

StillSecure® Safe Access™

Protecting your network through endpoint security compliance

Datasheet

StillSecure® Safe Access™ protects the network by ensuring endpoint devices are free from threats and in compliance with IT security policies before they are allowed on the network. An award-winning access control solution, Safe Access protects the network from the damage a single compromised or infected endpoint can unleash.

With multiple, flexible testing and enforcement options, Safe Access integrates seamlessly into virtually any network environment (figure 1, below). Safe Access controls network access for the full range of user types including trusted and untrusted, foreign and internal, remote, and wireless endpoints.

Safe Access is a flexible, integratable solution, offering:

- Purpose-built network access control engine
- True agent-less endpoint testing option; no software installed on or downloaded to endpoint
- Multiple enforcement options: 802.1x, inline enforcement, DHCP, and enforcement through Cisco's NAC architecture
- Integration with the IT environment through the StillSecure Enterprise Integration Framework™
- Deep endpoint testing with hundreds of off-the-shelf tests
- Compatibility with heterogeneous network infrastructure; no hardware upgrades required
- Comprehensive coverage of user types – network users, visitors, partners, remote users, etc. (LAN, VPN, RAS, and WiFi connections)



Best Endpoint Security Solution 2006

SC Magazine



"Safe Access' three testing methods, overall flexibility, and solid default configuration settings make it a top choice..."

