

# Securing the University Network

---

## Abstract

Endpoint policy compliance solutions take either a network-centric or device-centric approach to solving the problem. The body of this paper addresses these two categories of solutions in securing university networks. The difference between these two approaches is the method used to enforce policy: network-centric systems enforce compliance by controlling access at the switch or router. Device-centric approaches are more focused on locking down the endpoint itself and providing a basic means to grant or deny access to the network.

In addition to providing an overview of these access control technologies, this paper provides an introduction to Sentriant™ AG, endpoint compliance solution from Extreme Networks® that combines the best features of both the network- and device-centric approaches.



## Introduction

---

Universities have a difficult network environment to secure. Proprietary information must be protected and the network must be available 24x7, yet tens of thousands of untrusted student-owned computers must be given access. That is where the problem arises. Network administrators cannot control what students do or have done with their laptops and desktops, and that puts the entire network at risk.

Compared to users in the business sector, students have an enormous amount of flexibility over how they configure applications, change security settings download or install software, and use file sharing, messaging, and Peer-to-Peer (P2P) applications. It's a network administrator's nightmare. The security of student computers (referred to as endpoints) is usually unknown and is frequently inadequate or non-existent. There are no guarantees that these devices have the latest security patches, up-to-date anti-virus definitions, or a personal firewall. They may already be infected with malware; worms, Trojans, spyware and viruses when they arrive on campus.

In the university environment, a single unpatched or compromised endpoint threatens the entire network. It can serve as a backdoor to intruders, a conduit for worms and spyware and it can infect or re-infect the network. Educational institutions strive to implement a consistent security policy that defines what is permitted and what is prohibited on student endpoints, but a number of logistical hurdles prohibit such policies from being enforced. Major impediments include:

- **The wide range of Operating Systems (OSs) and OS versions.** Implementing and administering a security policy that efficiently accommodates multiple OS platforms and versions is a prohibitively complex process.
- **A limited time for registering devices.** Students must have network access when classes begin, making it unfeasible for network administrators to implement uniform security measures on a device-by-device basis in the limited time available at the beginning of the semester.
- **The difficulty of having to physically touch each device.** Limited resources and personnel prohibit effective physical management of each device.

A number of technologies, referred to as endpoint security solutions, have come on the market that address this problem. In short, these technologies assess the security status of an endpoint against a defined policy, and then allow or deny access to the network based on the level of compliance. This paper describes these technologies, their pros and cons and how each achieves the goal of securing the network from harmful endpoints.

Generally, endpoint policy compliance solutions take either a network-centric or device-centric approach to solving the problem. The body of this paper addresses these two categories of solutions. The difference between these two approaches is the method used to enforce policy: network-centric systems enforce compliance by controlling access at the switch or router. Device-centric approaches are more focused on locking down the endpoint itself and providing a basic means to grant or deny access to the network.

In addition to providing an overview of these access control technologies, this paper provides an introduction to Sentriant™ AG, endpoint compliance solution from Extreme Networks® that combines the best features of both the network- and device-centric approaches.

## Network-Centric Technologies

---

The network-centric approach to endpoint policy compliance takes the view that the network must be protected from any type of endpoint device connecting to the network. This includes devices managed by the university (such as computers issued to instructors and school administrators), and more importantly, the student machines that are not owned or controlled by the institution.

The emphasis of the network-centric approach is:

1. Provide a mechanism to quarantine or restrict access of any device when it initially connects to the network.
2. Query anti-virus, personal firewall and other device software and configuration information to determine the security health of the device.
3. Compare the endpoint device's security health with the policy requirements for connecting to the network.
4. Allow the endpoint access to the network if it is compliant or quarantine the device if it is non-compliant.

An endpoint's security health is usually determined using a security agent (discussed later) or a network-based approach. The agent-less solution does not require that security agents be downloaded or reside on the device.

Two large players in the IT market, Cisco and Microsoft, support the network-centric approach with their Network Admission Control (NAC) and Network Access Protection (NAP) programs respectively. Each of these architectures will continue to evolve over time. Both Cisco's NAC and Microsoft's NAP utilize agents on the endpoint device whose primary purpose is to retrieve and communicate security health information, via APIs, from other third-party software. These agents do not perform additional security functions themselves, such as firewalling traffic or monitoring the endpoint device for suspicious behavior. Their job is to collect security health information about the endpoint from other third-party security products such as Extreme Networks endpoint compliance solution, Sentiagent AG, to determine whether the endpoint will be allowed on the network. Once the agent receives the required device security health information, it will inform the policy decision-making elements of the network infrastructure, enabling the appropriate enforcement response.

