

Realtime  
publishers

# The Essentials Series

Increasing Performance  
in Enterprise  
Anti-Malware Software

*sponsored by*

**GFI**

*by Eric Schmidt*

---

Article 1: Why Is Traditional Anti-Malware Software So Slow?.....	1
Traditional Anti-Virus Software Is Slow.....	2
Multiple Endpoint Products Performing the Same Function .....	3
Scan Methodologies.....	3
Real-Time Scans .....	4
Scheduled Scan .....	5
Client Reporting .....	6
Anti-Malware Shouldn't Be Slow .....	6
Article 2: Considerations for Evaluating Performance in Anti-Malware Products.....	7
Examining the Code Base .....	7
Scan Methodologies.....	7
Integrated Scan Engines .....	8
Control and Manage Scheduled Scans .....	8
Scan Configuration .....	8
Scan Speed .....	9
Client Configuration .....	9
Heuristic Scan Engine .....	10
A High-Performance Client Is the Best Defense Against Malware .....	10
Article 3: Best Practices in Deploying Anti-Malware for Best Performance.....	11
Agent Installation .....	11
Agent Configuration .....	12
Policy-Driven Agent Configuration.....	12
File and Folder Exclusions.....	12
Threat Detection Integration.....	13
Agent and Management Server Communication .....	13
Anti-Malware Can Be Efficient Without Impacting System Performance .....	14

---

---

## **Copyright Statement**

© 2009 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers or its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.com).

---

# Article 1: Why Is Traditional Anti-Malware Software So Slow?

---

Since the beginning of the Internet, anti-malware software has been an essential component of every business computer. As the Internet continues to grow in scope and sophistication over time, so does the intelligence built into malicious software. Today's malware has evolved from its origins of viruses as a mostly harmless demonstration of self-replicating code to a full-fledged underground industry with its own motives for profit.

To that end, the malware threat landscape has changed dramatically in recent years. Today's threats are being created for far more insidious goals, including cyber-terrorism, identity theft, and corporate espionage. This reality has been made easier with the introduction of shrink-wrapped malware toolkits that enable the point-and-click invocation of attacks. These toolkits are easily downloadable through online forums that facilitate the collaboration and development of such attack software.

The solutions that protect computers from these types of attacks were developed shortly after the first viruses. Many of those products are still around today. To combat the ever-changing tactics of malware writers, those early "anti-virus" products have also evolved to address new threats. Unlike with malware, however, this sophistication in protection products comes at a cost. That cost relates to the actual system resources necessary to run their protective processes.

In effect, the slow evolution of anti-malware software over the long term has created a spaghetti of detection and removal mechanisms. This aggregation of today's solutions atop yesterday's code bases creates a major performance problem for enterprise computers. That loss in performance impacts employees' ability to accomplish their needed tasks, reduces business processing agility, and increases the computing infrastructure's total cost of ownership.

One solution for this problem involves an entirely new approach to creating anti-malware solutions for business. This approach throws away the aging code base of the past in favor of truly recreating the wheel. By electing to break with the software of the past, new and highly-optimized solutions can be developed to protect from malware while ensuring the best possible user experience for your desktops, laptops, and servers.

This, the first of three articles in this series, will discuss why many traditional anti-malware solutions have a negative impact on system performance. It discusses the risks to business operations that are created as a result of this performance degradation. Continuing with this discussion are two subsequent articles that focus on the factors you must consider when selecting an anti-malware product as well as what can be done to optimize your selected solution's performance.

---

## Traditional Anti-Virus Software Is Slow

Let's face facts. Traditional anti-malware solutions are a painful but historically necessary function of computing. The fact is there is a problem intrinsic to any software solution that has evolved over a long period of time. Most traditional anti-malware solutions in use today are the result of years of development, with much of their evolutionary updates done to the same code base originally created for the ancient operating systems (OSs) of yesteryear.

