

Anti-Tampering Checklist

Or, Ten Hacking Questions You Should Ask Yourself Before Choosing a Device Control Endpoint Security Solution

	Ask these questions...	Safend Protector	Product 2	Product 3
1	<p>Does the product distrust users with local administrator privileges and prevent the Local Admin from changing its settings? Regardless of how hard you try, a malicious user can easily gain local administrative privileges on his machine¹. The product should specifically prevent a Local Admin from making any changes to its settings.</p>	√		
2	<p>Is the policy file encrypted and signed? Protecting the policy file guarantees that only an authorized network administrator can read and write the policy that is enforced by the product. An unencrypted/unsigned policy can be changed by a rogue user, effectively removing the protection. In addition, policies cannot be copied from machines in other organizations.</p>	√		
3	<p>Are the product's registry settings protected? Every security product has to integrate with Windows, using the Windows Registry. A malicious user might try to delete or alter the product's registry settings in order to remove the protection.</p>	√		
4	<p>Are the product's own files protected against deletion/alteration? By definition, every security client has some files on the endpoint itself. If a malicious user is able to delete or alter these files, the protection can potentially be removed.</p>	√		
5	<p>Are the product's files signed and verified at run-time? If they are, then even if a rogue user succeeds in altering one of the files, he will be caught when the product periodically validates the integrity of its files.</p>	√		
6	<p>Can the end-user uninstall the product? Only an authorized network administrator should be allowed to uninstall the client. This is why an uninstall password mechanism should be implemented during the product's uninstall procedure.</p>	√		
7	<p>Are the logs protected and encrypted? The product's logs are an essential diagnostic tool for the network administrator (for example, reading and understanding them can uncover the source of information leaks). The log files should be protected from viewing, deletion and alteration by a rogue user.</p>	√		
8	<p>Is the product safe in "Safe Mode"? The product should protect against potential attacks against itself in Safe Mode just as it does in regular operation of the OS. This is because every user can switch to Safe Mode.</p>	√		
9	<p>Does the product avoid basing its anti-tampering capabilities on Rootkits? Rootkits are software components that hide data (registry/files) and/or its existence from other applications. Some endpoint security products use Rootkit techniques in order to restrict access to their files/registry settings. This compromises the security of the system, because Trojans and viruses can spread using these hidden keys or files. In order to check for Rootkits, you can run Sysinternals RootkitRevealer² on an installed agent and see if there are hidden keys/files.</p>	√		
10	<p>Can the product deal with advanced removable storage devices that are capable of running codes and applications when connected? A smart device that contains an Autorun file can fool the OS into thinking it is a standard Disk On Key, when in fact it is able to run code on an endpoint without your consent.</p>	√		

© Safend 2006. All rights reserved. All product names and trademarks are the property of their respective owners.

¹ Many tools let an attacker change the local administrator's password using an alternate OS. A summary of these tools can be found in [Daniel Petri's essay](http://www.petri.co.il/forgot_administrator_password.htm) on the subject (see http://www.petri.co.il/forgot_administrator_password.htm).

² Sysinternals RootkitRevealer can be found at <http://www.sysinternals.com/Utilities/RootkitRevealer.html>.