Sentiagent AG extends the capabilities of both the NAC and NAP architectures with the ability to test endpoints that do not have an agent installed. In these situations, Sentiagent AG can perform testing using its agent-less testing methods, i.e., the direct access and browser plug-in methods discussed later in this paper.

Sentiagent AG also acts as the compliance policy engine to test and determine the enforcement options for each endpoint device. After it makes this determination, Sentiagent AG instructs the network infrastructure devices as to whether the device should be quarantined or allowed access into the network. In the case of Cisco NAC, switches are updated to allow the endpoint full access or no access to the network. Microsoft NAP shares a similar approach but uses the IAS proxy server and IP address assignment to accomplish the goal.

## **Device-Centric Technologies**

The device-centric approach comprises a range of technologies, a number of which include built-in enforcement capabilities. Device-centric technologies are divided into two primary categories: network-delivered solutions and agent-based solutions.

### **Network-Delivered Endpoint Security**

Securing endpoint devices via network delivery means the network provides the means to assess the connecting endpoint's security posture and then quarantine or allow the endpoint device network access. This is performed without the use of a persistent agent or any pre-installed software. Network-delivered endpoint security, sometimes referred to as the agent-less approach, is comprised of three methods: direct access, network scanners and browser plug-ins. These methods are discussed in more detail in the following sections.

### **Network Delivery: Direct Access**

The direct access method is one of the easiest endpoint security architectures to implement, both for the student and for the IT Team. Using direct access, a central policy server connects to endpoint devices using NetBIOS or TCP session protocols. From this network connection, devices are tested for a range of security requirements such as patch levels, anti-virus state, security settings, browser settings, P2P software and banned applications. The tests performed examine the operating system registry, running processes and services, files, file attributes and other aspects of the endpoint device.

The direct access method, a device testing method provided by Sentiagent AG, is one of the only true agent-less architectures as it does not require any additional software on the endpoint device. The testing time and network performance of the direct access method is typically very efficient since most of the analysis is managed by the central policy server, code is not download across the network and the information retrieved from the endpoint is relatively small in size. Direct access is also advantageous where the endpoint connects over dial up or slower connections where downloading software to the endpoint is not a viable option. The direct access method is attractive in the educational environment, as no software need be installed on the student's endpoint, and the device does not need to be physically managed.

### **Network Delivery: Network Scanners**

The network scanner method examines endpoint devices by scanning across the network. The endpoint is scanned to determine the device's operating system, open ports, and running applications. These are used to test if the device has the required operating system fixes, if any exposed applications present a risk (such as P2P applications), and any other threats the device may pose. Some network scanners may also provide local checks, using administrator credentials to log onto the device.

The network scanner method is an extension of technology adapted from open source and commercial vulnerability scanners. Vulnerability scanners, such as the open source scanner Nessus, are customized with additional checks to test for endpoint requirements. Network scanning technologies typically require more network bandwidth and take longer to test endpoint devices since a wide range of ports and services must be examined. End users typically experience longer wait times for testing to complete when connecting to the network, or must be scanned after the fact. It is also important that other security technologies not restrict access to the endpoint device as they may see the port scanning and service analysis network traffic transmitted as possible network attacks. On their own, network scanners do not typically include any enforcement capabilities; they primarily alert administrators of devices that have network-threatening vulnerabilities.

### Network Delivery: Browser Plug-ins

The third network delivery method, browser plug-ins, executes browser plug-in software modules delivered to the endpoint device over the network. When the endpoint connects to the network, the user is prompted to allow the browser plug-in to be downloaded and installed into the running web browser window. The plug-in software may be a Windows ActiveX control (applicable only to endpoints running supported Windows operating systems and browsers) or a Java-based plug-in (which may support multiple types of operating systems). Using the security access level of the logged-in end user, the plug-in software examines registry settings, processes, services and other settings on the device. The results are then used to determine if the device will have further access to the network, will be quarantined or have no network access.

Browser plug-ins are frequently used in Secure Sockets Layer (SSL) Virtual Private Network (VPN) endpoint security technologies that already require a browser to access network resources. Extreme Networks Sentriant AG also offers an ActiveX browser plug-in option for endpoint device testing. Agent-based technologies (discussed below) also offer browser plug-ins as a so-called agent-less alternative to requiring the installation of a persistent agent. Browser plug-ins have some disadvantages. Some universities restrict end users from installing browser plug-ins, so this option may not be viable in all situations. The download size of the software executable may also be an issue for slower networks. The direct access network delivery option is a good alternative when browser plug-ins are not acceptable.

