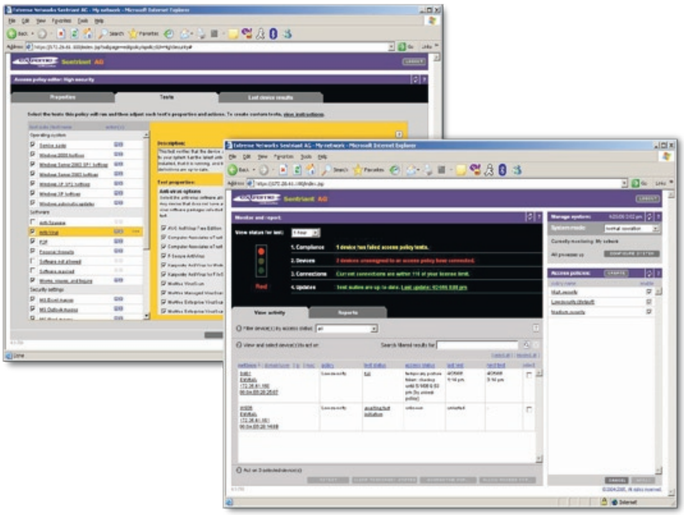
Sentriant™ AG



Endpoint policy compliance—protects the network by making certain that endpoint devices are free from threats and in compliance with IT security policies.

Noncompliant Endpoint Remediation

- Flexible access policies
- Agent-less solution
- Protection for remote and local connections

Comprehensive Yet Scalable Solution

- Deep endpoint testing
- Simple, easy deployment
- Flexible enforcement options

Powerful Enterprise Integration

- Enterprise Integration Framework
- Sharing endpoint compliance data
- Acting on input from other systems

While efforts to improve network security have been focused on locking down the network perimeter and securing critical internal network assets, the security of endpoint devices, which make up the majority of networks, have gone largely untouched.

Attackers, however, are increasingly targeting endpoint devices, such as LAN workstations, remote access laptops and home computers to compromise networks. Their motivation is simple: endpoint devices typically bypass standard perimeter security measures and connect directly into the network.

Extreme Networks® Sentriant™ AG verifies that endpoint devices, such as laptops and desktops, accessing the network are free from security threats and in compliance with the organization's security standards. It systematically tests endpoint devices for compliance with organizational security policies, quarantining non-compliant machines before they can damage the network.

Sentriant AG dramatically reduces the cost and effort of securing those devices—devices used by remote employees and contractors using VPN or dial-up, devices connecting to the network directly, and devices connecting through wireless networks—including devices your IT group may not own or adequately control.

Target Applications

- Wireless and mobile computing
- Regulatory compliance for security initiatives
- Quarantines endpoint devices that are not in compliance
- Remote access using devices that are not controlled by the organization

Endpoint security—Safeguarding your network.

extreme networks™

Noncompliant Endpoint Remediation

Sentriant AG intercepts device connections and examines the connecting device to see if it meets the organization's policies for security such as security settings, patches and antivirus safeguards. Devices not meeting policy can be denied access or quarantined.

Flexible Access Policies

Using Sentriant AG, administrators create access policies that define which applications and services are permitted and specify the actions to be taken when devices do not comply. Sentriant AG tracks all testing and connection activity and produces a range of reports for auditors, managers and IT staff.

Agentless Solution

Sentriant AG is very simple to deploy because it does not require an agent to be installed on endpoint devices. However, for organizations that prefer an agent-based approach, Sentriant AG provides that alternative too. There are three options for testing endpoint devices:

- **Agent-less**—No client-side agent required on endpoint
- **ActiveX plugin**—Tests endpoint through web browser
- **Sentriant AG agent**—Tests endpoint through installed client

The agent-less option is ideal for testing Windows® 2000 and Windows XP Pro machines. It offers zero-maintenance device administration as no client needs to be installed or supported on the endpoint.

The ActiveX plug-in tests all Microsoft–supported Windows operating systems and foreign endpoints where an installed agent is impractical.

Sentriant AG agent also tests all Microsoft–supported Windows operating systems and can be used for internal legacy devices such as those running Windows 98 or NT.