InfoWorld magazine

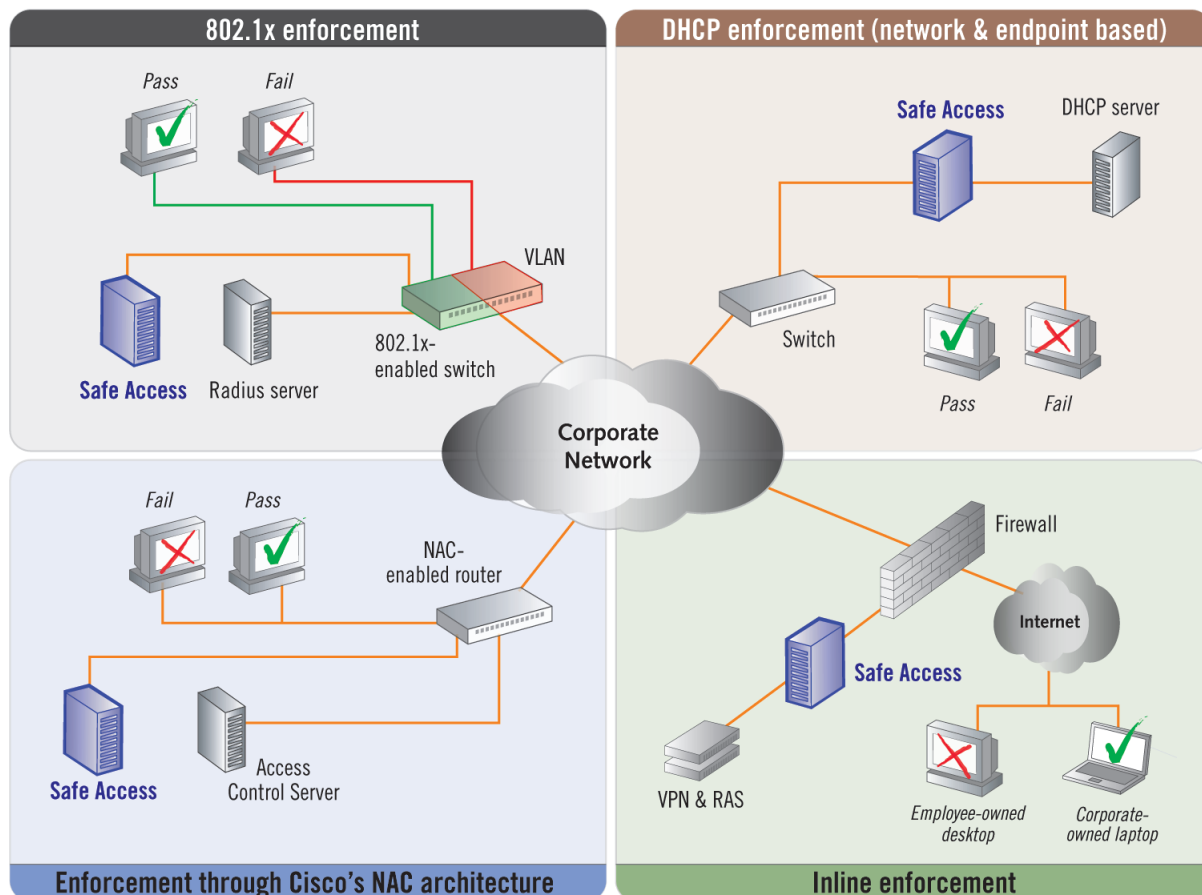


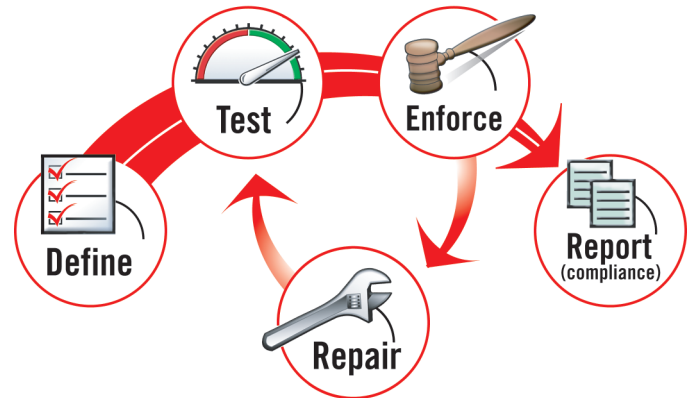
Figure 1. Safe Access offers four enforcement options that allow for seamless deployment on all network architectures. Endpoints that pass Safe Access testing are allowed onto the network; endpoints that fail are denied access or placed into quarantine, thereby protecting the network from the threats posed by non-compliant, non-secure devices.

How it works...

Using Safe Access, administrators create access policies that: (1) define which applications and services are permitted and (2) specify the actions to be taken when devices do not comply. Safe Access automatically applies access policies to devices as they log onto the network. It answers the question: Is it safe to give this device access?

Based on test results, devices are either permitted or denied network access or quarantined to a specific part of the network, thus enforcing organizational security standards. Enforcement can be accomplished through multiple methods as shown in Figure 1 (p.1).

Safe Access™ process



Access policy definition

Access policies consist of individual tests that evaluate the security posture of endpoint devices (PCs, laptops, PDA's, etc.).

- **Out-of-the-box access policies** – Pre-defined High, Medium, and Low access policies.
- **Custom access policies** – Any number of custom access policies easily created through point-and-click menu.
- **Standard tests** – Hundreds of standard tests included (see box on page 4).
- **Custom tests** – Custom tests created through Safe Access' application programming interface (API).
- **Automatic test updates** – Tests covering new threats downloaded automatically as frequently as hourly.
- **24x7 threat monitoring and test development** – Tests written and released by StillSecure Security Alert Team (SAT).



Endpoint testing

Safe Access automatically tests all devices attempting to access the network through LAN, RAS, VPN, or WiFi connections.

- **Purpose-built network access control engine** – Fast, scalable testing engine built specifically to determine security posture; not a re-purposed vulnerability scanner or personal firewall.
- **Agent-less testing option** – Testing accomplished without installing or downloading agent or client.
- **ActiveX and agent-based testing options** – Tests endpoints when agent-less testing is not feasible.
- **Rapid testing** – 3 to 10 seconds on a 100 Mbps network.
- **Robust device management** – Thousands of endpoints tested and managed simultaneously.
- **Continual testing while connected** – Retests devices on admin-defined interval to ensure compliance is maintained.



