

Agent Based or Agentless scanning – should you have to choose?

Combining Resident Agents and Agentless Scanning to Safeguard Information Assets, Ensure Trusted Configurations and meet Regulatory Requirements

“The debates rage on” – a quote from a recent paper by a vendor which is arguably responsible for most of the agentless vs. agent-based security assessment ‘debate’ in the first place and is of course one of the leading exponents of agentless technologies!

Marketing departments from one or two vendors are pumping vast amounts of one-sided views into this subject, suggesting there is only one way to deliver these solutions – their way. Meanwhile, users continue to struggle with the challenges of protecting their information assets and meeting their compliance needs in a way that works for them!

Some major technology analysts have also joined this fatuous argument, when in fact it should be about using the right technology to meet the user’s needs, not the needs of some vendors.

The true reality – what meets the customer’s needs is what counts!

In practice, there are times when a resident agent solution is the only way to deliver a secure, fully automated and in-depth solution to on-going configuration assurance, compliance and system integrity monitoring needs (*especially when automated change detection is required*). On the other hand, there are times when an agentless solution will deliver what’s needed and may be more cost effective.

This debate should really be about which technology will meet security and compliance requirements, not about what the vendor has available. While periodic remote scans of servers to give snapshot views of configurations for compliance purposes can meet regulatory audit requirements, this approach may not satisfy enterprise security configuration assurance and file integrity monitoring needs. This is particularly true for mission critical systems which need fully automated security and integrity monitoring to continue even if the network is unavailable or where there are network bandwidth restrictions. This can only be guaranteed with self sufficient resident agent based solutions.

For most organisations, it’s about selecting the appropriate tools for the task in hand. Where physical servers are employed for short term projects and then cleared and recycled for new projects it may not make sense to expend efforts and resources on installing and configuring agents for compliance and configuration scanning when agentless scans will be adequate.

On the other hand, agentless systems may be much less effective with virtual servers (see *Virtual Servers need to protect themselves!* below) or with mission critical systems which remain in operational use for long periods and which are normally under strict change control.

In these cases, meeting the more stringent needs for fully automated and frequent system or file integrity monitoring (*and constant configuration change detection to maintain systems in a ‘known and trusted state’*) may not be possible using agentless remote scanning. Here, a resident agent approach will be needed, and the one-off installation and configuration costs can be easily offset against the greater security and control benefits to be derived from agent based solutions.

Compliance with regulatory standards does not necessarily ensure good security!

While any organisation that has achieved compliance with standards such as PCI-DSS will have significantly improved its overall security posture, compliance alone will not ensure that its information assets are actually secure. This requires much more than just periodic compliance reviews. More and more high profile organisations are suffering major IT security incidents in spite of being compliant with relevant standards.

This may be in part because compliance snapshots do not measure security and integrity controls or assess configurations frequently enough. Even small, un-noticed configuration changes can introduce security vulnerabilities and also take systems out of compliance.

Of course, periodic remote compliance scans are useful and quarterly pen-tests are essential in meeting regulatory requirements, but these may not tell you if the payroll application has been compromised in any way or if someone has been wrongly given superuser privileges, or if some critical data has been altered – in other words they won't tell you if your systems are in a 'known and trusted' state. To achieve this level of security posture requires much more automation and control and it's for this reason that most enterprise system management solutions use resident agents.

Virtual servers need to protect themselves!

Virtualisation is bringing cost and environmental benefits to datacentres, but this technology is also introducing unforeseen security and monitoring challenges. Virtual servers, while having all of the same security vulnerabilities and challenges as physical servers, also pose new security challenges due to the inherent mobility of VM's. Maintaining secure, compliant and trusted configurations and forensic audit trails becomes much more complex, as virtual machines easily move around the physical network. In this environment, powerful, automated and self contained software agents provide a means of self protection for virtual servers – when the VM moves, so the resident agents move with it!

Yet more software agents vs. yet more black box appliances!

For some organisations, installing and managing software agents may well stretch their resources too far, and may even be counter to their security policy. On the other hand for others, installing more black box appliances (*as used by most agentless solutions*) in the appliance server room and managing it, creates different problems again. There are black box appliances available for so many applications and many major enterprises are struggling to manage these appliance farms and now refuse to cram any more of these black box appliances into their premises.

Agentless solutions need external privileged access to mission critical systems

There is also a debate about allowing remote privileged access to critical systems from external applications, especially where large numbers of target systems are involved. Indeed, many organisations' IT security policies expressly forbid it and servers are configured to disallow remote access logins. This has made the agentless solution much more difficult to implement in the data centre and in the server farm. Integration with Active Directory or use of enterprise wide centralised authentication systems with Single Sign On (SSO) facilities, can help to counter this challenge.

Why are some vendors pushing agentless only solutions so hard?

Well, maybe for a number of reasons. But, for one thing, it would make no sense for 'next generation' scanning vendors to attempt to build all the agents that the established host based vendors have available, especially for all the legacy systems that customers are still using. It would just be too difficult and costly to do and they may not have all the knowledge and experience or even access to the platforms required to do it.

So what is the answer?

Simple. Go with a vendor who's solution employs both efficient resident agent and secure agentless technologies to achieve your security, integrity and compliance needs, depending on the circumstances and roles of the target systems.

Being forced to choose between these two very different and potentially valid approaches is pushing organisations down a single path that might not fit their needs now or in the future!