Administrators can prioritize the order that testing options are applied as devices initially connect to the network. For example, on an internal network, the Sentriant AG agent might be selected as the preferred testing method, while on remote access or VPN connections, the agent-less option might be the desirable method.

Protects Remote and Local Connections

Sentriant AG also protects the LAN from threats by remote users or from internal users. Any machine that poses a risk can be quarantined, whether that machine is connecting from an external location via a VPN, or connecting locally (see Figure 1).

VPN connections secure information, but they do not protect your network from infected devices or malicious traffic. Sentriant AG identifies remote devices that pose a threat and quarantines the device.

Sentriant AG also protects from threats by internal users (see Figure 2). Compliant devices are allowed LAN access while noncompliant devices are quarantined.

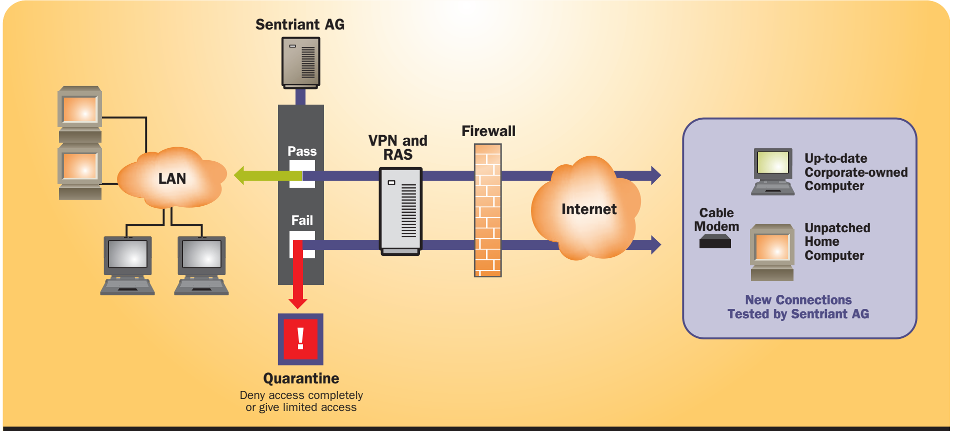

Sentriant AG
LAN
Pass
Fail
VPN and RAS
Firewall
Internet
Cable Modem
Up-to-date Corporate-owned Computer
Unpatched Home Computer
New Connections Tested by Sentriant AG
!
Quarantine
Deny access completely or give limited access

Figure 1: Protection from Remote Users

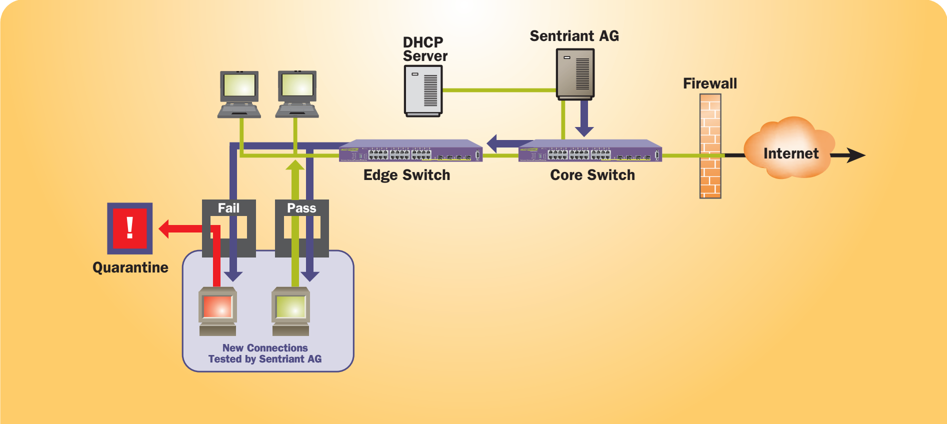


Figure 2: Protection for internal LAN Connections

Comprehensive and Scalable Solution

Sentriant AG is a powerful endpoint security solution that provides deep and comprehensive testing of endpoint devices. At the same time, it is easily deployed, supports industry standards and scales to meet the needs of the largest organizations.