The network delivery-based approaches discussed above offer the most user-friendly experience for security administrators and end users alike as they do not require the permanent installation of software agents onto endpoints. The direct access and browser plug-in methods offer the most comprehensive and compelling approach to ensuring that endpoints do not pose a threat of the network.

## Agent-Based Endpoint Security

The alternative to the network-delivered approach is the use of permanently installed, or persistent, software agents. Software agents are always running in the background on the student's computer, monitoring it for suspicious or non-compliant activities. Most agents must be pre-installed prior to the endpoint device connecting to the network. In some cases students can install an agent over the network when presented the option via web page that is displayed when the endpoint is initially quarantined.

### Security Agents

Security agents (or trust agents) are the least intrusive type of endpoint security software agents. The job of a security posture agent is to act as the negotiation point between the network and the endpoint device. The security agent informs the access control mechanism about the security health of the endpoint device.

In some cases, such as Sentriant AG, the security agent also acts as the conduit for providing information about the state of security elements on the endpoint device, such as patch levels or anti-virus health. Security agents do this by working cooperatively with third-party security products such as anti-virus programs. Security agents are typically small in size and have little impact on the endpoint device's operations or the reliability of other endpoint software since their interference with the actions of underlying operating system is minimal. Some examples of security agents are the Cisco Trust Agent (part of the Cisco NAC architecture discussed above) and Sentriant AG Security Posture Agent.

### Host Intrusion Detection Agents

Host Intrusion Detection Systems (HIDSs) are software agents that reside on endpoint devices and strictly monitor specific activities on the endpoint. The first job of a HIDS is to monitor network connections, processes, file activities, logging, and other aspects of the underlying endpoint's operations. This requires that the HIDS software be configured so it understands normal operations versus unusual or unauthorized actions that might occur on an endpoint device. For example, only certain system processes should write to system logs, whereas root kit software might attempt to overwrite or remove entries for a system log in an attempt to cover up the intrusion. The second job of a HIDS is to prevent or limit malicious operations by unauthorized software on the endpoint device. The HIDS agent may block access to files by unauthorized software, prevent important process from being shut down, such as anti-virus software, or shut down network connections that may be under the control of malicious software.

HIDS technology can be effective at preventing the compromise or spread of malware because it maintains strict control of activities on the endpoint device. This can also present some challenges when deploying HIDS technologies as they may require a significant amount of configuration and tuning to properly understand malicious versus non-malicious system, application, and end user activities. As such, these technologies may not be practical to implement on a university scale. Software compatibility and upgrade testing can also be an issue since HIDS agents typically embed themselves deeper into file, network, and process operations of the operating system.

### Personal Firewall Agents

Personal firewalls have been around for some time, as either consumer products or enterprise-managed products. The basic function of a personal firewall is much like the network firewall at the perimeter of most networks. Personal firewalls allow certain network connections to be established to and from the endpoint while restricting others. For example, it is usually permissible for an email client application to communicate over port 110 (used by the POP3 protocol) to a POP3 email server, but it may not be acceptable for the same endpoint device to perform an IP address sweep or port scan that might be used by a worm to spread to other vulnerable devices. The personal firewall agent is controlled by firewall rules that specify what types of network connections are allowed to and from the endpoint, and which applications may perform these actions. Any other network action not allowed by the personal firewall rules is restricted. Rather than relying on end users to configure, either properly or improperly, their own firewall rules, enterprise-managed personal firewalls distribute rules to each endpoint from a centrally managed server.

Many legacy personal firewall products have been upgraded to also check for endpoint security requirements. In addition to monitoring and controlling network access to and from the endpoint device, the personal firewall agent may also check the patch level of a device, monitor the health of anti-virus software, restrict applications such as P2P software or check security settings on the device. Personal firewall agents are larger in size than security posture agents and also require strict control of TCP communications to and from the device. They must also monitor which software and applications are attempting network actions that should be blocked as indicated by the personal firewall rules. As with HIDS agents, personal firewall agents embed themselves deeper within the operating system and network stack to perform these monitoring and blocking functions. Similarly, they also have the same considerations for configuration, software compatibility, and operating system software upgrades.

