



White paper

WHEN IS 'AGENT-LESS' NOT AGENT-LESS?

Interpreting endpoint testing options for
network access control

Prepared by:

Mitchell Ashley
CTO and VP of Customer Experience
StillSecure®

October 2005

Table of Contents

Introduction	2
Network access control 101	2
The benefit of a true agent-less approach	2
ActiveX: An agent by any other name	3
StillSecure Safe Access: A true agent-less solution	3
Safe Access' agent-less approach to testing endpoints	3
Optimized testing on a device-by-device basis	4
The Safe Access approach to network access control	4
Conclusion	4

About the author

Mitchell Ashley is Chief Technology Officer and Vice President of Customer Experience at StillSecure[®]. He is responsible for product strategy and development of the StillSecure suite of network security software. Mr. Ashley has more than 20 years of experience in data networking, network security and software development. He is a graduate of the University of Nebraska, with a Bachelor of Science degree in Computer Science and Business Administration.

INTRODUCTION

Security-conscious organizations are becoming increasingly interested in network access control solutions. Administrators and security professionals are striving to better protect their networks from the dangers posed by both managed and un-managed endpoints.

One of the consequences influencing the viability of implementing a network access control solution is the need to maintain an agent or client on the endpoint. Many organizations are reluctant to commit to an agent-based approach; past experiences have shown that it would make additional demands on IT resources. From their perspective, installing and supporting an agent on all network endpoints means an increased IT work load, support-related headaches, and unwanted complexity.

Solution vendors are aware of the problems surrounding the use of agents. As such, vendors make numerous claims of 'agent-less' or 'client-less' network access control products. In a majority of cases, these so-called agent-less products actually rely on an ActiveX browser plug-in to test endpoints. While the agent-less claim makes for a compelling marketing story, in reality ActiveX is still a client-side agent, just a non-persistent, network-delivered one, and it has many of the same administrative drawbacks as a persistent agent.

This paper clarifies how the 'agent-less' label is being applied in the network access control market. It examines true agent-less solutions and ActiveX-based approaches that claim to be agent-less. The paper concludes with an overview of StillSecure Safe Access, an award-winning network access control solution that offers testing flexibility. Along with true agent-less endpoint testing, Safe Access offers agent-based testing and testing through an ActiveX control, giving you control over the full range of endpoints.

NETWORK ACCESS CONTROL 101

Network access control technologies emerged in response to the shift from perimeter-focused attacks to attacks that target the endpoint, such as worms and Trojans. Endpoint-focused attacks attempt to gain access and spread havoc through exploits and 'backdoors' on PCs and remote and mobile laptops. Examples of such attacks include Blaster, MyDoom, Sobig, Sober, Zotab and many others.

Organizations have learned that they can't adequately control or secure every endpoint accessing the network. On most networks access is typically provided to a range of devices, including corporate-owned endpoints, remote users, visitors, and employee-owned computers. Additionally, it's next to impossible to police what users do on their devices; lax security habits, risky surfing activity, questionable software and peer-to-peer connections, to name a few, all provide opportunities to unknowingly pick up malicious code.

Network access control isn't necessarily about keeping the endpoint device secure—it's about protecting the network from the havoc a single compromised endpoint can unleash. In that context, network access control provides a method to police endpoints before they gain full access to the network. Network access control solutions typically have two primary functional components:

Testing—The security posture of the endpoint is assessed. Are OS patches up to date? Are AV rule definitions current? Is there spyware or Trojans residing on the device? Is required software, such as a corporate security software, patch management and a personal firewall, present, up-to-date, and running?

Enforcement—Based on testing results, the endpoint is quarantined, given restricted access, or provided full access to the network.

Numerous technical approaches are available to accomplish endpoint testing and enforcement. Initiatives such as Microsoft NAP and Cisco NAC are seeking to build these capabilities directly into the network infrastructure. Other vendors are leveraging existing network standards, such as 802.1x to control access. Others are patching together a mix of established security technologies, such as vulnerability scanners, intrusion prevention systems, and personal firewalls to accomplish the testing and enforcement end goal.