Flexible Enforcement Options

Sentriant AG supports IEEE 802.1x, DHCP, inline and other enforcement schemes for maximum deployment options and easy integration with existing security systems. These industry-wide initiatives enable the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources.

Sentriant AG also adds extensive policy compliance and enforcement features in order to verify that the applications and services running on endpoint devices comply with security and access policies. Figure 3 highlights the key features and benefits of the Sentriant AG.

Deep Endpoint Testing

Access policies consist of one or more tests to assess operating system integrity, verify that key hotfixes and patches have been installed, verify that anti-virus and other security applications are present and up-to-date and detect the presence of other malware. Any incidence of potentially dangerous applications such as file sharing, Peer-to-Peer (P2P), or spyware is also checked. Administrators can also create custom tests through Sentriant AG's Application Programming Interface (API). Sentriant AG ships with dozens of out-of-the box tests in the following categories:

- **Operating systems**—Tests for services packs and hotfixes
- **Browser security policy**—Verifies browser security settings match the organization's policy
- **Security settings**—Tests for macros, services, Windows security policy, and startup registry entries
- **Software:**
  - **Anti-virus**—Tests for required AV software
  - **P2P**—Tests for prohibited P2P software
  - **Personal firewalls**—Tests for required firewall
  - **Software required and software not allowed**—Defined by administrator
  - **Worms, viruses and Trojans**—Checks for the presence of dozens of attacks and infections

Simple, Easy Deployment

Sentriant AG installs on a dedicated server. Installation includes the hardened Linux operating system, so the installation process is fast, easy and completely self-contained. Because Sentriant AG requires no client-side agents, setup, administration and deployment is greatly simplified.

Sentriant AG easily scales from the smallest to the largest networks. Most importantly, the solution is cost-effective.

Network Protection

Feature	Benefit
Tests endpoints as they connect to the network	Mitigates network damage caused by infected or unsafe endpoints
Test library updated as frequently as hourly	Automatically protects against newly released threats
Multiple test categories, dozens of tests	Protects from the range of endpoint-specific threats
Fast custom test creation through open API	Organization-specific testing
Flexible enforcement options (grant, deny or quarantine access) driven by corporate security policies	Does not inhibit the flow of business
Offers range of enforcement on a per access policy basis, from passive monitoring (no enforcement) to strict enforcement; allows controlled rollout of Sentriant AG	Graduated enforcement
Unlimited number of customizable access policies tailored to, for example, the level of threat, operating system and organizational requirements	Provides tailored testing/enforcement for variety of user types (e.g., visitors, executive staff and Windows 2000 users)
Enterprise Integration Framework: • Allows import/export of security compliance data • Allows third-party systems to control Sentriant AG functions	Leverages existing network security investments

Compliance and Reporting

Tests endpoints against user-defined access policies	Verifies that endpoints conform to security policy(s)
Regularly retests endpoints while logged in on administrator-specified schedules	Eliminates threat from endpoints that become non-compliant while connected
Endusers of non-compliant endpoints informed of the steps required to bring devices into compliance	Reduces administrative overhead
Detailed reporting meets the needs of auditors, managers and IT staff members	Documents security/compliance status

Administration

Offers three flexible endpoint testing methods: • Agent-less • ActiveX • Sentriant AG agent	Maximizes protection/endpoint coverage with minimal demands on IT resources
Predefined access policies (High, Medium, Low) available out-of-the-box	Quick time-to-value
Thousands of endpoints tested and managed simultaneously	Enterprise-wide protection
Manual overrides allow administrators to retest, quarantine or grant access on demand	Ability to react to/control dynamic environment in real time
Notifies administrator of testing status via email; displays all testing activity in real time	Enables rapid response to security priorities
High-availability bypass switch with fail-open functionality	Guards against single point of failure

Figure 3: Sentriant AG Features and Benefits

Powerful Enterprise Integration

Sentriant AG leverages existing enterprise security systems by making it easy for endpoint compliance data to be shared between the systems. Sentriant AG can also take input from other enterprise security systems which can be used to dictate if a connection should be allowed or not.