## Extreme Networks Sentriant AG

---

### Protect the Network by Ensuring Endpoints Comply with Security Policy

By combining the best of both network- and device-centric endpoint security approaches, Sentriant AG gives administrators control over unsecured, untrusted student endpoints. It protects the network from the crippling worms, viruses, spyware, and dangerous applications that endpoints can introduce.

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 student computers may specify that:

- Antivirus must be running and the virus definitions must be up to date
- All Widows service packs and hotfixes must be installed
- P2P networking software is prohibited
- The endpoint must be free of all worms, trojans, and spyware
- A personal firewall must be present.

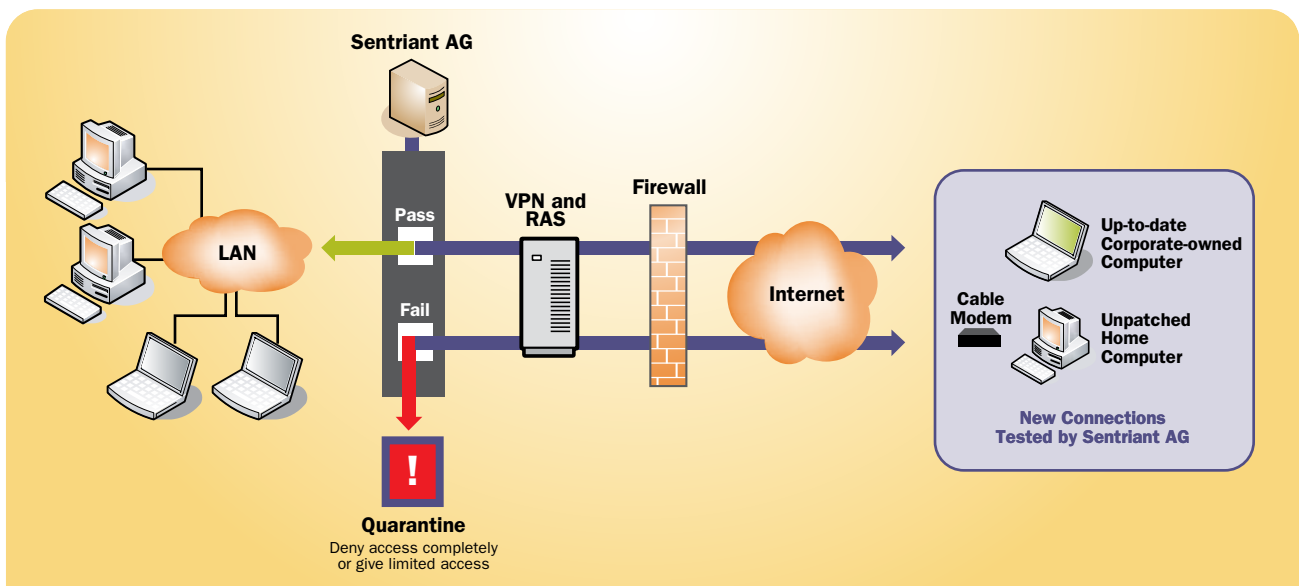
Endpoints that fail any of these tests are subjected to the enforcement actions specified in the defined policy. For example, Sentriant AG can completely deny access to the network, it can provide access for a grace period, or it can quarantine the endpoint limiting access to, for example, the Internet. With this limited, quarantined access, the endpoint is prohibited from damaging the network, yet it is able to download the patches, updates, etc. 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. Sentriant AG is part of both the Cisco NAC and Microsoft NAP initiatives and functions seamlessly in NAC/NAP environments.