Like any software company, Microsoft releases new OSs every few years. Each of those OSs includes dramatic changes to their core kernel. Those changes mandate equivalent changes to protective software such as anti-malware solutions. At a high level, anti-malware solutions operate very "close" to the kernel, intercepting file system calls and monitoring processes and process threads. Architecturally, anti-malware's close proximity to the kernel itself requires it to evolve with the OS. Ultimately, as Microsoft releases new OSs, anti-malware solutions must change to support each new version. One problem is that such solutions must also support legacy OSs. As such, traditional anti-malware solutions grow heavier and heavier with each new OS release, making their use less optimized over time.

Further, the ways in which the "bad guys" write malware evolves over time as well. The growth in malware code base accommodates each OS release, addresses new attack vectors, and includes new features. The vast majority of commercial anti-malware software has grown from simple virus scanning to comprehensive suites that provide protection from viruses, malware, and spyware; some also include firewall features. The goal of these products is to provide total endpoint protection from every possible angle. Although they can provide greater protection than their predecessors offer, much functionality has been bolted on and shimmed into the products in a way that places much higher demands on system resources. The higher resource requirement forces companies to make critical decisions about how their systems will be protected.

The first option is to purchase more expensive hardware (more RAM, faster processors) to ensure that the system and anti-malware suite perform at acceptable levels. This approach may resolve the issue; however, IT budgets are tight. Dumping money into hardware just to accommodate slow software is always a poor business decision. The most common solution is to limit the components that are implemented or come up with creative solutions in order to maintain optimum performance. Ultimately, throwing hardware answers to what is really a software problem is not a smart solution. Needed are improvements to the software itself that reduce the performance impact of anti-malware solutions overall.

---

## Multiple Endpoint Products Performing the Same Function

There are also circumstances in which an anti-malware suite may excel in one area but be deficient in another. To accommodate for deficiencies, an enterprise may choose to install multiple products on the same system to achieve the best level of protection. This overlap can have a huge impact on performance and potentially result in an unstable system or products that are ineffective.

A common issue that occurs when multiple products are installed is an overlap in functionality. For example, each installed product is performing real-time scans simultaneously. In this situation, each product requires every file to be scanned before it is available to the user. This delay in opening files and applications will be very visible to the user. In some cases, the conflicting products will create a situation in which files are not scanned at all or they are never allowed to be opened.

Running two or more products also complicates the task of troubleshooting application and performance issues. During the troubleshooting process, a determination has to be made as to which product is doing what. This will help determine the product in need of further investigation. Once the offending product has been identified, the issue may be resolved, but at what cost? What was the offending products' role? If it is uninstalled or disabled will that put the system at risk? Can the product be reconfigured so that the issue won't return?

Although it might be possible to run two products in a complementary manner, rare is the vendor that will recommend and/or support such a configuration.

## Scan Methodologies

Another contributor to slow performance with anti-malware software involves scan methodologies and the engines that run them. Before examining the different scanning methodologies, it is important to discuss the processes and mechanisms that enable scans to work in the first place:

- **Malware Signatures and Definitions**—The first and most well-known method involves malware signatures or definitions. These definitions encompass a list of known viruses or malware and the marks they leave on an infected system. These breadcrumbs are used when a scan is performed. While performing a scan, the engine uses signatures as a reference to compare against the OS state and files. If something is found that matches a signature, it's marked as infected, blocked from execution, and quarantined or deleted.
- **Heuristics**—Heuristics are used to identify infected files where no signature is readily available. The benefit of an effective heuristics engine is that systems are no longer exclusively dependent on the receipt of signatures in order to stop an infection. Heuristic scanning is a very complicated process that infers certain behaviors as being malware-like. Due to this complexity, in some cases, legitimate files can be marked as infected.

