Sentriant® AG200

Network Access Control (NAC)—protects the network by verifying that endpoint devices are free from threats and in compliance with IT security policies.

Advanced Endpoint Integrity Testing

- Flexible access policies
- Comprehensive test suite
- Pre-connect testing
- Wide range of endpoint support

Flexible Deployment Options

- Multiple enforcement methods
- Single-server or multi-server deployment
- Simple, easy installation and rollout

Enterprise-Class Management and Administration

- Centralized management
- Multi-user, role-based administration
- Powerful reporting capabilities
- Enterprise Integration Framework

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 devices on the network, have gone largely untouched.

Security attacks, however, are increasingly originating from endpoint devices such as LAN workstations, remote access laptops and home computers to compromise networks. The reason is simple: endpoint devices typically bypass standard perimeter security measures and connect directly into the network.

Extreme Networks® Sentriant AG200 verifies that endpoint devices accessing the network, such as laptops and desktops, 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 AG200 dramatically reduces the cost and effort of securing internal network access. It tests 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

- Preventing the introduction of malware or use of high risk software in the network
- Protecting the LAN from remote or foreign devices that are not controlled by the organization
- Security initiatives for regulatory compliance (SOX, HIPAA, PCI-DSS)

Sentriant security solutions—Safeguarding your network.

extreme networks™

Advanced Endpoint Integrity Testing

Sentriant AG200 intercepts device connections and examines the connecting device to see if it meets the organization's policies for security. Devices not meeting policy can be denied access or quarantined.

Flexible Access Policies

Sentriant AG200 allows administrators to create rich policies for controlling network access through a simple point and click policy editor. Each policy consists of one or more tests to assess if endpoints meet the required security level and the actions to be taken when devices do not comply. Actions can include logging the test results, sending an email alert to IT, providing the end-user a warning along with a limited time window to resolve the issue, or quarantining the device immediately. Sentriant AG200 can support multiple policy sets in order to meet the varying security requirements of distinct user communities and network locations.

Comprehensive Test Suite

When creating policies, administrators can choose from hundreds of off-the-shelf endpoint integrity tests that ship with the product. Test categories currently include:

- OS service packs and hotfixes
- Browser and OS security settings
- Wireless security settings
- Anti-virus software (installed, running and up-to-date)
- Anti-spyware software (installed, running and up-to-date)
- Personal firewall software (installed and running)
- Peer-to-peer applications (presence of)
- Worms, viruses, trojans, spyware (presence of)
- Required or prohibited software (administrator defined)

All tests are constantly updated to maintain the most current level of protection. Custom tests can also be created in order to address unique customer requirements.

Pre-Connect Testing

Sentriant AG200 automatically tests devices as they connect to the network against the access policies that have been defined. With this form of testing the network is not put at risk as access is not allowed until the health of each endpoint has been fully assessed. The purpose-built testing engine of Sentriant AG200 can complete a full integrity check in only seconds, thereby minimizing the impact to end-users. Non-compliant devices can be placed in quarantine where they can be repaired before being allowed onto the network. Sentriant AG200 will periodically re-test devices that remain connected to the network to ensure ongoing policy compliance.

Wide Range of Endpoint Support

Sentriant AG200 supports both Microsoft Windows (2000/2003/XP/Vista) and Mac OS X endpoint devices, and provides three options for assessing endpoint integrity:

- **Agent-less—No client-side software required on endpoint**
  The agent-less option is ideal for managed PCs operating in a Microsoft domain environment. It offers zero-maintenance device administration, as no client software needs to be installed or supported on the endpoint.
- **Agent—Tests endpoint through installed client**
  The Sentriant AG200 agent is available for Microsoft Windows operating systems as well as Mac OS X. The agent is lightweight, easy to install and automatically kept up-to-date making it ideal for both managed endpoint and long-term guests.
- **ActiveX—Tests endpoint through browser**
  The ActiveX plug-in tests machines running Microsoft Windows operating systems and is ideal for foreign endpoints where agent-less testing or an installed agent is impractical.

