Agentless Comes of Age

Streamlined Approaches to Administration and Authentication

The debates rage on. Creationism vs. evolution. Republicans vs. Democrats. Chocolate ice cream vs. vanilla. Agentless vs. agent-based network security assessment systems. Well, maybe the last one hasn't reached a level of zealous fervor yet, but it's many an IT professional who has dug in his heels to staunchly defend agent-based technologies or to tout the benefits of next generation agentless systems.

In the end though, agentless systems are likely to be victorious as the preferred means of network security and configuration auditing for several reasons:

- significantly faster to implement
- cost less to own and operate
- scale more easily to cover large numbers of assets
- provide coverage of devices that cannot support an agent
- support heterogeneous assets in distributed or centralized locations

These are clear differentiators in a world where money, resources and time are always scarce, IT environments get more expansive and harder to control and audit every day and the risk to an organization through configuration changes can be significant.

Because they don't require installed software on every device, agentless technologies are far easier and faster to roll out and manage over large numbers of systems. The 'time to value' for agentless technologies is typically measured in hours, rather than days or weeks. An IT security professional can bring an agentless system online in as few as four hours, without having to seek permission from other departments. Agents typically can only be deployed at the rate of 10-20 per day, after permission and access to the target system is granted. Agents may also be required to run with root authority, taking control out of the hands of the system administrators.

Agentless systems are not invasive, and they are easier to maintain over the long haul since updates only affect a handful of servers. From a network control perspective, agentless systems can solve critical IT problems without creating turf battles – IT security staff can implement and maintain them with or without the cooperation of other departments or the need to install proprietary software on equipment owned by others, such as business partners.

Agentless systems can detect and monitor all devices on the network, such as routers, switches, firewalls and other devices that cannot support agents but still can become vulnerable with configuration changes. And very critically, the only way to find rogue systems is using an agentless solution. If they're rogue, then by definition they do not have agents installed. Agentless systems can't be disabled by users like agent-based systems. And when it comes to unknown devices on the network, what you don't know can definitely hurt you and can certainly impact your audit results.

In environments where security and compliance auditing systems need to be scaled to large numbers of users or implemented in highly distributed networks, agentless solutions are fast becoming the preferred choice. Why? Because of the widespread adoption of centralized administration and authentication technologies.

Centralized Administration Enables Agentless Technologies

Active Directory for Windows was introduced in 2000 and today, some form of directory-based authentication exists for every major operating system. Centralized administration is the key enabler of agentless systems and is driving their ever-increasing popularity.

Centralized authentication systems provide single sign on (SSO), allowing users to authenticate themselves across a variety of applications, systems and services with one set of credentials. Centralized administration relies on one directory and eliminates the need for administrators to create and manage accounts for every device on the network, something that would be very difficult to manage across hundreds or even thousands of devices.

Agentless systems take advantage of centralized authentication to scale to large numbers of devices with a minimum of administrative burden. Without centralized administration, every computer needs to have its own account of authorized users. To perform a scan under that scenario, an agentless system would need unique credentials for every device on the network. The maintenance load for administrators would be similar to that of agent-based software, eliminating one of the key benefits of agentless technologies.

Utilizing centralized administration and authentication, agentless systems can log into target systems across an entire network using single sign on credentials, just as a user or administrator would. Once in, they can check security settings, find out what software is installed and what updates are needed, while detecting any changes or trouble spots that would indicate a violation of security policy or a vulnerability.

Agentless systems are then able to consolidate data from all network devices into reports that can alert systems administrators to maintenance needs or breaches—all without the need for any software installed on assets and without the need for administrators to manage authorization for hundreds or thousands of transactions. The cost savings of using agentless technology can now be measured.

For 500 Servers	Agent	Agentless
Sever License Fees per IP[1]	$600	$200
Annual Maintenance Rate	22%	22%
Annual Maintenance Fees Per IP	$132	$44
Estimated Annual Operating Costs per IP[2]	$75	0
Total Year 1 Cost	$807	$244
Annual Ongoing Cost	$207	$44
3 Year Cost of Ownership for 1 Server	$1,221	$332
3 Year Cost of Ownership for 500 Servers	$610,500	$166,000
Agentless Cost Savings Over 3 Years for 500 Servers		$444,500

The table above show estimated cost savings for an agentless solution versus one deployed using agents.

[1] *UNIX (HPUX,AIX) or iSeries (OS400) agents often exceed $1000.*

[2] *Estimated annual operating cost includes initial implementation and ongoing maintenance. Initial implementation estimates vary from 10-30 agents per day, and daily operations include verification all agents are running, none have reported errors, fixing any issues, upgrades and maintenance, including scheduling and change control procedures.*

Given the cost savings and significant reduction in maintenance headaches, most IT and security professionals would have probably favored agentless technologies all along had centralized administration been available, but because there was no seamless way to manage credentialing, agent-based systems seemed like the only viable alternative.

Today, the widespread adoption of centralized administration, especially in Windows environments, makes the deployment of agentless systems practical and has given IT security professionals many more options when choosing systems management and network security solutions.

Agent-based technologies remain widely used and may still be an acceptable solution for some situations, but thanks to centralized administration, they're not the only game in town. A whole new way of streamlining administration and authentication has opened the door for agentless technologies that give IT and security departments broad new levels of flexibility, provide audit capability on devices that cannot support agents, help control costs, and significantly reduce maintenance burdens across an ever-expanding pool of users, devices and distributed environments.