ConSentry Endpoint Posture Validation

PERMANENT AND DISSOLVABLE AGENTS FOR SCANNING ENDPOINTS

ConSentry Networks delivers intelligent control at the LAN edge, making it easy for IT to control users, devices, and applications in the LAN. The company's LANShield Controllers and Switches monitor all traffic coming onto the LAN and control what users can do on the network. ConSentry's endpoint posture validation (EPV) software is a key piece of protecting LAN access, providing a complete PC health check to ensure that only compliant machines are admitted onto the network. With a permanent agent for managed devices and a dissolvable agent for guest machines, the software also features automatic remediation to simplify IT's job in getting devices compliant with endpoint security policy.

COMPREHENSIVE HEALTH CHECK AND ACCESS CONTROL

Business productivity depends on network connectivity, including for guests, contractors, partners, and other people outside the organization. However, allowing unhealthy PCs and personal devices onto the LAN risks the loss of intellectual property due to Trojan infections and increased network downtime due to the spread of malware. Out-of-date operating system (OS) patches, out-of-date anti-virus or anti-spyware definitions, or improper firewall settings can all increase vulnerability to these worms and Trojan infections. ConSentry Networks' EPV software ensures that only healthy desktop and laptop PCs connect to the network. ConSentry EPV offers a full range of posture check deployment options and verification steps for both managed and unmanaged PCs. The EPV engine and enforcement point is built into the ConSentry LANShield Controllers and Switches, giving IT a turnkey posture check solution with no dependency on additional software or authentication websites and no need to reconfigure the network.

For managed machines, ConSentry provides the EPV permanent agent, which is installed on a user's system. To support the unmanaged machines belonging to guests, contractors, or employees' or partners' personal devices, ConSentry offers a dissolvable version of the EPV agent, which downloads via a web browser. Both agents run a customized scan periodically and report their status to the InSight Command Center, ConSentry's policy management and activity monitoring platform. If the agent reports an unhealthy condition, the ConSentry switch or controller can quarantine or simply warn the user, based on IT preference. In many cases the auto-remediation feature will quickly and automatically correct the problem. In other cases, IT can include customized messages to inform users about the status of their posture check.

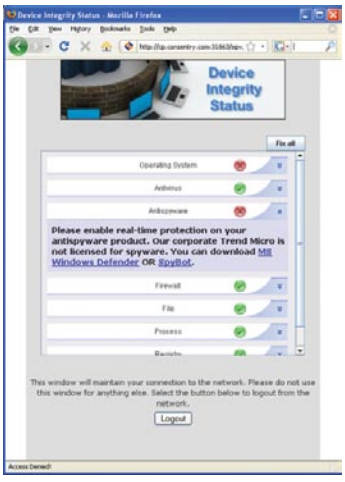
ConSentry EPV software determines the health of the user's PC by examining the status of the following client software:

- Anti-virus
- Anti-spyware
- Firewall
- Operating system types
- OS patches
- Files
- Running processes
- Registry
- Health agents

ENFORCEMENT ACTIONS AND POST-ADMISSION CONTROL

Completely programmable, the ConSentry EPV solution allows IT to establish scanning policy as to which software systems the agent should check. If the health scan of a machine does not find

CONSENTRY EPV AGENT AT-A-GLANCE



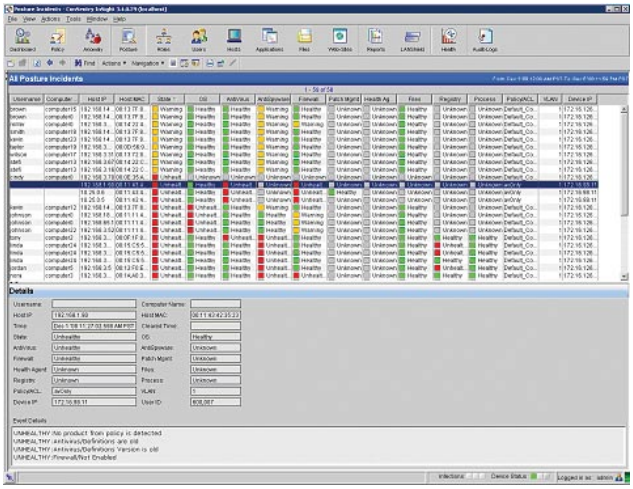
- Available as a permanent agent or Java dissolvable agent in web browser
- Both agents offer identical functionality
- Display text and company logo easily configurable by IT staff
- Customizable privacy consent page can be sent to user prior to scan
- Comprehensive scanning of device integrity applications
- Auto-remediation of faults by invoking third-party components for updates
- Customizable warning messages and clickable URLs including international language and Unicode font support

any issues, the ConSentry switch or controller will grant the user access to network resources as defined for the user's role. If the health check indicates a faulty status, such as anti-virus software not installed or not up to date, the agent will take one of the following steps as configured by IT:

