

AEP Netilla Security Platform

Client Integrity - Enforcing Corporate Policy

Ensuring that application resources are available – from any location, at any time – has become a fundamental requirement of doing business. Yet opening up your network for access from various locations – which are outside of your IT department’s control – creates new risks of digital leakage and endpoint dangers.



That’s why the AEP Netilla Security Platform offers a deeply integrated endpoint security solution, ensuring that remote PCs adhere to corporate security policy before they gain access to your network, eliminating remote access threats and providing a true end-to-end security solution.

AEP Client Integrity Feature Overview

Feature	Description	Benefit
Host Integrity Checking by V-Realm	Validates the presence and version of antivirus software, personal firewalls, service packs, patch levels, and custom objects.	Ensures compliancy with corporate policy.
Adaptive Policies by V-Realm	Checks pre-defined end station parameters (e.g., registry entry/IP address).	Confirms the identity/location of remote devices.
Secure Desktop integration by V-Realm	Creates encrypted virtual workspace and performs DoD wipe at session end.	Prevents “digital leakage” and ensures the confidentiality of corporate information.
Cache Cleaning by V-Realm	Deletes all traces of session data (e.g., browser history, cache, etc.)	Removes the danger of sensitive data being left behind at remote locations.
Self Remediation	AEP Client Integrity allows administrators the ability to redirect non-compliant users to resources where they can self-heal their devices to attain compliancy.	Eliminates help desk intervention.
Additional Endpoint Security Tools Provided by the NSP include:		
Inactivity Timeout	Monitors keyboard/mouse activity and ends session after configurable timeout period.	Prevents data leakage due to open sessions.
Periodic Re-authentication	NSP can also force periodic re-entry of access credentials	Prevents data theft by terminating unattended sessions
Client Machine Identification Authentication	Creates a unique profile (based upon CPU, memory, network card addresses and other information) to uniquely identify a specific corporate-issued computer.	Iron-clad method to limit access to pre-approved devices.

Feature Description Detail

Cache Cleaning and Secure Desktop

A critical function required of a Client Integrity solution, especially in the case of corporate data access from non-corporate devices (Kiosks etc.), is that no trace of the session be left behind on that device, thus preventing data appropriation for malicious purposes.

Upon a session’s termination, as much information as possible regarding that session should be erased from the end station. The events that trigger data removal are: User

Logoff, System Shutdown, Inactivity Timeout and Secure Desktop closure.

The AEP NSP has two features that provide different levels of security with regards to the removal of session data. These are Cache Cleaner and Secure Desktop.

Cache Cleaner (CC)

The CC feature performs a standard “Delete” of session data upon session termination. Data deleted includes browser cache (temporary internet files) and browser history.

Secure Desktop (SD)

The SD feature opens a “virtual” workspace on the end station after authentication. A window opens automatically in this workspace displaying the familiar authenticated user “web top”. Without the SD feature, session data would be stored in the normal locations for each of the applications in use, resulting in data being recorded in various files on the disk. However, in the SD environment, all data is stored in a single, encrypted “vault” on the hard drive.

On session termination this file is deleted and a Department of Defense (DoD) standard of “wipe” is performed on the disk area where the file was located, making recovery of deleted data almost impossible.

As a configurable option, if the SD is unable to install itself on the end station, it will attempt to install the CC component as a fallback. This is done to ensure that at least some measure of data removal is carried out. If this option is not required, then CC should not be enabled for that V-Realm.

Secure Desktop offers a number of configurable policy options, including:

- Enable/disable the use of removable drives
- Enabled/disable printing
- Enable/disable switching desktops

Host Integrity (HI)

The HI feature enables the administrator to enforce corporate policy by determining which software components are running on the end station before authorization is granted. Checks can be made for the market-leading Personal Firewall (PFW) and Anti Virus (AV) packages, as well as the Patch level of the OS. Custom rules can also be written to check for other components not explicitly listed. Not only can checks be made to ensure that these components are running, but also that the signature files are recent enough to satisfy corporate policy.

Additionally, Host Integrity can be applied on a polling basis; this means that the Integrity checking continues throughout the life of the session and will detect situations where firewall or AntiVirus software has been disabled.