- Behavioral Analysis—Like heuristics, behavioral scanning provides the ability to detect malware without relying on definitions. Behavior analysis examines the actions of a program in order to identify malicious activity. Some examples of suspicious program actions include writing to protected parts of the OS or registry. This is considered a malware-like activity because legitimate applications don't display these behaviors. Eliminating the dependency on definitions for threat detection has tremendous benefits; however, there can be a risk of false positives when legitimate but poorly written applications are used.
- Emulation—Another method that has been developed involves emulation. Here, a potentially malicious application is opened in a protected area to identify malicious behavior. This protected area emulates the OS so that files can be opened and analyzed for malicious activity in a protected and temporary environment. If the file is infected, it can be allowed to perform all its actions, which then allows heuristic and behavioral analysis to be fully performed without harming the actual system. Once the execution and analysis has completed, the emulated environment and all the changes that were made are safely removed. Good heuristics and the use of emulation have become increasingly important in confronting modern attacks, as the possibility of zero-day exploits has dramatically increased in recent years.

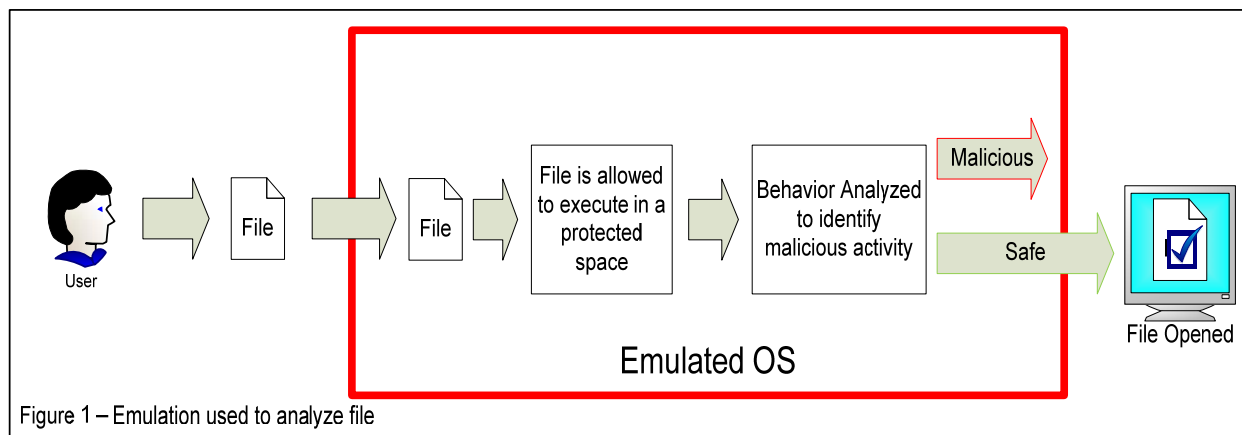


Figure 1 – Emulation used to analyze file

### Real-Time Scans

Real-time scans are often the first method of scanning to prevent systems from being infected with viruses and malware. Real-time scanning requires a client that runs continuously and monitors every file that is opened or executed. When a file is opened, it is first scanned by the engine and evaluated using one or more of the methodologies previously described. Real-time scans act as the first line of defense against malware because they monitor the OS and all attempts to change protected areas such as the system files, registry keys, and system services.

---

Traditional real-time scans can have a negative impact on performance because the file being opened must first be scanned. If the anti-virus software is slow or poorly written, files will take longer to open and programs will run slower because they must wait for the real-time scan to release its hold on files. This can have a direct impact on user perception of overall computer performance, resulting in decreased user productivity and unnecessary calls to the Service desk.

There are also risks to other computers on the network if real-time scanning is slow. It is possible for a system to become overloaded to the point where there are communication delays between the agent and its management server. In these situations, an overloaded agent may not be able to receive the latest definition files or provide status reports. If this were to occur during an active malware attack, delayed communication could result in an infected system. Another thing that will happen with more savvy users or support staff when performance is slow is that they can turn off their anti-virus software, which obviously then places the system at risk of being infected. Anti-malware solutions that do not incorporate a policy-based approach to defining client configurations are particularly at risk for these user behaviors.

