacks.

Is better anti-virus software needed? Are personal firewalls the solution? IT organizations are in a rush to determine what's required to defend against this new breed of attacks. Vendors would have you believe that product upgrades, enterprise-managed versions of their product, even OS upgrades that include anti-virus software and personal firewalls are the answer. It is not about locking down the endpoint device; it is about protecting the network. End users often knowingly or unknowingly disable security applications (such as anti-virus software 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. All of these factors have historically been beyond the control of IT administrators.

Bottom line: we cannot assume users can secure their own devices; administrators must protect the network from all endpoints, managed and unmanaged. Endpoint devices must be considered suspect and administrators must regain control over them.

Sentriant AG Protects the Network by Requiring that Endpoints Comply with Security Policy

Sentriant AG protects your networks by verifying that local or remote endpoints such as desktops, laptops or servers do not have dangerous configurations or applications, and that they are free of malicious code such as worms, viruses and spyware. Sentriant AG prevents unsafe endpoints from connecting to the network and launching malicious code.

How does Sentriant AG protect the network? By allowing you to define your security policy for endpoints and then enforcing that policy by testing each endpoint as it logs onto the network. For example, your security policy for remote endpoints connecting through VPN may specify that:

- A personal firewall must be present
- Anti-virus software must be running and the virus definitions must be up to date
- All Windows service packs and hotfixes must be installed
- Peer-to-Peer networking software is prohibited
- The endpoint must be free of all worms, Trojans and spyware

Endpoints that fail any of these tests are subjected to the enforcement actions specified in the defined policy. For example, Sentriant AG can completely deny access to the

network, it can provide access for a grace period or it can quarantine the endpoint limiting access to, for example, the Internet. With this limited, quarantined access, the endpoint is prohibited from damaging the network, yet it is able to download the patches, updates and such, needed to bring the device into compliance with the security policy. Sentriant AG presents non-compliant end users with detailed instructions on how to bring their machines into compliance.

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. Many security-conscious organizations immediately incorporated these recommendations into their IT security policy. In this case, Sentriant AG would test each endpoint to make sure these changes had been implemented, and then grant or deny network access on a device-by-device basis based on the test results.

Test Categories

Sentriant AG goes well beyond simply checking for the latest patches and anti-virus files. It tests for a wide range of security settings on the device. Sentriant AG ships with more than 80 individual tests in the following categories:

- OS updates, hot fixes and critical updates
- Windows automatic update settings
- Anti-virus 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

Sentriant AG also allows you to create custom tests through its open Application Programming Interface (API) to meet organization-specific testing requirements.

In addition to these out-of-box test categories, Sentriant AG administrators combine selected tests into access policies. Devices are then assigned to access policies, and the tests contained with the policy are applied to the assigned devices as they log on. For example, access policies can be created specifically for managed endpoints located at satellite branch offices, for endpoints that run a specific operating system, for wireless endpoints, for example. Sentriant AG is extremely flexible and adaptive, allowing you to maintain unlimited number of access policies. It accommodates the compliance process that makes the most sense for your organization.

Implementing Sentriant AG

Sentriant AG is a stand-alone solution; no other modules are required. It is infrastructure-agnostic and will work in any network environment. It installs on a dedicated server, and includes the hardened Linux operating system so the installation process is fast, easy and completely self-contained. Sentriant AG requires no client-side agents, greatly simplifying setup and administration. It also scales to the largest networks and the solution is very cost-effective.

Sentriant AG supports both in-line and out-of-band deployments. In the in-line mode Sentriant AG is positioned in the network between the endpoint devices and the rest of the network. Sentriant AG acts as a gateway, only providing access for endpoint devices that have met the necessary security requirements. Since Sentriant AG itself denies endpoint devices access to the network, no policy enforcement via internal routers, switches or other devices is required. In-line deployment is perfect for handling remote VPN/RAS endpoints by placing the Sentriant AG server directly behind the VPN concentrators.

For out-of-band deployments Sentriant AG supports both DHCP and 802.1x based enforcement. Out-of-band deployment allows the Sentriant AG server to reside anywhere in the network and yet still test and enforce access policies across all endpoints in network. In the DHCP mode Sentriant AG acts as a proxy for the existing DHCP server and assigns non-compliant machines IP addresses in an isolated quarantine subnet. In the 802.1x mode Sentriant AG can leverage the existing 802.1x infrastructure to add powerful endpoint testing to basic network authentication. The 802.1x mode can work with any supplicant and RADIUS server and is agnostic to the specific EAP method being used. 802.1x allows Sentriant AG to quarantine non-compliant devices by placing them into a isolated quarantine VLAN or through the user of dynamic ACLs.