Sentriant AG200 provides the same depth of testing regardless of which option is used. All three options can be used in conjunction to ensure complete coverage across the complete range of endpoint devices (see Figure 1). For endpoints that cannot be tested, such as printers, IP phones or handheld devices, Sentriant AG200 supports flexible exclusion rules to control whether or not to provide access to these devices or not to provide access to these devices.

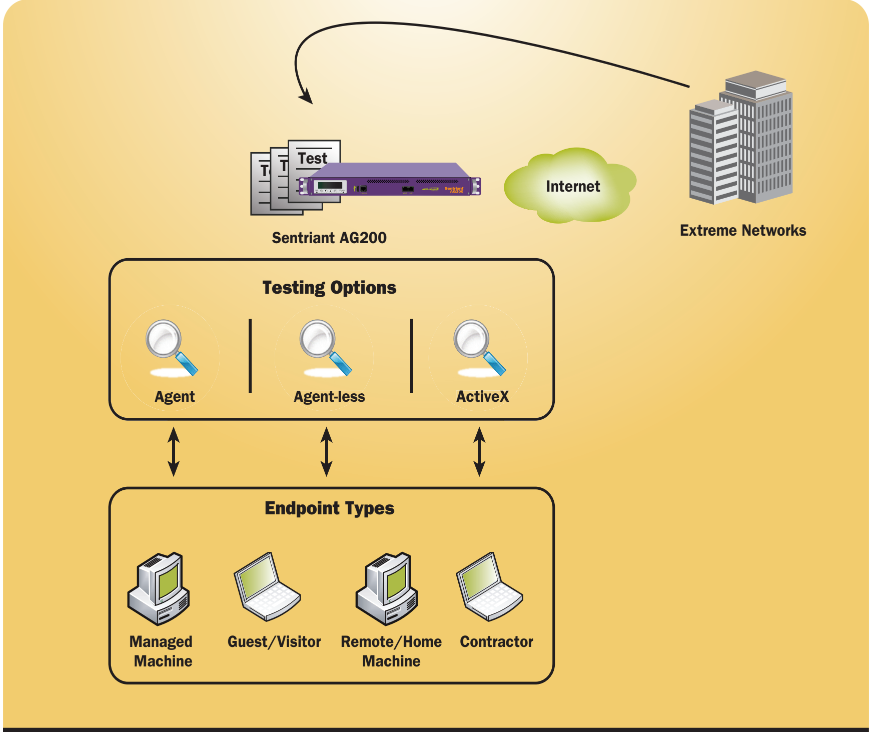

Figure 1: Testing Options

Flexible Deployment Options

Sentriant AG200 is a powerful access control solution that is easily deployed, supports industry standards and scales to meet the needs of the largest organizations.

Multiple Enforcement Methods

Sentriant AG200 supports several standards-based enforcement schemes for quarantining endpoints making it well suited to a variety of network infrastructures (see Figure 2). For out-of-band deployment, Sentriant AG200 supports both DHCP and 802.1X enforcement methods. Out-of-band deployment allows the Sentriant AG200 server to reside centrally and yet still test and enforce policy across all endpoints in the network.

When using DHCP enforcement, Sentriant AG200 integrates with an existing network DHCP server to assign non-compliant machines IP addresses in an isolated quarantine subnet. When using 802.1X enforcement, Sentriant AG200 leverages existing 802.1X-enabled infrastructure to add powerful endpoint testing to basic network authentication. Non-compliant devices are quarantined by placing them into an isolated VLAN or by creating dynamic ACLs using RADIUS attributes passed back to the network infrastructure. The 802.1X enforcement option works with any client supplicant and supports authentication pass-through to an existing RADIUS server, Microsoft Active Directory or OpenLDAP.