### Testing University-owned and Untrusted Endpoints

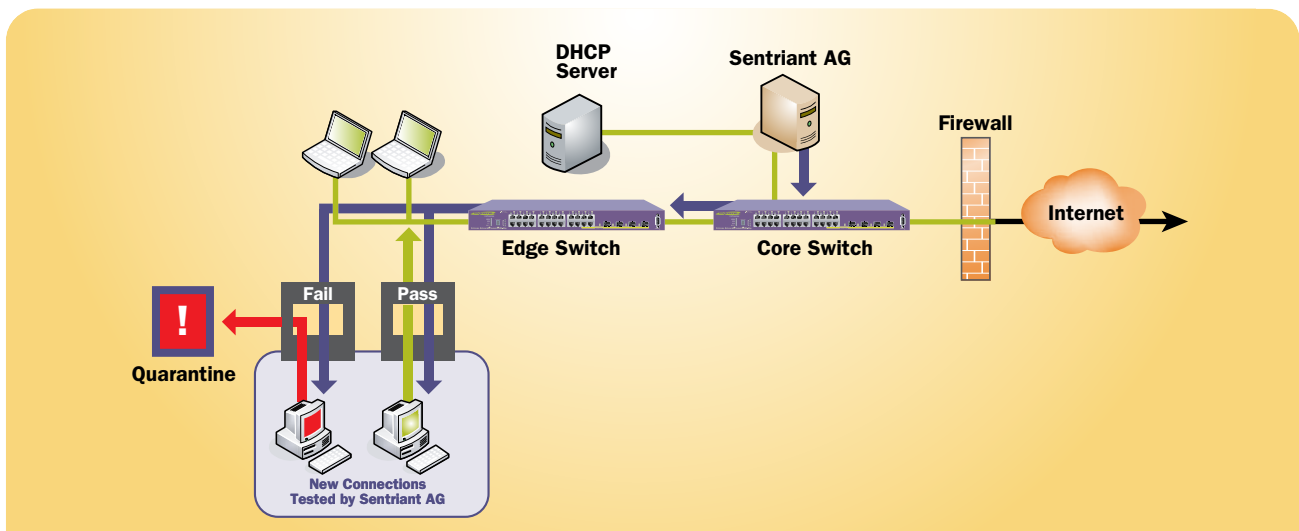
Sentriant AG tests for security policy compliance on endpoints connecting directly to the university network—both university-owned devices and untrusted student machines. Sentriant AG also enforces policy compliance on devices connecting remotely through VPN, RAS, or wireless devices.

Figure 1 shows how the Sentriant AG server is deployed to test endpoints connecting directly to the campus network. Machines that are non-compliant are cordoned off into a separate quarantine network and only provided the access necessary to receive virus definitions, update software, or receive updates from a patch management solution.

Additionally, Sentriant AG tests endpoints connecting to the network remotely before they are granted full access to network resources, as shown in Figure 2. 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 students and faculty updating their home computers through the university’s VPN. A VPN connection secures information, but does not protect your network from infected devices or malicious traffic.



**Figure 1. Sentriant AG protects from threats by students, faculty and administrators connecting directly to the network. Sentriant AG tests two machines logging on and determines one is noncompliant with security policy and quarantines the device.**



**Figure 2. Sentriant AG protects from threats from remote users. Two remote endpoints attempt to connect through the VPN; Sentriant AG determines that one poses a risk and quarantines the device.**

## Agent-less, ActiveX, and Agent-based Testing Options Simplify Administration

Sentriant AG testing is fast and the user is kept informed of test progress and results. Sentriant AG provides three testing methods: agent-less, ActiveX, and security posture agent. These options maximize protection / endpoint coverage with minimal demands on IT resources.

Administrators can prioritize the testing methods to be applied to endpoints. Upon the user's initial connection attempt, Sentriant AG applies these in the order specified. Which testing method is applied is driven by the endpoint OS and the installed browser.

After the initial compliance tests, Sentriant AG continually tests devices that have been granted access to ensure that real-time system changes do not violate the Access policy.

### Test Categories

Sentriant AG goes well beyond simply checking for the latest patches and antivirus 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, 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 P2P 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 within the policy are applied to the assigned devices as they logon. For example, access policies can be created specifically for various users such as students connecting remotely, endpoints that run a specific operating system and wireless endpoints. Sentriant AG is extremely flexible and adaptive, allowing you to maintain unlimited number of access policies to accommodate the compliance process that makes the most sense for your institution.

## Conclusion

Universities face the unique challenge of securing networks that must provide access to thousands of untrusted student endpoints. In the past any attempts at implementing a security policy to govern these devices have been hampered by limited time and resources and the diversity of machines students bring on campus.

Technologies are now available that solve the problem. Network and device-centric technologies use a variety of approaches to secure endpoints and protect the network from potentially harmful machines.

Sentriant AG combines the best capabilities of these two approaches. It protects the network by ensuring both student- and university-owned endpoints comply with security policy before they are allowed access. It defends against attacks delivered by endpoint devices. 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
- Flexible endpoint testing options: agentless, ActiveX, and agent-based testing
- Self remediation for noncompliant end users



[www.extremenetworks.com](http://www.extremenetworks.com)

[email: info@extremenetworks.com](mailto: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 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.