Compliance enforcement

Devices testing compliant are granted access. Non-compliant devices are either quarantined or are given a grace period of access.

- **Flexible enforcement options** – 802.1x enforcement, DHCP enforcement, inline enforcement, enforcement based on Cisco's NAC architecture.
- **Manual overrides** – Administrators may retest, quarantine, or grant access on demand.
- **Administrator notifications and alerts** – Based on testing and access activity.
- **Graduated enforcement** – Allows controlled system rollout.



Automated and manual repair

- **Automated remediation** – Integration with BigFix® and Microsoft® SMS natively supported; additional patch management integrations in development and available on request.
- **Self remediation** – Users notified of where their devices are deficient and provided with the remediation instructions.
- **Access 'grace period'** – Provides administrator-defined window of access (e.g., 3 days) to non-compliant machines to facilitate remediation.



Reporting for management and auditing/compliance

- **Concise security status information** – On device compliance and access activity.
- **Tailored reporting** – For auditors, managers, and IT staff members.
- **Report examples** – Device list, Actions taken, Access policy results, Test details, Test results, Test results by device, Test results by user, Test results by IP address, and more.

True agent-less endpoint testing

Safe Access offers multiple testing options, enabling the full range of endpoints to be assessed, regardless of connection methods and OS versions. Testing options include:

- **Agent-less testing** – No manually installed or downloaded client-side agent required on endpoint. Ideal for testing Windows 2000 and Windows XP Pro machines (both corporate-owned and foreign devices).

Safe Access agent-less testing option is truly agent-less—no code or ActiveX controls are installed. This simplifies administration and support, enables scalability, and allows for rapid deployment on both managed and foreign endpoints.

- **StillSecure agent** – Tests endpoint through downloadable persistent client. Tests all Microsoft-supported Windows OSs; ideal for internal legacy devices (e.g., Windows 98 or NT endpoints).
- **ActiveX plugin** – Tests endpoint through web browser. Tests all Microsoft supported Windows OSs and foreign endpoints where the installed agent is impractical.

Administrators prioritize the order that Safe Access applies testing options to endpoints as they initially connect to the network. Table 1 shows the recommended priority based on user type.


USER TYPE	Agent-less	StillSecure Agent	ActiveX
Internal corporate user (XP, 2000)	1	2	3
Internal corporate user (NT, 98 or lower)	NA	1	2
Non-corporate user (Remote user, visitor, contractor, etc)	1	3	2

Table 1. Recommended order of priority in which Safe Access testing methods are applied to endpoints. Priority is user-configurable in Safe Access.

Flexible enforcement for any network architecture

Safe Access supports a variety of enforcement methods that allow it to control network access regardless of architecture (see Figure 1, p.1):

- **802.1x enforcement** – Safe Access leverages 802.1x-compliant switches to control access, placing endpoints on the appropriate VLAN (quarantine VLAN, guest VLAN, production VLAN) based on test results.

- **Inline enforcement** – Safe Access sits inline acting as a layer 2 bridge. Ideal for controlling access through VPN, dial-up, and wireless networks.
- **DHCP enforcement** (network and endpoint based) — Controls access by assigning temporary IP addresses to devices being tested and devices that have failed tests. In the network-based option, enforcement occurs at the router. In the endpoint-based option, enforcement occurs through routing configurations on the endpoint, eliminating the need to re-configure infrastructure devices.
- **Enforcement through Cisco's NAC architecture***—Safe Access integrates with NAC-enabled components to control access at Cisco router. 

These enforcement options allow organizations to secure the network from all endpoints, regardless of the network topology, configuration, hardware, versioning, etc. All endpoint testing methods, discussed above, work seamlessly with all the enforcement methods.