Generally, endpoint policy compliance solutions take either a network-centric or device-centric approach to solving the problem. The difference between these two approaches is the method used to enforce policy: network-centric systems control access at the switch or router (e.g., 802.1x, DHCP, Microsoft NAP, or Cisco NAC). Device-centric approaches are more focused on locking down the endpoint itself and providing a basic means to grant or deny access to the network (e.g., a personal firewall).

THE BENEFITS OF A TRUE AGENT-LESS APPROACH

The agent-less approach to endpoint testing requires minimal resources to implement and support. It offers considerable benefits over testing through a persistent agent or an ActiveX control. Key advantages include:

Easily test unmanaged endpoints—Determine any endpoint's security posture without installing an agent or downloading an ActiveX control.

No client-side software installation—Eliminates the need to support a downloaded or manually installed application. Additionally, testing can be accomplished on devices where application installation is prohibited.

Reduced or negligible help-desk calls—Eliminates the need to support/maintain/troubleshoot application software on each connecting endpoint.

Rapid deployment—Enables network access control system to be rolled out quickly. The application server is the only device requiring installation/configuration.

Eliminates the possibility of impacting endpoint performance—Agent installation can cause unforeseen problems with endpoint functionality. A true agent-less approach eliminates this risk.

True agent-less testing is doubly beneficial when applied to unmanaged endpoints—the devices that are not directly owned by the organization. These are the machines used by visitors, partners, and employees remotely connecting to the network with their home PCs. Testing such devices using the agent-less approach significantly enhances the security posture of the network.

By definition, unmanaged devices represent a greater risk than managed or corporate-owned devices. There is no ability to police the applications installed or the activity engaged on these devices. Clearly, installing an agent (ActiveX or a persistent agent) on a majority of unmanaged devices connecting to your network is neither practical nor desirable. Agent-less testing, however, gives the organization a high degree of control of these machines—much more than was previously possible. It ensures unmanaged devices comply with security policy before they can access the network. Only an agent-less approach can accomplish this efficiently on a large scale.

ACTIVEX: AN AGENT BY ANY OTHER NAME

ActiveX testing of endpoints can be a valuable alternative option when agent-less testing or testing through a persistent agent is not feasible. Advanced network access control solutions, such as StillSecure Safe Access, offer all three testing methods.

The issue with ActiveX testing is that it is not agent-less or client-less, as some vendors want you to believe. ActiveX controls are applications (i.e., agents) that are downloaded and launched from an ActiveX-compatible browser such as Microsoft's Internet Explorer (IE). Because ActiveX controls are not permanently installed on the endpoint (i.e., not persistent), vendors relying on the technology feel they can claim to have an 'agent-less' solution. Not so.

Compared to true agent-less testing, ActiveX testing has a number of drawbacks:

ActiveX only runs in the ActiveX-compatible browsers—Devices running FireFox, Netscape, Mozilla, or other browser cannot be tested.

Testing activities may be prohibited based on users' permissions—admin access is likely required for deep testing.

IE can be configured to block ActiveX controls—Blocking ActiveX is a common security practice.

ActiveX control must be downloaded each time testing occurs—There is capability to retest a device after it's been granted access. Machines that become non-compliant while connected are not identified. Continual downloading over dialup or slow WAN links is likely to be problematic.

Browser must be open for testing to occur

ActiveX testing likely to be unacceptably slow over dial-up connections

When one or a combination of these conditions are present, the testing process itself is likely to fail, in which case two possible outcomes are likely:

- The endpoint would be given access without any assessment of its security posture.
- The endpoint would be placed into quarantine or denied access, resulting in a call to the help desk.

Even if a small percentage of devices experience problems with ActiveX testing, it could overwhelm support staff, especially on large networks with thousands or tens of thousands of endpoints.