For inline deployments, Sentriant AG200 is positioned physically between the endpoint devices and the rest of the internal network. Since Sentriant AG200 can itself deny endpoints access to the network, no policy enforcement via internal routers, switches or other devices are required. Inline deployment is perfect for handling remote endpoints by placing the Sentriant AG200 server directly behind any VPN concentrator or for handling wireless endpoints by placing Sentriant AG200 between the wireless controller and the wired LAN.

Single-Server or Multi-Server Deployment

For basic network environments a single Sentriant AG200 can be used to provide a complete standalone NAC solution for up to 1,500 endpoints. For more complex environments, Sentriant AG200 supports a multi-appliance architecture consisting of a central Management Server that controls one or more dedicated Enforcement Servers. Each Enforcement Server can be positioned in a different region of the network, and can and utilize a different enforcement method. This approach makes it possible to deploy the NAC solution across complex, heterogeneous networks and manage policy consistently across all access types (wired, wireless, VPN) in all locations. Sentriant AG200 also supports an advanced clustering capability that allows groups of Enforcement Servers to operate together to achieve superior scalability and resiliency at each enforcement point. Sentriant AG200 automatically distributes the overall endpoint testing load across all servers in a cluster, providing a straightforward way to scale the solution beyond the limits of a single Enforcement Server. Clustering also provides a solution for high availability needs. All endpoint state information is synchronized throughout the cluster and should any one server fail, the remaining servers will automatically recover.

Simple, Easy Installation and Rollout

Regardless of enforcement method, Sentriant AG200 offers a range of enforcement levels from passive monitoring (no enforcement) to strict enforcement where non-compliant endpoints are quarantined immediately. These graduated enforcement levels can be can be configured globally or on a per-policy basis. This level of flexibility allows Sentriant AG200 to be rolled out gradually into a network in a controlled manner to minimize impact to IT staff and end-users.

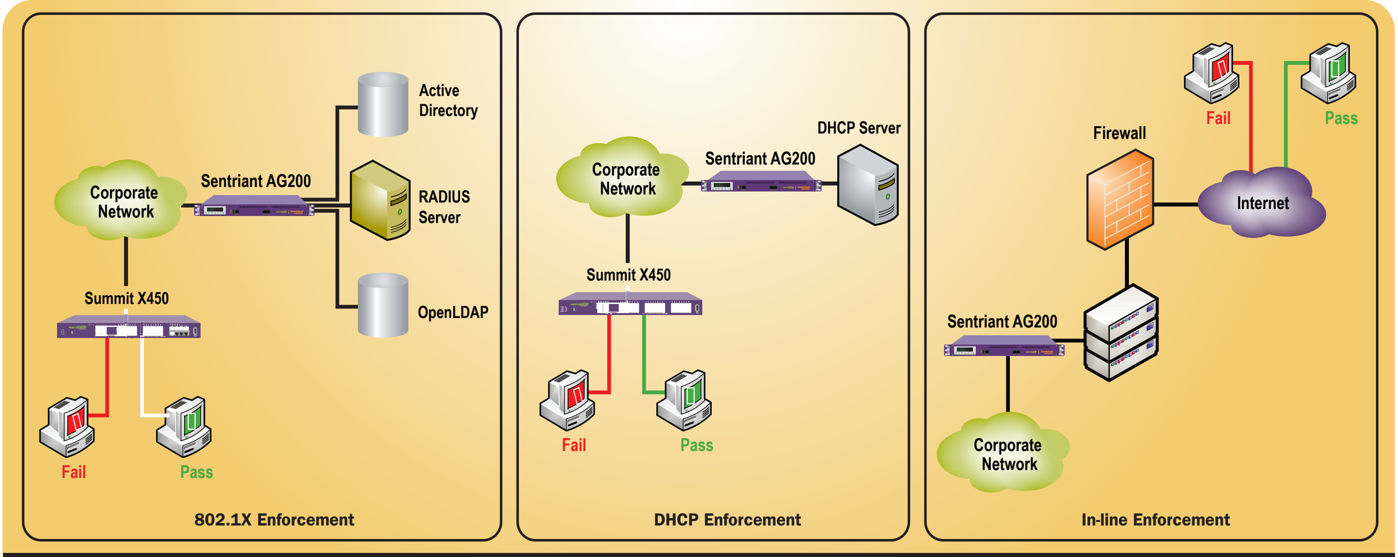

Figure 2: Enforcement Options

Enterprise-Class Management and Administration

Sentriant AG200 offers a complete set of management capabilities in order for it to operate seamlessly in any IT environment.

