Realtime publishers

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

Considerations for Evaluating Performance in Anti-Malware Products

sponsored by

GFI

by Eric Schmidt

Copyright Statement

Considerations for Evaluating Performance in Anti-Malware Products

The anti-malware product space consists of many bloated, slow product suites that have been around for a very long time. The products have evolved along with the threats they are intended to defend against. This evolution has at the same time created massive suites that create major impacts on system performance.

When choosing an anti-malware solution for an enterprise, it is very important to consider several factors. The first consideration is the ability of the product to protect the systems it's running on. The second aspect, which is often overlooked, is the impact the product will have on overall system performance. This article will focus on what you should examine from a performance perspective during the product-selection process.

Examining the Code Base

The first area to be examined is the anti-malware code base itself. The most popular anti-virus products today are a result of years of development. In some cases, the latest code base was developed for a legacy operating system (OS) and then simply updated to support the most current one. Although the fact that a product has been around for a long time can be a testament to its maturity, it can also be an indicator of a potential negative impact to performance due to the presence of legacy code. The product may still contain calls to APIs of older OSs. In some cases, the product may still rely on legacy APIs instead of leveraging new features and improvements of a modern OS. This can lead to poor performance.

Scan Methodologies

The next area that should be focused on with respect to performance is scan methodologies. The first article in this series described in detail different types of scan methodologies, including real-time scans, scheduled scans, heuristics, behavioral analysis, and emulation.

Integrated Scan Engines

Today, most enterprise products are not limited to virus protection. They have evolved into suites that include protection from malware and spyware as well. Although this feature set can simplify product selection, one should examine how those different types of scans are being performed. In some cases, product suites are a set of solutions that were bolted together but not integrated. In these cases, there may be no integration between the anti-virus and anti-malware engines. This lack of integration creates performance issues because each component in the suite has independent scans that need to be performed. For these products to perform effectively there may be additional resource requirements. Often, these performance issues can be avoided by selecting a product that has the ability to protect against all types of threats using a single, integrated scan engine.

Firewalls

This discussion can also be extended to suites that include firewalls. With Vista and Windows 7, Microsoft made significant improvements in the built-in firewall, thereby making it optional to select anti-malware suites that include one. Windows XP, however, does not include a robust built-in firewall, forcing companies to deploy third-party solutions. The inclusion of a firewall should be weighed carefully, comparing the additional control and functionality of a third-party firewall versus the potential penalty of unnecessary code bloat.

Control and Manage Scheduled Scans

Although every anti-malware product today has the ability to configure and manage the scheduling of scans, there are important details to their specific features that shouldn't be overlooked. As mentioned in the first article, scheduled scans are an excellent proactive process that can detect and prevent malware infections. When looking for an anti-malware solution, consider two specific areas in which the details of scheduled scans can have an impact on performance: scan configuration and scan speed.

Scan Configuration

How effectively can a scan be configured? In some circumstances, it is necessary to exclude certain files or folders from scheduled scans. This is critical as the scan itself can have an impact on application or system performance. On database servers, for example, it is recommended that database files themselves be excluded because the scanning of their very large files can result in poor database performance. When evaluating anti-malware products, it's important to look at the management console and the functionality it offers to manage exclusions across all clients in your infrastructure.

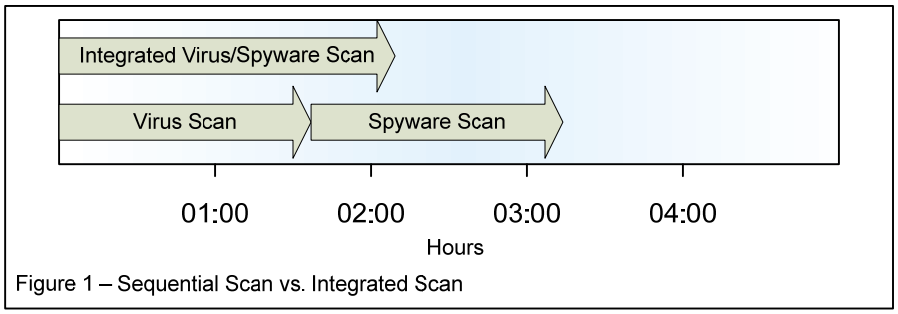

Figure 1 – Sequential Scan vs. Integrated Scan

Scan Speed

The second factor is the speed at which scans can be completed. It has already been stated that products that employ multiple scan engines can take longer than those with an integrated approach. When multiple scan engines are employed, they must be staggered to run at different times or their concurrent operation will compete for disk resources. This is of particular importance with mobile computers now outselling traditional desktop computers. Mobile computers are often only on when the user is intending to use it. By selecting a product that can perform scheduled scans in the most efficient manner possible, one can minimize the impact to the user while the scan is being performed.

Client Configuration

During the evaluation of an anti-malware server console, one should also look at the ease with which other client behaviors and attributes can be configured. These include the ability to deploy the client itself as well as updates. The console should also facilitate the ability to easily deploy definitions and signatures both on a scheduled and ad-hoc basis. The ability to deploy on an ad-hoc basis is necessary due to the increasing number of exploits that are experienced on a daily or less-than-daily basis. In most cases, the threats are identified before mass infections occur. Anti-malware solution vendors create updated signatures that must be deployed to all clients in an efficient manner to prevent widespread outbreaks.

Especially problematic are the types of exploits that propagate before signatures have been updated. These are commonly known as *zero-day exploits*. When a zero-day exploit is discovered, the quality of the clients' anti-malware engine is tested because signatures have yet to be created. Here, clients must rely on heuristics, behavioral analysis, and emulation to protect against these threats until a signature is created. Once anti-malware vendors release a signature, it becomes imperative that it be quickly deployed to all the clients as this enhances the clients' ability to detect the threat. A poorly performing client may be slow to check in with the server to get the updated definitions, which then puts the system at risk of being infected.

Heuristic Scan Engine

The risk of zero-day exploits can be lessened by selecting a product with effective heuristic behavior and emulation scan engine. Recall from the first article that heuristics look for virus-like behavior. A good heuristic scan engine can be augmented even further by leveraging advanced detection features such as emulation and behavior analysis. When these advanced features are available, every file can be opened in a protected environment. This provides the heuristic scan engine with greater insight into every file, which then increases the likelihood that a zero-day exploit will be detected. This type of scan can also be optimized by the vendor for performance. It is important to select a vendor that offers heuristic scanning that can be performed quickly with an integrated engine that detects all types of threats. Similar to the other consequences of a product that wasn't written for Microsoft's most current OS, the heuristic scanning should be optimized for that platform. If it too relies on legacy code, there is the potential that it will have a negative impact on system performance.

A High-Performance Client Is the Best Defense Against Malware

The best defense against viruses and malware is an efficient, high-performance client in concert with a management server that is easy to use and configure. There are several factors to consider when choosing an anti-malware solution, including the code base on which it was written and the integration of the various scan engines. The ideal product will be one that combines anti-virus, anti-malware, and anti-spyware scanning into a single engine that has been optimized to run on the OS for which it will be used. It will leverage the OS's built-in security enhancements and not require that those features be disabled.

This article explored what makes anti-malware products slow and what should be examined when selecting a product. The final article in this series will focus on the best practices for deploying anti-malware solutions for optimal performance.