StillSecure® Safe Access™

Protecting your network through endpoint security compliance.

Features, functions, and benefits

Feature	Function	Benefit
Endpoint testing		
Purpose-built network access control engine	▪ Tests endpoints against security/access policies ▪ Enforces policy by denying, quarantining, or allowing access to endpoints based on test results ▪ Fast testing (approx. 3-15 seconds per device) and scalable	▪ Designed and developed specifically to determine security posture of endpoints and control access ▪ Not a re-purposed vulnerability scanner, personal firewall, or other re-packaged security solution ▪ No potential legal complications with usage (unlike Nessus-based NAC solutions) ▪ Meets enterprise-class requirements
Flexible testing, flexible enforcement	▪ Accommodates any network architecture ▪ Allows virtually all user types to be tested: -- LAN -- VPN -- RAS -- Wifi -- Internal/external -- trusted/untrusted -- managed/unmanaged	▪ Maximize control over endpoints connecting to network ▪ Minimizes administration and support requirements to protect the network from harmful endpoints
Multiple endpoint testing options	▪ Provide flexibility, maximum coverage in endpoint testing ▪ Three endpoint testing options: -- Agent-less -- Agent based (StillSecure agent) -- ActiveX	▪ Allows full range of endpoints to be tested ▪ Minimizes administration and support
Agent-less testing	Truly agent-less (or 'client-less'); tests devices without agent or ActiveX control	▪ Easily test unmanaged endpoints ▪ No client-side software installation ▪ Reduced or negligible help-desk calls ▪ Rapid deployment of Safe Access solution ▪ Eliminates possibility of impacting endpoint performance ▪ Reduced management overhead; no need to support thousands of agents on the network
Prioritized application of testing options	Enables administrators to specify the order in which testing methods are applied to endpoints upon initial connection attempt	▪ Tests devices with optimal testing method ▪ Maximizes the likelihood that devices will be tested
Continual device re-testing	Re-tests network-connected devices on administrator-specified interval (e.g., every 30 minutes)	Ensures endpoints maintain compliance while on the network
Out-of-the-box tests	Test devices for the full range of threats: ▪ 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 ▪ Spyware (presence of) ▪ Peer-to-peer (presence of) ▪ Worms, viruses, and Trojans (presence of) ▪ Required software, administrator defined ▪ Prohibited software, administrator defined	▪ Thoroughly assess endpoint security posture (not just patch level and anti-virus status) ▪ In-depth testing without requiring any custom test development ▪ Enables rapid deployment, rapid time to value
Custom tests	Allows users to easily create tests through open API	Test endpoints for organization-specific threats and concerns
Automatic test updates	Keeps test library up to date against recently identified threats in the wild	▪ No work required to stay current ▪ Assurance that tests are thoroughly QA'ed before release

Enforcement/quarantining		
Multiple enforcement/quarantining technologies	▪ Enforces endpoint security policies on any network architecture ▪ Enforcement options include: -- 802.1x enforcement -- Inline enforcement -- DHCP enforcement (network and endpoint based) -- Enforcement through Cisco's NAC architecture	▪ Provides flexibility in implementing enforcement regime ▪ All enforcement technologies work seamlessly with all testing options (described above) ▪ Maximizes control over endpoints connecting to network
Graduated enforcement	▪ Enables enforcement for non-compliant endpoints to be ratcheted up over time, from admin notifications to full quarantining ▪ Provides flexibility in implementing enforcement regime	Allows a controlled, methodical rollout of the Safe Access solution
Per test enforcement settings	Four enforcement options available for failed test: ▪ Send email notification to administrator ▪ Quarantine access immediately ▪ Grant temporary access for x days ▪ Initiate patch management activities	▪ Provides flexible control over enforcement process ▪ Enables enforcement commensurate with level of threat
Accessible services and devices list	Allows administrators to specify devices and services that are accessible to endpoints that fail compliance testing	Gives end users access to resources required for remediating noncompliant machines
Access policies		
Access grace period	Provides network access to noncompliant devices for admin-defined window (e.g., 3 days)	▪ Enables self remediation ▪ Does not disrupt flow of business ▪ Reduces support calls
Pre-defined access policies	Versatile access polices (High, Medium, Low security policies) available out of the box	Allows rapid implementation of Safe Access solution
Custom access policies	Allows admins to easily create custom policies to meet organization specific needs.	Tailors Safe Access to your business environment
Default access policy	Specifies default policy to be applied to unknown devices connecting to network	Enforces a consistent, standard policy for access across the network
Always allow/deny access	Specifies devices that will always be allowed or denied access regardless of level of compliance with access policy	▪ Ensures key personnel (e.g., CEO) will always be allowed access ▪ Ensures risky individuals (e.g., disgruntled contractor) will not be granted access
Endpoint remediation		
Automated remediation	▪ Automatically remediates noncompliant endpoints ▪ Native support for integration with BigFix® patch management system ▪ Additional patch management integration in development and available upon request	Automated, rapid remediation of noncompliant devices
Scheduled remediation	▪ Native support for integration with Microsoft® SMS ▪ Enables Safe Access to schedule remediation for non-compliant endpoints	Provides greater control over remediation process
Help text for self remediation	Informs end users of where devices are noncompliant and the steps required to bring devices into compliance	Enable remediation without impacting IT support resources
Access 'grace period'	Provides administrator-defined window of access (e.g., 3 days) to non-compliant machines	Provides window of access to enable self remediation
Reporting and compliance		
Drill-down capabilities	Pinpoints specific testing/ /device/compliance data	Enables in-depth analysis of access activity

