Realtime publishers

The Essentials Series: Increasing Performance in Enterprise Anti-Malware Software

Best Practices in Deploying Anti-Malware for Best Performance

sponsored by

GFI

by Eric Schmidt

Copyright Statement

Best Practices in Deploying Anti-Malware for Best Performance

New malware is being released at record numbers on a daily basis, yet the products that defend against these threats remain a common source of performance issues today. The threats that enterprises face necessitate a robust anti-malware solution while maintaining high-performing systems. The first two articles in this series focused on what makes anti-malware slow and what should be examined to ensure optimal performance during the anti-malware solution selection process. In this, the final article of the series, the focus will be on the best practices for deploying anti-malware software to optimize performance and the protection it's intended to provide.

Agent Installation

The agent is the obvious place to begin a discussion on optimizing performance, with agent configuration beginning at installation. The server console should provide two features with respect to agent configuration. The first is the ability to deploy the agent from the console to all systems with minimal effort. This enables administrators to quickly deploy the agent to all systems or reinstall agents on systems where they have become unhealthy.

The second is to create a preconfigured installation that can be distributed by both manual installation and automated software distribution methods. The installation that is created should require little or no user input. This ensures that every client will be installed the same way by reducing or eliminating the ability for the person installing the application to make changes. Optimal performance and the ability to manage clients are achieved through a consistent and reliable installation of the client.

Agent Configuration

Once the agent has been installed, the next area to look at is its configuration. Before a discussion on what should be configured, it's important to address the benefits of controlling how the agent configuration is managed. Next, files and folders that should be excluded from scans will be addressed. Each of the scan methods should be configured in such a way to optimize system performance and limit the impact to the end user.

Policy-Driven Agent Configuration

Smart organizations leverage a policy-based approach to agent configuration. Here, all client behavior and configuration options are established on the anti-malware server and deployed to the agents in a way that prohibits end users from making changes. This is critical because every attribute that is permitted to be modified by the user creates the opportunity for inconsistency. When environments are inconsistent, they become more difficult to manage and troubleshoot and increase the likelihood of accidental exposure. In extreme cases, the ability for agents to detect and eliminate threats is hampered because the user disabled or crippled a component that would have prevented the threat.

File and Folder Exclusions

Real-time and scheduled scans require the identification of files and folders that should be excluded. The vast majority of software vendors will publish information on what should be excluded for their products. For example, Microsoft has an article http://support.microsoft.com/kb/943620 that details what should be excluded for some of their server products. When deploying an anti-malware solution, it is critical that all installed applications are reviewed in order to determine whether there is a need to exclude some files or folders in order to achieve optimal performance.

WOL

In the past, it was common for desktops to remain on 24 hours a day to simplify maintenance during non-business hours. With the move toward green IT, many companies have chosen to turn off desktops during non-business hours. In these situations, technologies such as Wake-On-LAN (WOL) can be leveraged and allow the scans to still be performed during non-business hours. WOL enables computers that are off but connected to the network to be turned on as needed in order to perform maintenance tasks such as virus scanning and patch installation. If WOL can be leveraged, scheduled scans can be configured to run nightly. In cases where WOL is not available but systems are still turned off during non-business hours, the frequency of scheduled scans may be reduced from a daily activity to a weekly one with quick scans performed daily.

Mobile computers present a similar challenge to desktops that are not on at night. Scheduled scans are often disabled because the systems are only on when someone is intending to use the mobile device. In these cases, it is also best to limit scheduled scans to run on a weekly basis. Of course, the best mitigation that enables scheduled scans to be run while a user is present is to select a product that has a single, integrated scan engine that has been optimized for the operating system (OS). If the right product has been chosen, the impact of running a scheduled scan may not even be noticed by the user because it doesn't consume a large amount of system resources. Finally, a high-performance client in conjunction with the ability to exclude files and folders based on vendor recommendations will result in the ability to run scans on a daily basis with little or no impact to the user.

Threat Detection Integration

Scanning performance is also impacted by how the vendor has chosen to integrate the various types of threat detection. With more and more systems being on only while users are actively working, the performance of anti-malware agents is dependent on the engine itself. Some vendors have bolted the various threat detection engines together in a way that requires multiple scans, one for each type of threat. With these products, there may be no practical way to accomplish all the scheduled scans without impacting the user. In order to minimize the impact to the user, it is best to choose a product where all types of threat detections have been integrated into a single engine. This simplifies the scheduling of full scans while enabling them to be run more frequently because an integrated efficient scan won't impact performance; thus, they can be run even while someone is using the system.

Agent and Management Server Communication

Agent communication with the management servers can also have a direct impact on client performance. Ideally, the intervals that agents check in with their management servers should be configurable. At most, the agent should not be configured to check in more than once an hour. In most cases, every 4 to 8 hours is sufficient, but they should never be configured to check in less than once a day. This setup provides a high enough frequency for clients to get urgent definition updates, which are often released multiple times each day. This also enables the agents to get configuration changes in a relatively short amount of time. This interval is largely dependent on the type of connection the clients have with the server. In large enterprises, the management servers may be in another physical location. If the WAN links are limited in size, the interval should be reduced to eliminate unnecessary traffic.

To maximize protection, the server console should also have the ability to initiate a definition update for all the clients on an ad-hoc basis. This enables the servers to update the definitions on all clients without waiting for them to check in. Malware has the ability to spread throughout an organization very quickly and there will be situations where there isn't time to wait for clients to check in for updates. In these cases, the ability to initiate a definition or configuration update from the server console could mean the difference between a full enterprise infection and one that is limited to a few systems. Issues surrounding the communication interval can also be mitigated by selecting products that have effective heuristic engines as well. Products with good heuristic engines and other methods such as emulation can provide a solid defense against virus outbreaks, minimizing the reliance on immediate definition updates.

Anti-Malware Can Be Efficient Without Impacting System Performance

This series has examined the factors that contribute to slow anti-malware performance, the factors to consider when selecting an anti-malware solution, and finally, the best practices for deploying anti-malware products. Anti-malware software is an essential defense against malicious software that should be run on every system whether at home or in a large enterprise. These products have evolved into threat detection suites designed to protect systems against very sophisticated attacks. At the same time, they have become so resource intensive that they impact overall system performance and user productivity. It's now critical to select a product that has an efficient, integrated, single scan engine and has been optimized for the OS on which it is to be used. This will result in an anti-virus, anti-malware infrastructure that's easy to manage while at the same time minimizing the impact on system performance and user productivity.