*Safe Access v3.5 has tested compatible with Cisco's Network Admission Control Program, v.1. Operation with Windows 2003 server has not been certified. For disclaimer go to: www.stillsecure.com/disclaimer/nac.php.

Comprehensive test library, customizable access policies

Safe Access includes hundreds of off-the-shelf tests that fully assess endpoint security posture. Tests categories include:

- OS Service Packs and Hotfixes
- Browser and OS security settings
- Anti-virus, installed and up to date
- Personal firewall, installed and up to date
- Anti-spyware, installed and up to date
- Peer-to-peer applications (presence of)
- Worms, viruses, and Trojans (presence of)
- Required software, administrator defined
- Prohibited software, administrator defined

Specific tests within these categories are shown in the box on page 4.

Individual tests are combined into access policies. Safe Access ships with predefined access policies (High, Medium, and Low policies), and administrators may create any number of custom policies to meet specific business requirements (e.g., specific policies for visitors, home users, satellite offices, laptops in the field, etc.).

Integration for improved security, productivity, and efficiency

Safe Access includes the Enterprise Integration Framework™, an open architecture that allows for the import/export of data to/from Safe Access. Integration allows third-party systems to control Safe Access testing and quarantining functions, and it enables Safe Access to share endpoint security data with other IT systems, such as patch managers, intrusion detection/prevention systems (IDS/IPS), vulnerability managers, security information managers, third-party reporting tools, etc. (see Figure 2).

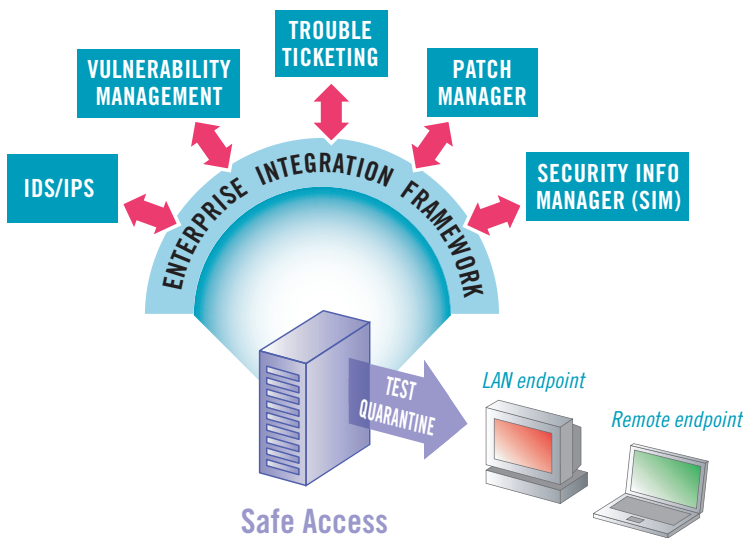


Figure 2. The Enterprise Integration Framework enables third-party systems to control Safe Access testing and quarantining functions and allows Safe Access to export endpoint compliance data.

For example, if your intrusion prevention system (IPS) detects attacks emanating from an endpoint, it could instruct Safe Access to immediately quarantine the device. Likewise, Safe Access can integrate with your trouble ticketing system, opening tickets for noncompliant endpoints.

Integration leverages Safe Access' quarantining and testing capabilities and the capabilities of the other security-related systems on your network, thereby enhancing security and improving productivity and efficiency.

Availability

Safe Access is available as software or as preconfigured hardware appliance.

We invite you to try a free demonstration. Contact 303-381-3830, sales@stillsecure.com, or visit www.stillsecure.com.

Standard tests that ship with Safe Access

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-spyware

Ad-Aware Plus
Ad-Aware Professional
CounterSpy
McAfee Anti-Spyware
Microsoft Windows Anti-Spyware
Pest Patrol
Spyware Eliminator

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.AB@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.Blastar.K.Worm
W32.Blastar.Worm
W32.Doomhunter
W32.Dumar.AD@mm
W32.Dumar.AH@mm
W32.Gali.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...