ODBC / SQL access to database	Standardized protocol allows custom queries and reports	Allows you to customize reports and queries
Diverse range of reports	Including: ▪ Access policy results ▪ Actions taken ▪ Device list ▪ Test details ▪ Test results ▪ Test results by IP addresses ▪ Test results by device ▪ Test results by netbios name ▪ Test results by user	Provide targeted, highly specific data for auditors, managers, and IT staff
Integration with third-party reporting tools	Export data to third-party reporting tools.	Leverage existing systems and data; centralize management of endpoint data
Integration/extensibility		
Enterprise Integration Framework™	▪ Open Java/XML-based API ▪ Allows third-party systems to control Safe Access testing and enforcement functions ▪ Allows external systems to import data to, export data from, and act on data maintained in Safe Access	▪ Leverages IT investments ▪ Proactively mitigates risk ▪ Seamlessly integrates network access control into IT infrastructure
Integration with BigFix® patch management system	Automatically remediates noncompliant endpoints	Automated, rapid remediation of noncompliant devices
Integration with Microsoft® SMS	Enables Safe Access to schedule remediation for non-compliant endpoints	Provides greater control over remediation process
Software development kit	Enables users to create connectors to external systems within the Safe Access API	Allows users to extend Safe Access functionality on their own
On-request connector development	Contract with StillSecure to write customer-requested connectors	Takes advantage of StillSecure development expertise in extending functionality
StillSecure suite integration	Natively supports integration of Safe Access with other solutions in the StillSecure suite including: ▪ StillSecure VAM™—vulnerability management ▪ StillSecure Strata Guard™—intrusion prevention/detection	▪ Provides layered protection for the network ▪ Maximizes efficiency of management and threat response ▪ Leverages existing security network investments ▪ Simplifies administration with suite-wide common functionality, usability, and data management
Implementation/system management		
Readily adapts to all network architectures/existing network infrastructures	Allows Safe Access to control endpoint access on all networks, regardless of architecture, topology, hardware, versioning, etc.	▪ Allows for rapid, seamless implementation ▪ Enables uniform standard of NAC control on complex, heterogeneous networks ▪ Obviates the need for costly infrastructure upgrades to accommodate NAC capability ▪ Requires minimal or no changes to existing network configuration
Allow-all mode	Allows access to all devices, yet tests each device for compliance	▪ Enables controlled implementation ▪ Allows administrators to view/familiarize themselves with all system functions before enabling enforcement/quarantining
Anywhere, anytime access	Web-based interface	Management flexibility
Supports multiple browsers	Management console accessible through IE 6.0, Firefox 0.9, and Mozilla 1.7	Provides management flexibility
HA bypass switch	▪ Provides 'allow all' access in the event of a hardware failure. ▪ Does not require HA configuration to ensure access.	▪ Ensures there is no single point of failure.
Authenticated proxy server support	Receive Safe Access license validation and rule updates through proxy server	Allows easy integration into existing network environments
Automatic data archiving	Archive historical data by offloading to external media or install a commercial back-up client on the Safe Access machine	▪ Store appropriate amount of historical data ▪ Easily keep historical data for compliance/audit purposes ▪ Ensures system integrity ▪ Reduces/eliminates system downtime
Commercial data back-up	Compatible with leading back-up solutions for long-term data archiving	Helps meet regulatory or audit requirements in addition to protecting against data loss
Historical per-device data	Maintains a log of all actions by device	Supports audit and reporting requirements

Manual overrides	Allows administrators to manually grant or deny access on demand	Provides flexible control
Notifications	Alerts administrator of network access control activity	Keeps administrators informed of testing and enforcement activity in real time.
At-a-glance access status overview	Provides real-time summary of all network access activity across network	Provide up-to-the-minute snap shot of system status
Availability		
Software appliance	Provides implementation options as software solution installed on user-provided equipment	▪ Flexible delivery options ▪ Lets you select the implementation appropriate for your environment
Hardware appliance	Provides implementation option as a high-performance hardware appliance	Pre-configured and standardized
Secure locked-down OS	Customized, hardened Linux® operating system	Ensures network access control system is secure
Subscription-based payment or purchase-plus-maintenance payment structures	Includes test updates, software updates, report updates, and engineer-delivered technical support	▪ Provides affordable, cost-effective protection; low cost of entry ▪ Provides all-inclusive, fixed cost of ownership

StillSecure®
www.stillsecure.com

StillSecure
100 Superior Plaza Way
Suite 200
Superior, CO 80027

P (303) 381-3800
F (303) 381-3880