Agentless Deployment Simplifies Administration

Sentriant AG tests for and enforces security-policy compliance without requiring an agent be installed on the each endpoint. There are no software downloads or installations required on the client side. This offers substantial benefits/advantages over the agent-centric approach found in many endpoint solutions. Since no software runs on the endpoint, Sentriant AG does not suffer the deployment problems or the increased administration that arise when clients/agents have to be installed and supported on each device. Software compatibility issues, upgrade deployment and support issues and increased helpdesk calls are all avoided. Because no client installations are included, the application can be implemented and the network secured much more quickly. Clearly, the agentless approach offers a compelling answer where unmanaged endpoints (that are not under the organization's control) are concerned.

Testing Managed and Unmanaged Endpoints

Sentriant AG tests for security policy compliance on managed endpoints directly under the control of an organization, such as corporate desktops and laptops, as well as unmanaged endpoints that are not under the organization's direct control.

The sections below demonstrate how Sentriant AG can be deployed to safeguard the network from a number of scenarios, including managed LAN connections and external or unmanaged connections via remote access, wireless or from remote offices.

Deployment Scenario: Testing Managed Endpoints

Internally, Sentriant AG tests for and enforces compliance on endpoints that connect directly to the internal LAN. This includes devices at a central location as well as devices at smaller or remote offices. Figure 1 shows how the Sentriant AG server is deployed to test internally connected endpoints. Sentriant AG tests two machines logging onto the network and determines one is non-compliant with security policies. Machines that are non-compliant are cordoned off into a separate quarantine network by Sentriant AG and only provided the access necessary to receive virus definitions, update software or receive updates from a patch management solution.

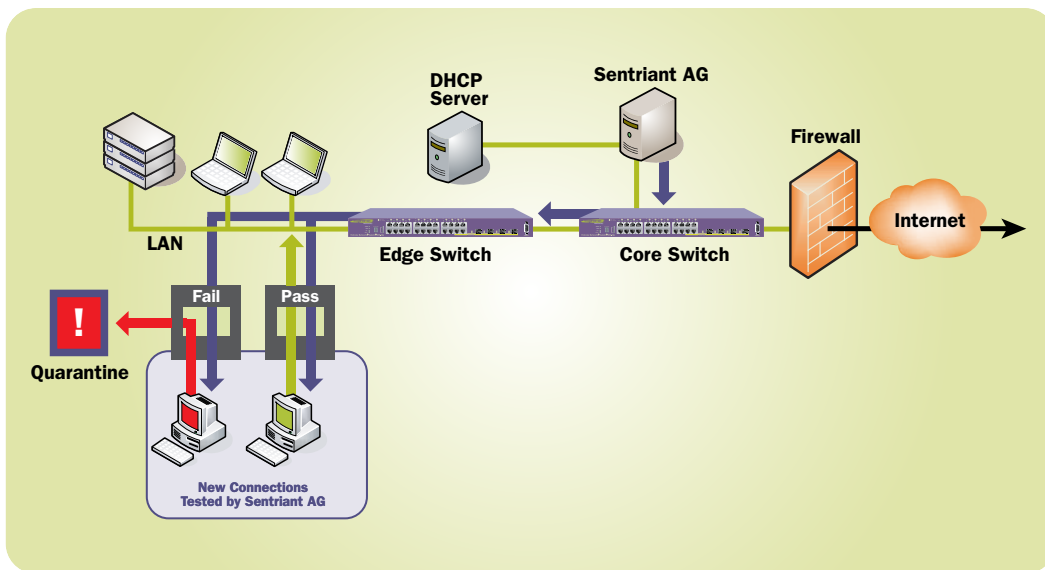


Figure 1. Sentriant AG Protects the Network from Threats by Internal Users

Deployment Scenario: Testing Managed and Unmanaged Endpoints

Unmanaged endpoints pose a greater risk than corporate-owned machines because their security is unknown and likely to be inadequate or non-existent. Unmanaged endpoints include:

- Laptops and desktops that may be brought into the organization by visitors, contractors or employees.
- Devices that the organization may never physically see or control, such as employees' and contractors' home computers and devices attaching to the network through VPN or dialup.

A VPN connection secures information, but does not protect your network from infected devices or malicious traffic. As shown in the Figure 2 diagram, two remote endpoints attempt to connect through the VPN. Sentriant AG tests these external endpoints before they are granted full access to network resources. Again, 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. In this diagram, Sentriant AG determines that one poses a risk and quarantines the device, while the other device is given full access.