Enterprise Integration Framework

Sentriant AG includes the Enterprise Integration Framework, an open architecture that allows for the import and export of data to and from Sentriant AG. Integration allows Sentriant AG to share endpoint security data with other IT systems. It also allows third-party systems to control Sentriant AG functions, such as testing and quarantining.

Sharing Endpoint Compliance Data

Sentriant AG can share endpoint data with other enterprise security systems. For example, Sentriant AG could be integrated with your trouble ticketing system. If a Sentriant AG test determines an endpoint does not have a corporate-approved personal firewall installed, Sentriant AG Access could automatically open a trouble ticket on the device. Likewise, endpoint device and testing data could be shared with patch managers, Intrusion Detection/Prevention System (IDS/IPS), vulnerability managers, security information managers, third-party reporting tools, and wide array of other IT systems.

Acting on Input from Other Systems

The Enterprise Integration Framework also allows IT systems to initiate testing and quarantining activities through Sentriant AG. For example, if your IPS detects attacks emanating from an endpoint, it could instruct Sentriant AG to immediately quarantine the device. Integration leverages Sentriant AG quarantining and testing capabilities and the capabilities of the other security-related systems on your network, thereby providing enhanced security for the network and improved productivity and efficiency with the IT environment.

Enterprise Integration Framework examples:

- Network IPS detects attacks emanating from an endpoint and instructs Sentriant AG to immediately quarantine the device.
- Sentriant AG determines an endpoint does not have a corporate-approved personal firewall and automatically opens a trouble ticket on the device

Benefits of the Enterprise Integration Framework are that it improves security, productivity, and efficiency with the IT environment, leverages Sentriant AG quarantining and testing capabilities and leverages capabilities of the other security-related systems on your network.

The Enterprise Integration Framework allows third-party systems to control Sentriant AG endpoint device testing and quarantining functions. The Enterprise Integration Framework also allows endpoint compliance data to be exported from Sentriant AG to other security systems (see Figure 4).

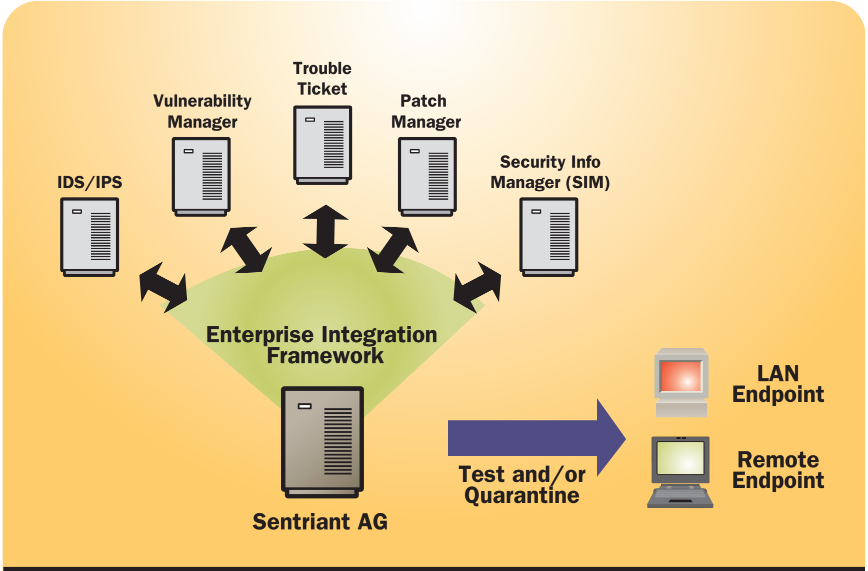


Figure 4: Enterprise Integration Framework

Technical Specifications

System Requirements

A dedicated server for product installation with the following minimum system requirements:

- Pentium® 4, 1.2 GHz or above
- 1 gigabit RAM
- 10 gigabit disk space
- Two network interface cards 10/100 (3Com or Intel)
- CD ROM drive
- An Internet connection that allows outbound SSL communications

Management console: A workstation running one of the following browsers (128-bit encryption required):

- Mozilla Firefox 1.0 and higher (Linux, Windows®)
- Mozilla 1.7 and higher (Linux, Windows)
- Internet Explorer 6.0 and higher (Windows)