### Scheduled Scan

The purpose of scheduled scans is to proactively evaluate all the files on a computer—some of which may be dormant—to detect viruses, malware, spyware, and adware. This approach is as critical as a real-time scan because it can find and stop the propagation of a threat before it is opened and given a chance to execute. Scheduled scans also have a negative impact on performance if the anti-virus client is slow or demands a significant amount of resources while the scan is being performed. Disk I/O is one resource that is heavily impacted—in addition to significant processing and RAM consumption. Slow clients will take longer to perform the scan and, during this time, the overall system performance will be slower as the client examines each file. This can be of particular concern with today's large hard drives as well as the amount and type of data being stored (for example, virtual machines, email archives, images, documents, and spreadsheets).

Many organizations attempt to alleviate this performance impact by scheduling scans during off hours; however, this is only a band-aid approach to what is really a core software problem. The off-hour approach may work fine for desktops that never move and can be left on overnight. Yet more and more companies are moving to a mobile workforce—they are replacing desktops with laptops. Day-to-day use with laptops is very different than with desktops because laptops tend to be powered on only when they are being used. With laptops, scheduled scans can run while the user is trying to use the system, thereby making it critical that the anti-malware software is lean and efficient while performing scheduled scans.

When such is not the case, performance is impacted by scheduled scans. To resolve user performance complaints, the decision is often made not to perform scheduled scans and rely solely on real-time scanning. In some cases, users may also stop a scheduled scan in order to restore system performance. These actions eliminate an important method of virus and malware detection, which puts the system and infrastructure at risk of infection.

---

## Client Reporting

For enterprises, administrators rely on the communication between the anti-malware clients and the servers that manage them. Clients are configured to communicate with management servers in a bi-directional manner for several reasons. The first is to enable the rapid distribution of malware signatures and client updates. The second aspect is the client reporting its status back to the server. Client status reporting is one of the most important aspects of limiting the impact of a malware infection; it relies on the ability to collect and analyze data from every client. The type of data that is needed includes the health of the client, which is determined by the version and/or date of the virus definitions on the client. Clients will also report back any infections that are found and the actions performed. This reporting enables administrators to assess the overall threat to their infrastructure and take appropriate action. Clients that are overloaded or slow to report their status limit an administrator's ability to properly manage and protect the infrastructure.

## Anti-Malware Shouldn't Be Slow

To address the ever-increasing sophistication of threats, software vendors have created more sophisticated anti-virus and anti-malware solutions, but the cost of this development is decreased performance both from the system perspective and from the anti-virus software itself. Many factors contribute to this poor system performance, such as code bloat, the requirements of OS support, and products that were bolted together over time to provide a suite of solutions. Only through the use of new and specifically-targeted solutions for anti-malware will today's IT environments ensure the highest levels of protection while maintaining good performance in their computing infrastructures.

---

# Article 2: 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

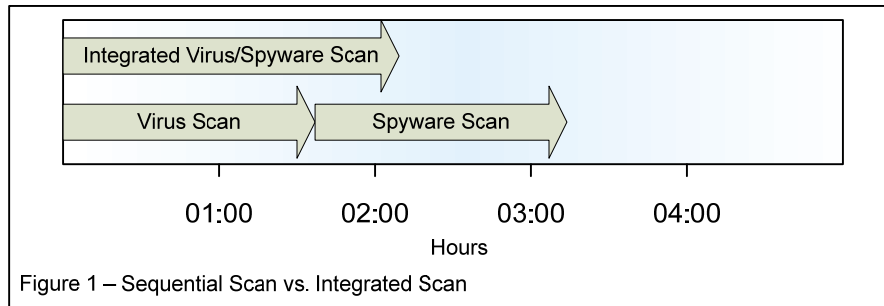
This discussion can also be extended to suites that include firewalls. With Vista and Windows 7, Microsoft made significant improvements in the built-in firewall, thereby making it optional to select anti-malware suites that include one. Windows XP, however, does not include a robust built-in firewall, 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.



### 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.

---

# Article 3: 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.