ActiveX has a place at the endpoint testing table, alongside true agent-less testing and testing through a persistent agent. There are instances where ActiveX may be the only option that will work, for example when the user does not have permissions to install an agent. The key is not to rely on ActiveX as the only or even the primary method.

Advanced network access control solutions offer multiple testing methods and allow you to prioritize the order in which they are applied to the endpoint. Such an approach ensures that the maximum number of endpoints will be tested with a minimal impact on network and support resources.

STILLSECURE SAFE ACCESS: A TRUE AGENT-LESS SOLUTION

Safe Access, StillSecure's network access control solution, offers true agent-less endpoint testing. It also offers an ActiveX plugin testing option and a agent-based option. This provides considerable flexibility; it allows Safe Access to optimize network resources and test the full range of endpoints attempting to access the network. Safe Access automatically applies the optimal testing method to endpoints connecting to the network

Safe Access' agent-less approach to testing endpoints

StillSecure Safe Access accomplishes agent-less testing by accessing the endpoint directly from the Safe Access central policy server. Safe Access connects to endpoint devices using NetBIOS or TCP session protocols. From this network connection, devices are tested for a range of security requirements such as patch levels, anti-virus state, security settings, browser settings, peer-to-peer software, and banned applications. The tests performed examine the operating system registry, running processes and services, files, file attributes, and other aspects of the endpoint device.

The testing time and network performance of the agent-less approach is typically very efficient since most of the analysis is managed by the central policy server, code is not download across the network, and the information retrieved from the endpoint is relatively small in size.

Optimized testing on a device-by-device basis

The table below shows optimal priority with which Safe Access applies the following three testing options to the range of network endpoints.

- **Agent-less**—Ideal for testing Windows® 2000 and Windows XP Pro machines (managed and unmanaged). It offers zero-maintenance device administration as no client needs to be installed or supported on the endpoint.
- **StillSecure agent**—Tests all Microsoft-supported Windows operating systems and can be used for internal legacy devices such as those running Windows 98 or NT.
- **ActiveX plug-in**—Tests all Microsoft-supported Windows operating systems and foreign endpoints where an installed agent is impractical.

Administrators can prioritize the order that testing options are applied as devices initially connect to the network. For example, on an internal network with many legacy devices, the StillSecure agent might be selected as the preferred testing method, while on remote access or VPN connections, the agent-less option might be the desirable method.

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.

The Safe access approach to network access control

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 tests devices by applying access policies as devices log onto the network. As discussed above, testing can be accomplished with three different approaches: agent-less, agent-based, and ActiveX.

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. Safe Access offers multiple options for enforcing compliance including:

- DHCP enforcement
- Gateway enforcement
- 802.1x enforcement
- Cisco NAC-enabled enforcement

These enforcement options enable Safe Access to secure any network topology against the dangers that non-compliant endpoints can introduce. Safe Access tracks all testing and connection activity and produces a range of reports for auditors, managers, and IT staff.

In addition to serving as a turnkey network access control solution, Safe Access integrates within your IT environment, enhancing threat-response capabilities and leveraging IT investments. This is accomplished through the Enterprise Integration Framework™, which allows third-party systems to control Safe Access' testing and quarantining functions. Through integration, Safe Access serves as the focal point for endpoint access control and enforcement.

CONCLUSION

Knowing that administrators shun solutions that are labor and support intensive, many vendors attempt to pass off products that test endpoints through an ActiveX control as “agent-less” or “client-less.” In reality, ActiveX controls have the same—if not more—drawbacks than a persistent agent.

True agent-less testing, which is available in advanced solutions such as StillSecure Safe Access, offers significant administrative advantages compared to ActiveX or agent-based testing approaches. No software is installed on the client side, so installation and support requirements are negligible. Unmanaged devices can be seamlessly tested, and there’s no chance of adversely affecting the performance or operation of the target endpoint.

Flexibility is crucial for successful network access control—flexibility in testing and flexibility in enforcement. StillSecure Safe Access offers multiple testing and enforcement options to provide the highest level of protection with minimal administrative overhead.