Centralized Management

Sentriant AG200 consolidates all NAC operations within a centralized web-based console providing a single pane view for monitoring and controlling all aspects of the solution. When administrators first login to the console they are immediately presented with a high level dashboard, alerting them to the number of endpoints that have failed testing and been quarantined, the "Top 5" most frequently failed integrity tests, and an overview of all server health information. From the dashboard, administrators can drill down in any area to obtain more detailed information. For any endpoint, administrators can see which tests passed or failed and perform a manual override to force a retest, quarantine or allow access for the device. The console also allows access policies and all other aspects of system configuration to be managed globally and pushed down to individual servers or clusters of servers with the click of a button.

Multi-User, Role-Based Administration

Sentriant AG200 provides tailored access to the management console based on user and role. This provides for shared administrative use across the organization allowing multiple IT or security groups to utilize aspects of the NAC solution (see Figure 3). For example, IT Help Desk users can access information on why a particular endpoint device has been quarantined but cannot change any configuration or policy settings. Administrative roles can also be defined on a per-server or per-cluster basis causing an administrator to just see the servers or endpoints in the region of the network they are responsible for managing. Out-of-the-box Sentriant AG200 is pre-configured with the following administrative roles and additional roles can be created as needed:

- System Administrator
- Cluster Administrator
- Help Desk Technician
- View-Only User

Powerful Reporting Capabilities

The robust reporting capabilities of Sentriant AG200 are useful for auditors, managers and IT staff and can server as proof that access policies are actually being enforced to meet compliance needs. Sentriant AG200 offers the following standard reports:

- Endpoint List
- Policy Results
- Test Results
- Test Details

These reports can be further refined by date, by server/cluster, by endpoint (IP/MAC) or using other supported search criteria. For advanced reporting needs Sentriant AG200 provides a documented SQL interface to allow third-party reporting packages to extract all endpoint compliance data from Sentriant AG200.

Enterprise Integration Framework

Sentriant AG200 includes a rich set of APIs for the import and export of data to and from the management server. This allows Sentriant AG200 to be tightly integrated with existing IT systems and processes. For instance, the framework allows Sentriant AG200 to share endpoint security and compliance data with other IT systems such as SIM/SEM products or trouble ticketing systems. It also allows third-party systems, such as a network IDS/IPS, to control Sentriant AG200 functions, such as testing and quarantining (see Figure 4).