Adaptive Policies (AP)

The AP feature provides many options to assist in the identification of the end station itself and also where that end station might be connecting from. This is done by facilitating checks for specific details such as Source IP address, Registry entries and host name.

Idle Timeout

Idle Timeout allows you to specify whether client PCs should be disconnected from the NSP after an amount of inactivity that you specify. The Idle Timeout feature is based on mouse and key stroke activity. Note that if there’s a large file transfer or print job and no other mouse or keyboard activity, then the inactivity timer remains in effect.

Periodic Re-authentication

Periodic re-authentication is an admin-defined feature that is used to force a user to re-enter their access credentials after an admin-defined time period. A re-authentication timer is displayed on the user’s NSP webtop indicating the amount of time left for the next re-authentication challenge (as shown).

Users are able to re-authenticate at any time during the session simply by clicking the link and entering their credentials. At this point, the timer countdown resets to the original time period.

Client Machine Identification (CMID) Authentication

CMID authentication is ideal for organizations that would like to limit access to corporate-issued computers. When enabled, the NSP takes a “snapshot” of an incoming PC according to a series of admin-defined parameters (MAC address, registry entries, service packs, and a wide range of other options). These unique identifiers are then stored in a secure hash which is meaningful only to the NSP itself. Every time the user attempts to login to the NSP, the appliance first confirms that they are accessing from an approved appliance, and allows or denies access accordingly.

Configuration By V-Realm!

All components are configured on a per V-Realm basis, providing an organization with a powerful tool to enforce policy on different sets of users. Any combinations of components are configurable for each V-Realm.

Self-Remediation

Should an end station fail to comply with the policies configured, its browser will be redirected to an admin-configurable URL results page. This URL can include instructions to bring the end station in line with corporate policy.

Additionally, NSP administrators can redirect non-compliant – thus, “riskier” - users directly into V-Realm landing pages that provide access to fewer application resources, as befitting their less secure status.

Minimum System Requirements - Detail

On-Demand Manager

To run the On-Demand Manager, a Windows 2000, Windows XP workstation, or a Windows Server 2003 meeting at least the following specifications will be required:

- Pentium 633MHz or faster
- 128 MB RAM
- 10 MB available hard disk space
- Java Runtime Environment (JRE) version 1.4.2 or later.

Secure Desktop

- Pentium 633MHz or faster
- 128 MB RAM
- 25 MB available hard disk space
- Windows 2000 Pro, Windows 2000 Server, Windows Server 2003, Windows XP, Windows NT4 (SP6)
- Browser: Internet Explorer 6.0 and later, Netscape 6.0, 7.0, Mozilla 1.7 or higher, Sun Java Runtime Environment (JRE) version 1.4 or later, or Microsoft JVM

Host Integrity / Adaptive Policy

- Windows 98, Me, NT4 (SP6), Server 2003, 2000, XP
- Java Runtime Environment (JRE) version 1.4 or later or Microsoft JVM

Cache Cleaner

For Windows:

- Pentium 633MHz or faster
- 128 MB RAM
- 1 MB available hard disk space
- Windows 98, Windows Me: 64 MB RAM, or Windows NT4 (SP6), Windows Server 2003, Windows 2000, Windows XP
- Browser: Internet Explorer 6.0 and later, Netscape 6.0, 7.0, Mozilla 1.7. Sun Java Runtime Environment (JRE) version 1.4 or later or Microsoft JVM

For Linux (Thin and Web only)

- Pentium 633MHz or faster
- 128 MB RAM
- 1 MB available hard disk space
- Red Hat Linux 9.0 or later
- Browser: Mozilla 1.4 or later. Sun Java Runtime Environment (JRE) version 1.4 or later.

Contact AEP Networks

- www.aepnetworks.com
- info@aepnetwork.com

© AEP Networks, Inc. All rights reserved. AEP Networks and the AEP Networks logo are trademarks of AEP Networks, Inc., with registration pending in the United States. Netilla, SmartGate, SmartPass and SmartAdmin are registered trademarks of AEP Networks, Inc. All other trademarks or registered trademarks contained herein are the property of their respective owners.