Standard Endpoint Tests That Ship with Sentriant AG:

Operating Systems
- Service Packs
- Windows 2000 hotfixes
- Windows Server 2003 SP1 hotfixes
- Windows Server 2003 hotfixes
- Windows XP SP2 hotfixes
- Windows XP hotfixes
- Windows automatic updates

Browser Security Policy
- IE internet security zone
- IE local intranet security zone
- IE restricted site security zone
- IE trusted site security zone
- IE version

Security Settings
- MS Excel macros
- MS Outlook macros
- MS Word macros
- Services not allowed
- Services required
- Windows security policy
- Windows startup registry entries allowed

Software Anti-virus
- AVG AntiVirus Free Edition
- Computer Associates eTrust EZ
- AntiVirus
- Computer Associates eTrust AntiVirus
- F-Secure AntiVirus
- McAfee VirusScan
- McAfee Managed VirusScan
- McAfee Enterprise VirusScan
- Norton AntiVirus
- Symantec Corporate AntiVirus
- Trend Micro AntiVirus
- Trend Micro OfficeScan Corporate
- Edition
- Sophos AntiVirus

P2P
- Altnet
- AOL instant messenger
- BitTorrent
- Chainsaw
- Chatbot
- DICE
- dIRC
- Gator
- Hotline Connect Client
- IceChart IRC Client
- ICQ Pro
- IRCXpro
- Kazaa
- Kazaa Lite K++
- leafChat
- Metasquarer
- mIRC
- Morpheus
- MyNapster
- MyWay
- NetIRC
- NexIRC
- Not Only Two
- P2PNet.net
- PerfectNav
- savIRC
- Trillian
- Turbo IRC
- Visual IRC
- XFire
- Yahoo! Messenger

Personal Firewalls
- Computer Associates EZ Firewall
- F-Secure Personal Firewall
- McAfee Personal Firewall
- Internet Connection Firewall
- (Pre XP SP2)
- Symantec Client Firewall
- Norton Client Firewall
- Sygate Personal Firewall
- Tiny Personal Firewall
- Trend Micro Personal Firewall
- ZoneAlarm Personal Firewall
- Windows Firewall

Software not allowed
- Administrator defined

Software required
- Administrator defined

Spyware, worms, viruses, and trojans
- Keylogger.Stawin
- Trojan.Mitglieder.C
- VBS.Shania
- W32.Beagle.A@mm
- W32.Beagle.AB@mm
- W32.Beagle.AG@mm
- W32.Beagle.B@mm
- W32.Beagle.E@mm
- W32.Beagle.J@mm
- W32.Beagle.K@mm
- W32.Beagle.M@mm
- W32.Beagle.U@mm
- W32.Blaster.K.Worm
- W32.Blaster.Worm
- W32.Doomhunter
- W32.Dumaru.AD@mm
- W32.Dumaru.AH@mm
- W32.Galil.F@mm
- W32.HLLW.Anig
- W32.HLLW.Cult.M@mm
- W32.HLLW.Deadhat
- W32.HLLW.Deadhat.B
- W32.HLLW.Doomjuice
- W32.HLLW.Doomjuice.B
- W32.HLLW.Lovgate@mm
- W32.Hiton
- W32.IRCBot.C
- W32.Kifer
- W32.Klez.H@mm
- W32.Klez.gen@mm
- W32.Korgo.G
- W32.Mimail.Q@mm
- W32.Mimail.S@mm
- W32.Mimail.T@mm
- W32.Mydoom.A@mm
- W32.Mydoom.B@mm
- W32.Mydoom.M@mm
- W32.Netsky.B
- W32.Netsky.C
- W32.Netsky.D
- W32.Netsky.K
- W32.Netsky.P
- W32.Rusty@m
- W32.Sasser.B
- W32.Sasser.E
- W32.Sasser.Worm
- W32.Sircam.Worm@mm
- W32.Welchia.Worm
- and more...

Ordering Information

Part Number	Description
72025	Sentriant AG – per user, 100 - 250 users
72050	Sentriant AG – per user, 251 - 500 users
72100	Sentriant AG – per user, over 500 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