StillSecure® Safe Access™

Protecting your network through endpoint security compliance

Technical summary

Endpoint testing options

- Agent-less testing
  - *Leaves no code on endpoint; no ActiveX controls employed*
  - *Per test session data transfer: 51.8 k*
  - *Requires endpoint authentication/credentials*
  - *Inspects device utilizing the Windows RPC service*
  - *Ideal for testing domain/Active Directory devices including Windows NT, Windows 2000, Windows XP Pro, and Windows 2003 Server OSs*
- Agent-based testing (through the StillSecure agent)
  - *Client automatically downloaded and installed as Windows service*
  - *Per test session data transfer: 20.3 k*
  - *Agent size: 1.89 Mb; memory footprint: 5 Mb*
  - *Ideal for testing all Microsoft-supported operating systems, including Windows 98, Windows XP Home, and NT OSs*
  - *Modifies local Windows Firewall policies to allow service port access from Safe Access server*
- ActiveX testing
  - Tests through web browser; requires IE 6.x
  - No service/software permanently installed
  - Per test session data transfer: 27.8 k
  - ActiveX control size: 664 Kb
  - Tests all Microsoft-supported Windows OSs
  - Ideal for foreign endpoints where installed agent is impractical

Testing administration

- Testing methods applied to endpoint in priority set by admin
- Multi-threaded architecture for speed, scalability (less than 3 seconds in LAN architecture)
- Testing upon connection attempt; retesting during session on admin-defined schedule (e.g., every 30 minutes)
- Fast, accurate OS detection using multiple techniques

Enforcement/quarantining options

- 802.1x enforcement
  - *Supports multiple switches: Cisco, Extreme, Foundry, Enterasys*
  - *Supports any RADIUS-based server: Cisco-ACS, Funk-Steelbelted-Radius, Merit-Radius, FreeRadius, and others through RADIUS proxying*
  - *Device control occurs at Layer 2 using VLANs, MAC addresses and ports*
  - *Authentication to a RADIUS server before the port is assigned a permanent VLAN, etc.*
  - *Test results determine which VLAN the port is assigned: testing VLAN, quarantine VLAN, production VLAN, guest VLAN*
- DHCP enforcement (network and endpoint based)
  - *Fulfills DHCP requests in quarantine network*
  - *Tests devices while in quarantine network*
  - *Enforcement accomplished through existing route/switch infrastructure*
  - *Network-based enforcement: quarantines using routing and access control lists (ACLs) on the router*
  - *Endpoint-based enforcement: quarantines using static routes on the client; does not require re-IP-ing the network or separate IP range for quarantine area*
- Inline enforcement
  - *Installed inline, behind VPN concentrator, RAS, or wireless access points*
  - *Runs as a layer 2 bridge*
  - *Enforcement accomplished through on-board firewall*
- Enforcement through Cisco's NAC architecture
  - *Safe Access server performs posture validation*
  - *Posture validated on Cisco Trust Agent-enabled endpoints and non-responsive endpoints*
  - *Enforcement accomplished through NAC-enabled network access devices*

Access policies

- Default High, Medium, and Low access policies ship with product
- Unlimited custom access policies supported
- Access policies can check registry settings, software, local security settings, services, and files
- Custom policies for different device and end-user types

Compliance tests

- Hundreds of tests ship with product; test library continually expanding
- Off-the-shelf tests exist to check for:
  - *Windows updates and update policies*
  - *Anti-virus software and updates*
  - *Anti-spyware software and updates*
  - *Local firewalls*
  - *Microsoft Hot fixes*
  - *Office Updates*
  - *Worms, viruses, Trojans*
  - *P2P software*
  - *Required or prohibited software*
  - *Required or prohibited services*
  - *Safe software configurations*
- Tests written, QA'ed, and released by StillSecure® Security Alert Team (SAT)
- Automatic test updates initiated by SSL request to SAT server; occur up to hourly
- SAT email notification as high-profile tests released
- New tests automatically incorporated into existing access policies
- Custom test creation/editing with Python-based API
  - *Rich, well-documented Python API allows for easy customization*
  - *Completely customizable web-based user interface screens*
  - *Software developer's kit included*