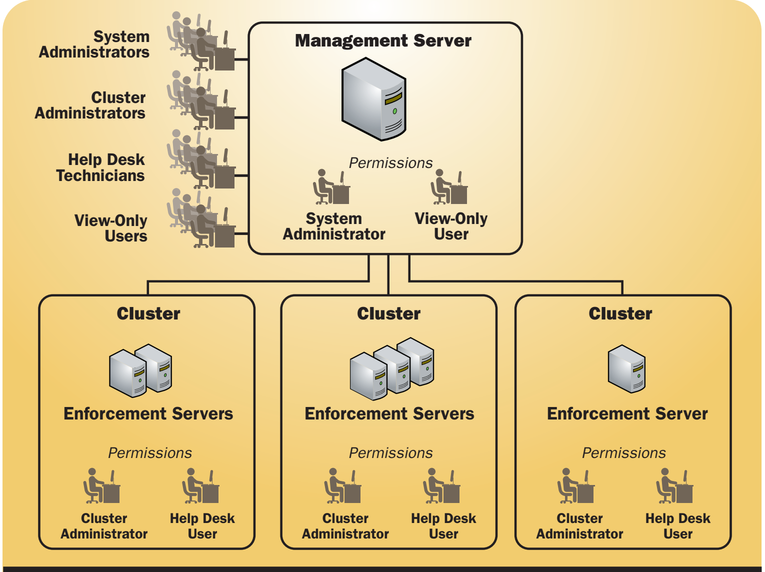

Figure 3: Multi-User Role-Based Administration

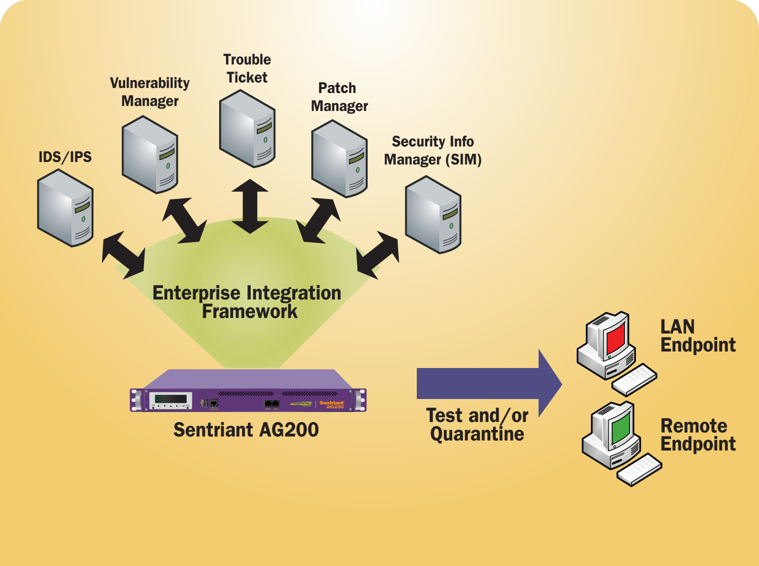

Figure 4: Enterprise Integration Framework

Technical Specifications

Performance

Number of endpoints per Management/Enforcement combination appliance	1,500
Number of endpoints per Enforcement server	3,000
Maximum number of Enforcement servers per Management server	10
Maximum number of Enforcement servers in a cluster	5

Appliance Internals

Processor	Intel® Core™ 2 Duo (1.86GHz)
Memory	2 GB RAM
Hard Drive	160 GB SATA
Network Interfaces	2 10/100/100 Ethernet ports LAN bypass switch
Nominal Power Rating	Nominal Input: 100-240V; 1.0A Voltage Range: 90-264V~ Frequency Range: 47-63 Hz Power (max): 250W Input Connector: IEC 60320 C14 Heat (max): 850 BTU/hr In-rush Current: 40A
Console access	Serial RJ-45 Connector

Chassis

Height	1RU (1.75 inches)
Depth	17.0 inches
Width	17.1 inches
Mounting	Bracket-based front mount
Certifications	UL 6950-1–IEC 6950-1 (U.S./Canada/Europe) FCC Part15/ISES003 Class A Emissions (U.S./Canada) CE (European Union) VCCI Class 1 ITE (Japan)

Sentriant AG Management System

Any workstation running Firefox 1.6 or higher; Mozilla 1.7 or higher; or Internet Explorer 6.0 or higher

Technical Specifications

Endpoint Support

Operating Systems

	Testing Method		
	Agent	**Agent-less**	**ActiveX**
Windows 2000	Yes	Yes	Yes
Windows XP Professional	Yes	Yes	Yes
Windows XP Home	Yes	No	Yes
Windows Server 2000, 2003	Yes	Yes	Yes
Vista Ultimate	Yes	Yes	Yes
Vista Home Basic	Yes	No	Yes
Vista Home Premium	Yes	No	Yes
Vista Business	Yes	Yes	Yes
Vista Enterprise	Yes	Yes	Yes
Mac OS X (10.3.7 or later)	Yes	No	No

Languages

- English
- German
- French
- Spanish
- Italian
- Dutch
- Danish
- Portuguese
- Swedish
- Norwegian
- Finnish
- Polish
- Russian
- Czech

For each supported language, all Operating System (OS) related integrity tests have been certified against the localized version of the OS and all third-party software related integrity tests (anti-virus, anti-spyware, personal firewalls, Peer-to-Peer (P2P)) have been certified against the language specific version of the software, if one exists.