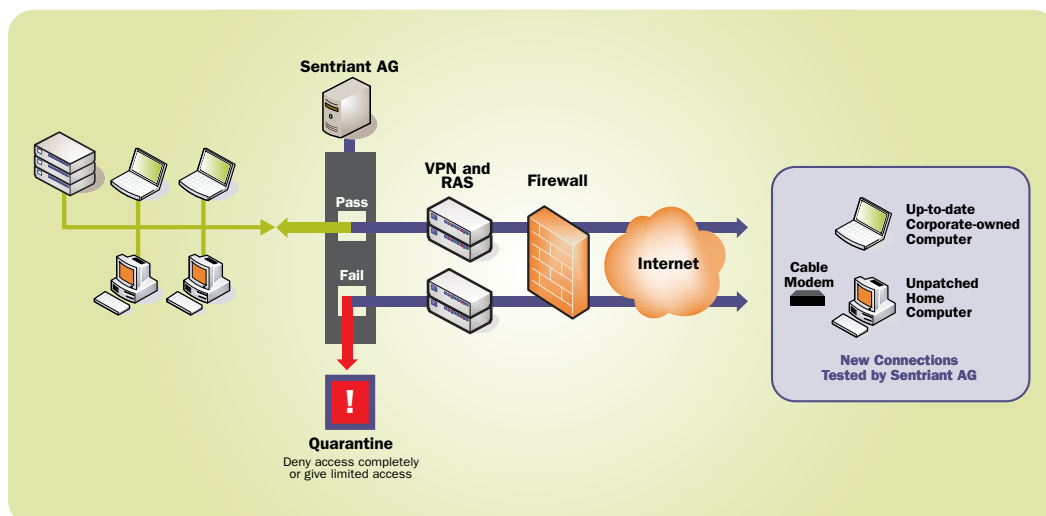


Figure 2. Sentriant AG Protects the Network from Threats by Remote Users

Deployment Scenario: Testing Wireless Connections

Sentriant AG can test and enforce compliance on endpoints that connect to the corporate network via wireless access methods. While wireless equipment can authenticate connecting devices, they do not protect your network from infected devices or malicious traffic. Figure 3 shows how the Sentriant AG server can be deployed behind wireless access points to test endpoint devices as they attempt to connect to the corporate network. Wireless devices that are

in compliance with corporate policies are allowed access to corporate resources while non-compliant devices can be denied access altogether, or quarantined or restricted from complete access until they are brought into compliance. In this example, two wireless devices attempt to connect through the wireless access points. Sentriant AG determines that one poses a risk and quarantines the device, while the other device is granted access.

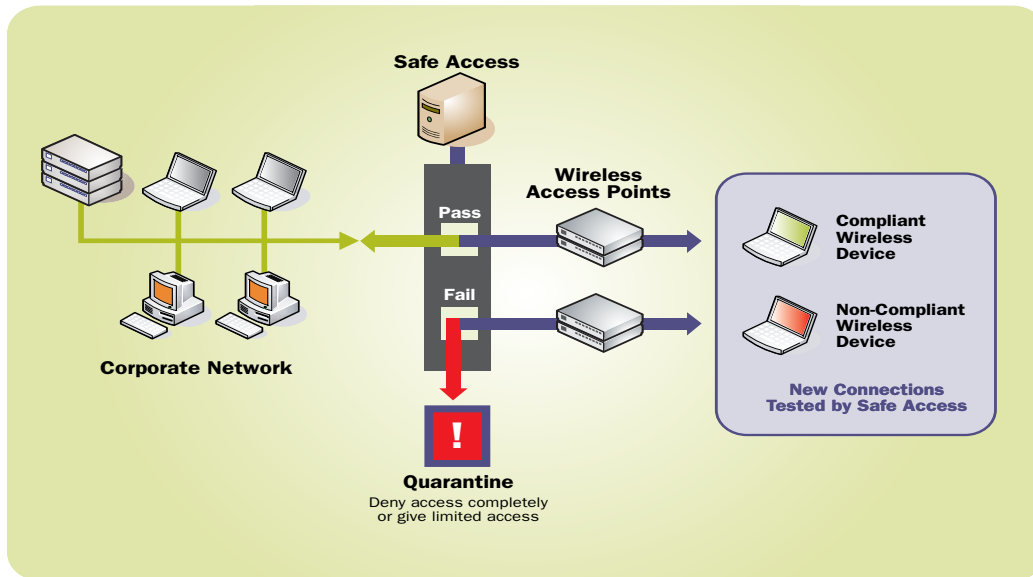


Figure 3. Sentriant AG Protects the Network from Threats by Wireless Connections

Conclusion

The increasing number and types of attacks launched from endpoint devices can no longer be ignored, and organizations must shift and expand their protection. While it is important to secure endpoints with up-to-date anti-virus software and personal firewalls, it is more important to protect the network from endpoints that may be compromised. Sentriant AG from Extreme Networks does exactly that. It protects the network by requiring endpoints to comply with security policy before they are allowed access.

Sentriant AG provides the following key capabilities:

- A full suite of testing capabilities
- Verification that harmful software, such as worms, Trojans or spyware, does not reside on the device
- Custom test creation
- Agentless testing
- Self remediation for noncompliant end users



www.extremenetworks.com

email: info@extremenetworks.com

Corporate and North America
Extreme Networks, Inc.
3585 Monroe Street,
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +852 2517 1123

Japan
Phone +81 3 5842 4011

© 2006 Extreme Networks, Inc. All rights reserved. Do not reproduce.
Extreme Networks, the Extreme Networks Logo, BlackDiamond, ExtremeXOS, and Sentriant are either registered trademarks or trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other trademarks are trademarks of their respective owners. Specifications are subject to change without notice.