Non-compliant endpoint remediation

- Help text for each test with suggested remediation steps
- Integration with BigFix® patch manager for automated remediation
- Integration with Microsoft® SMS for scheduled remediation
- Additional patch management integrations in development and available upon request

Reporting

- Report on all device information: IP Address, NetBIOS, MAC address, logged in user, windows domain, test status, last test time, network access status
- Extensible with LDAP/AD integration
- Report on test results: Test failure summary, device test results, policy summary
- Drill down on reports for additional detail

Deployment/scalability

- Single server tests thousands of devices in parallel
- Tests complete in 3 – 10 seconds on a 100Mbps LAN
- Deployment options for all network architectures (see Enforcement/quarantining options, above)
- High-availability bypass unit (fail open)

System management

- Rich, easy-to-use web-based console supports Firefox, Mozilla, and Internet Explorer
- Command line access and administration (limited) is available via SSH
- Authenticated proxy server support
- Manual overrides to immediately allow or deny access
- Graduated enforcement for controlled rollout; options include:
  - *Full denial of access/quarantine*
  - *Temporary access—allows window of compliance*
  - *Admin notifications*
  - *End user notification of test failure and quarantine via personal firewall-like popups*

Integration within IT environment

- Suite of open APIs (available in Java or XML) for integrating third-party IT/security systems including:
  - *Trouble ticketing*
  - *Patch managers*
  - *Asset inventory*
  - *Vulnerability management systems*
  - *Intrusion prevention/detection systems*
  - *Network managers*
  - *Change managers*
  - *Security information managers*
  - *Others*
- Remote control over key Safe Access functions
  - *Testing*
  - *Quarantining*
- Software developer's kit included
- Connectors available off the shelf for:
  - *BigFix® patch manager*
  - *Microsoft® SMS patch manager*
  - *StillSecure suite: VAM (vulnerability management) Strata Guard (IDS/IPS)*
  - *More under development*
- Custom connectors developed on request

OS/platform/architecture

- CommomOS: Hardened Linux® OS, ships/installs with Safe Access
- Open architecture; customizable extensible
- On-board ODBC-compliant SQL database
- Design incorporates multiple open-source components
- Data archiving options
  - *Automatic daily archiving of entire database*
  - *Configuration settings backup*
  - *Third-party backup tool integration*
  - *Offload database to other media or device*

Availability

- Available as:
  - *Software – user-installed on dedicated host*
  - *Hardware appliance – custom configured per consultation with customer*
- Purchasing models:
  - *Annual subscription*
  - *Perpetual: purchase plus annual maintenance*
- Subscription/purchase includes all test updates and product upgrades

Support

- Engineer-delivered
- Available at no charge to subscribers
- 8:00 a.m. to 6:00 p.m. MST; 24-hour support available
- Training and installation assistance available

System requirements

1. **A dedicated server for product installation with the following minimum system requirements:**
   - Pentium® 4, 1.2 GHz or above
   - 1 GB RAM
   - 10 GB disk space
   - CD ROM drive
   - An Internet connection that allows outbound SSL communications
   - Interface cards:
     - 802.1X/Inline/DHCP installation: two server-class network interface cards
     - NAC Cisco installation: one server-class network interface card
2. **Management console: A workstation running one of the following browsers (128-bit encryption required):**
   - Mozilla Firefox 1.0 and higher (Linux, Windows®)
   - Mozilla 1.7 and higher (Linux, Windows)
   - Internet Explorer 6.0 and higher (Windows)

Safe Access available as user-installed software (requires dedicated host) or as custom configured hardware appliance.

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

StillSecure®
www.stillsecure.com

StillSecure
100 Superior Plaza Way
Suite 200
Superior, CO 80027

P: [303] 381-3800
F: [303] 381-3880
www.stillsecure.com