Technical Specifications

Standard Endpoint Tests that Ship with Sentriant AG200:

Operating Systems—Windows

- Windows 2000 hotfixes
- Windows Server 2003 hotfixes
- Windows Server 2003 SP1 hotfixes
- Windows Server 2003 SP2 hotfixes
- Windows XP hotfixes
- Windows XP SP2 hotfixes
- Windows Vista hotfixes
- IIS hotfixes
- Internet Exporer hotfixes
- Office hotfixes
- Microsoft applications hotfixes
- Microsoft servers hotfixes
- Microsoft tools hotfixes
- Service Packs
- Windows automatic updates

Browser Security Policy—Windows

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

Security Settings—Windows

- MS Excel macros
- MS Outlook macros
- MS Word macros
- Services not allowed
- Services required
- Windows Bridge Network Connection
- Wireless Network Connections
- Windows Wireless Network SSID Connections
- Allowed Networks
- Windows security policy
- Windows startup registry entries allowed

Security Settings—OS X

- Airport Preference
- Airport User Prompt
- Airport WEP Enabled
- Bluetooth
- Internet Sharing
- Services
- Firewall
- QuickTime Updates
- Security Updates

Anti-Virus Software—Windows

- Avast 4 Professional Edition
- Avast 4 Professional Edition
- AVG AntiVirus Free Ed
- BitDefender AntiVirus / Internet Security v10
- BitDefender Enterprise Manager
- BitDefender AntiVirus for Windows Servers
- ClamWin Free AntiVirus
- Computer Associates eTrust AntiVirus
- Computer Associates eTrust EZ AntiVirus
- F-Secure AntiVirus
- Kaspersky Internet Security/AntiVirus 6.0
- Computer Associates eTrust EZ AntiVirus
- Kaspersky AntiVirus for FileServers
- Kaspersky AntiVirus for Workstations
- McAfee VirusScan
- McAfee Enterprise VirusScan 7.1.0, 8.0i, 8.5i
- McAfee Internet Security Suite 8.0
- McAfee Internet Security Suite 2007/Total Protection
- McAfee Managed VirusScan
- NOD32 AntiVirus 2.7, 3.0
- Norton AntiVirus 2004, 2007, 2008
- Norton Internet Security 2007, 2008
- Panda Internet Security
- Sophos Anti-Virus 6.5, 7.0
- Symantec Corporate AntiVirus
- Trend Micro AntiVirus
- Trend Micro OfficeScan Corporate Edition
- ZoneAlarm Security Suite
- Windows OneCare

Anti-Spyware Software

- Ad-Aware 2007
- Ad-Aware SE Personal
- Ad-Aware Plus
- Ad-Aware Professional
- McAfee AntiSpyware
- CounterSpy 1.0, 2.1
- Microsoft OneCare Anti-Spyware
- McAfee Anti-Spyware
- PestPatrol
- PestPatrol ITM bundle
- Shavlik NetChk 5.8, 5.9
- Spyware Eliminator
- Webroot Spy Sweeper
- Windows Defender

Personal Firewalls

- AOL Security Edition
- ISS Black ICE PC Protection
- Comodo Firewall
- Computer Associates EZ Firewall
- F-Secure Personal Firewall
- Internet Connection Firewall (Pre XP SP2)
- McAfee Personal Firewall
- Microsoft OneCare Firewall
- Norton Personal Firewall / Internet Security
- Norton Internet Security 2007
- Senforce Advanced Firewall
- Sophos Client Firewall
- Sygate Personal Firewall
- Symantec Client Firewall
- Tiny Personal Firewall
- Trend Micro Personal Firewall
- Windows Firewall
- ZoneAlarm Personal Firewall

