Sentriant® AG200

Sentriant AG200 protects the network by only allowing access for endpoint devices that are free from threats and meet IT security policies.

Features

- Advanced endpoint integrity testing—Sentriant AG200 tests each endpoint as it connects to the network to verify that it meets the organization's security policy before allowing access
- Flexible deployment options—Sentriant AG200 supports several enforcement schemes for easy integration with any network infrastructure without costly network upgrades
- Enterprise-class management and administration—Sentriant AG200 combines centralized system management with multi-user, role-based administration to minimize operational complexity for even the largest networks

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

Most IT organizations have experienced the pain and financial impact of network compromises originated via endpoint devices. 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 traditional endpoint security measures are important, they are not sufficient to protect the network from attack. 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 issues have historically been beyond the control of IT administrators.

Sentriant AG200 is the next generation in endpoint security appliances that lets administrators regain control by verifying that endpoint devices meet security policy requirements and do not introduce worms, Trojans or spyware into an organization's network. Sentriant AG200 automatically tests the health of each device, both managed and unmanaged, to verify it meets the organization's security requirements before allowing access to the network. This proactive approach to managing network access greatly reduces the risk posed by non-compliant or infected devices, without the cost or overhead of manual approaches.

Advanced Endpoint Integrity Testing

Using Sentriant AG200, administrators create access policies that define the minimum required security level for endpoint devices. These policies consist of one or more integrity checks to assess whether key operating system 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 or other potentially dangerous applications such as peer-to-peer file sharing. Sentriant AG200 ships with a wide selection of in-the-box tests that are continuously updated as new threats emerge, and offers the ability for administrators to create custom tests required in their environment.

When a device connects to the network, Sentriant AG200 quickly tests the device to determine its security level and quarantines devices that are not compliant. A non-compliant endpoint can be automatically remediated through integration with leading patch management systems or via end user self-remediation. Once repaired, devices are allowed access to the network (see Figure 1) where they will be periodically re-tested to verify ongoing policy compliance.

Sentriant AG200 supports both Microsoft Windows and Mac OS X endpoint devices and provides three options for assessing endpoint integrity:

1. Agent-less—No client-side agent required on endpoint
2. ActiveX Plug-in—Tests endpoint through web browser
3. Sentriant AG Agent—Tests endpoint through installed client

All three support the same depth of testing providing a consistent level of security protection regardless of the option selected.

Flexible Deployment Options

Unlike solutions that only function in specific network environments and architectures, Sentriant AG200 works with any IP infrastructure. Sentriant AG200 provides multiple enforcement options such as:

- 802.1X Enforcement
- DHCP Enforcement
- Inline Enforcement

for quarantining endpoints, ensuring all network entry points (LAN, WLAN, VPN) are properly guarded without requiring expensive upgrades or changes.

A single Sentriant AG200 appliance can be used to test up to 1,500 endpoints and multiple appliances (Management and Enforcement Servers) can be used to cover large, multi-site environments consisting of tens of thousands of devices. Sentriant AG200 Enforcement Servers can also be grouped in clusters for high availability and load balancing.

Enterprise-class Management and Administration

Even in a multi-appliance deployment, all management functions are consolidated within a centralized web-based console making the system easy to operate.

Multi-user, role-based access to the management console allows shared administrative use among multiple groups in accordance with staff responsibilities. 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. Out-of-the-box Sentriant AG200 is pre-configured with the following administrative roles:

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

Additional administrative roles may be created based on fine-grained permissions or based on an administrator's need to manage only a certain set of servers or endpoints.

The robust reporting capabilities of Sentriant AG200 allow you to meet the needs of auditors, managers and IT staff. Reports provide concise security status information on device compliance and access activity. For advanced management needs, Sentriant AG200 provides a rich set of APIs for integration with third-party IT systems.

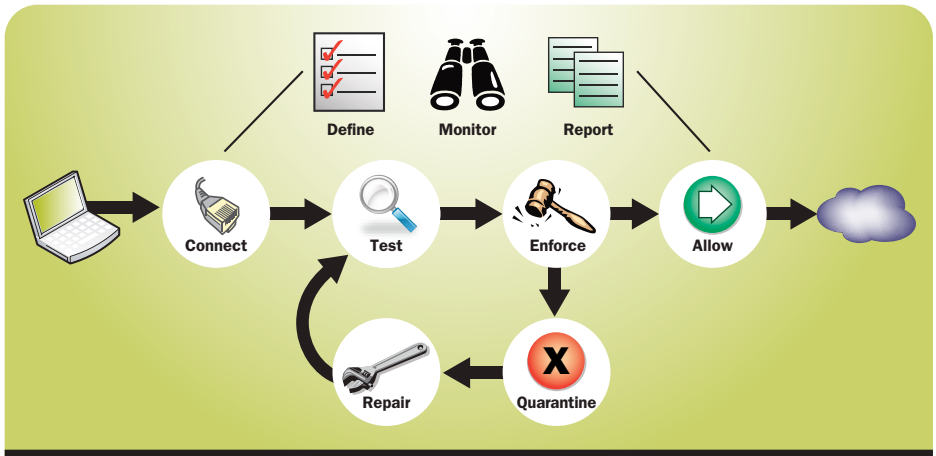

Figure 1: Sentriant AG200 Process

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