- Restrict the device – the agent does not allow the user onto the LAN until the endpoint is in compliance. A special quarantine policy allows the device to access remediation servers.
- Warn the user – the agent alerts the user to the improper setting but allows the user to enter the LAN
- Allow the user – the agent allows compliant endpoints directly onto the LAN

In addition to checking anti-virus software status, the EPV agent can check that personal firewalls are enabled, the latest Windows operating system patches are installed, company-specific entries in the Windows Registry remain in tact, or specific files are running on a device. Once a user is admitted to the network, ConSentry's user and application control capabilities limit access to those data and application resources IT has allowed for the user's role in the organization. ConSentry LANShield technology provides wire-speed, inline visualization and logging of every data flow from every user on the network, enabling enforcement, simplifying troubleshooting, and providing complete audit trails required for compliance.

SIMPLE, CENTRALIZED MANAGEMENT



ConSentry InSight Command Center provides a single focal point for administering and monitoring EPV policies and events that may be operating on multiple ConSentry LANShield Switches and Controllers, increasing IT's efficiency and lowering its OPEX. IT can use InSight to create and distribute global policies defining PC health criteria, quarantine policies, remediation steps, and warning messages.

Simple, easy-to-read global reports summarize the health of all managed and unmanaged machines on the network whether connected wired or wirelessly. The "Posture Incident" dashboard identifies unhealthy machines by user identity as well as IP and MAC addresses, and it indicates the status of each security component to speed troubleshooting.

CONSENTRY EPV FEATURE SUMMARY

PERMANENT AGENT

Users or IT can download the ConSentry EPV permanent agent onto machines owned and managed by the organization. An icon in the PC taskbar indicates that the agent is present and operational.

DISSOLVABLE AGENT

To support guest access to the network for PCs not managed by the organization, the ConSentry dissolvable agent downloads automatically when users launch an Internet browser. The agent periodically scans the PC while the user is logged onto the network. When the browser is closed, the agent expires.

ROLE-BASED SCAN POLICIES

The ConSentry solution allows IT to establish different scan policies depending on the role of the user or device. For example, guest machines can undergo a different set of scan criteria than employees, and executives might have yet another scan policy. IT can configure the EPV policy to avoid scanning printers and other network-attached peripherals.

SUPPORTED OPERATING SYSTEMS AND CLIENTS

The ConSentry EPV agents are available for Windows, Mac, and Linux operating systems. A comprehensive list of third-party security clients is supported for each OS including all major anti-virus, anti-spyware, and firewall applications.

OS PATCH LEVELS

The ConSentry EPV feature not only will verify an acceptable OS version but also can ensure that patches have been installed to meet a prescribed revision level. Many popular patch vendors are supported, including generic Microsoft WSUS and SMS.

AUTO-REMEDIATION

If an application component fails to meet the standard specified by IT, the user may simply be warned or denied access to the network. With one mouse click, the user can direct the EPV application to initiate remediation of the failed components.

CONFIGURABLE ENFORCEMENT

IT can establish and configure the policy for users in response to scan failures – allow, warn, deny – through the InSight Command Center EPV configuration module. Policy definitions are automatically distributed to every ConSentry switch or controller in the network from one InSight console. All components of the EPV scanning and decision process are integrated into the LANShield devices with no external dependencies.

CUSTOMIZED WARNING MESSAGES

The EPV application may be customized by IT to include a company logo as well as customized notifications and warning messages to the user. Messages may include URLs for additional instructions and can be programmed to appear in international languages including those requiring Unicode font support.

Corporate Headquarters
ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035

Phone 408.956.2100
Fax 408.956.2199
Toll-Free 866.841.9100
Email info@consentry.com
www.consentry.com

For a complete listing of all our office locations go to:
www.consentry.com/company.html

LIT# EPV-DS-0209