Software not allowed

- Administrator defined

Software required

- Administrator defined

P2P

- AIM
- Altnet
- 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
- savIRC
- Skype
- Trillian
- Turbo IRC
- Visual IRC
- Xfire
- Yahoo Messenger
- Windows Messenger

Spyware, worms, viruses, and trojans

- CME-24
- Keylogger.Stawin
- Trojans.Mitglieder.C
- VBS.Shania
- W32.Beagle.A
- W32.Beagle.AB
- W32.Beagle.AG
- W32.Beagle.B
- W32.Beagle.E
- W32.Beagle.J
- W32.Beagle.K
- W32.Beagle.M
- W32.Beagle.U
- W32.Blaster.K.Worm
- W32.Blaster.Worm
- W32.DoomHunter
- W32.Dumaru.AD
- W32.Dumaru.AH
- W32.Esbot.A.1
- W32.Esbot.A.2
- W32.Esbot.A.3
- W32.Galil.F
- W32.HLLWAnig
- W32.HLLW.Cult.M
- W32.HLLW.Deadhat
- W32.HLLW.Deadhat.B
- W32.HLLW.Doomjuice
- W32.HLLW.Doomjuice.B
- W32.HLLW.Lovegate
- W32.Hiton
- W32.IRCBot.C
- W32.Kifer
- W32.Klez.H
- W32.Klez.gen
- W32.Korgo.G
- W32.Mimail.Q
- W32.Mimail.S
- W32.Mimail.T
- W32.Mydoom.A
- W32.Mydoom.AX
- W32.Mydoom.AX-1
- W32.Mydoom.B
- W32.Mydoom.M
- W32.Mydoom.Q
- 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
- W32.Sober.0
- W32.Sober.Z
- W32.Welchia.Worm
- W32.Zotob.E
- And more…

Technical Specifications

Ordering Information

Part Number	Name	Description
72002	Sentriant AG200 Management Server w/100 endpoints	Sentriant AG200 Management Server with 100 endpoint licenses included. 1U appliance with 2x10/100/1,000 ports (integrated bypass switch), mounting brackets, AC PSU and US power cord. Supports deployment as a dedicate server for managing for one or more Enforcement Servers or as a standalone server with integrated enforcement capabilities. Service contract required.
72006	Sentriant AG200 Enforcement Server	Sentriant AG200 Enforcement Server. 1U appliance with 2x10/100/1,000 ports (integrated bypass switch), mounting brackets, AC PSU and US power cord. Service contract required.
72025	Sentriant AG200 add endpoint, 100-250 endpoints	Sentriant AG200 additional endpoint license for orders between 100 – 250 endpoints (100 minimum). Round up to the nearest 50. Service contract required.
72050	Sentriant AG200 add endpoint, 251-500 endpoints	Sentriant AG200 additional endpoint license for orders between 251 – 500 endpoints. Round up to the nearest 50. Service contract required.
72100	Sentriant AG add endpoint, 501-1,000 endpoints	Sentriant AG200 additional endpoint license for orders between 501 – 1,000 endpoints. Round up to the nearest 50. Service contract required.
72125	Sentriant AG200 add endpoint, 1001-2500 endpoints	Sentriant AG200 additional endpoint license for orders between 1,001 – 2,500 endpoints. Round up to the nearest 50. Service contract required.
72150	Sentriant AG200 add endpoint, 2,501-10,000 endpoints	Sentriant AG200 additional endpoint license for orders between 2,501 – 10,000 endpoints. Round up to the nearest 50. Service contract required.
72200	Sentriant AG200 add endpoint, over 10,000 endpoints	Sentriant AG200 additional endpoint license for orders over 10,000 endpoints. Round up to the nearest 50. Service contract required.
90535		Onsite Installation for Sentriant AG

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