

INFORMATION TECHNOLOGY
INTELLIGENCE CORP.

VIPRE Takes a Bite out of Bloatware



October 2008

Executive Summary

“Bloatware causes more problems than viruses or malware. Server and workstation performance slows to a crawl. End user productivity suffers. Our administrators spend countless hours troubleshooting problems and reconfiguring the antivirus software. I can’t remember the last time we got infected with a virus. Bloatware though rears its ugly head on a regular basis.”

That statement by Andrew Baker, typifies the conundrum confronting businesses on a consistent basis. Baker is VP of IT Operations at Callargi, a Montvale, New Jersey-based database management and subscription fulfillment firm with 250 employees. For Baker, bloatware is a constant and unwelcome fact he lives with as his firm battles to secure its data.

Preventive antivirus and antispyware packages are “must haves” in today’s networking environments. No company from the smallest business with 10 users up to the largest enterprise with 100,000+ employees is immune from the security threats posed by rogue code, which include viruses, trojans, bots, zombies, spyware, spam, and blended malware. The threats have become more sophisticated, pervasive, and pernicious with each passing day. In addition, since the overwhelming majority of companies have intranets, extranets and Internet connections, malicious code can penetrate systems and networks in stealth form, from even trusted sites and circumnavigate the globe faster than you can say “Magellan.”

Antivirus/antispyware vendors, particularly market leaders like Symantec, McAfee, and Trend Micro have responded by retooling their products to defend against the latest threats. Unfortunately, instead of building a better, more efficient package, many of the market leaders have simply built a bigger package.

When it comes to antivirus/antispyware software, bigger is definitely not better.

To counter the latest threats, market leaders like Symantec simply stack new layers of functionality on top of their existing engines. The result: the ever expanding code bases of the leading antivirus/antispyware packages invariably result in bloatware.

This is especially problematic for small and midsized businesses like Callargi with 100 to 500 end users, because they usually have very limited administrative resources to root out and resolve the bloatware problems.

ITIC surveyed 50 small and midsized consultants and corporate SMBs with 30 to 500 end users. The intent was to elicit their views on the current state of the virus, spyware, and malware landscape and their issues with traditional security packages.

The results showed:

- Security is a top priority for 100% of businesses irrespective of company size or vertical market.
- An overwhelming 82% of the respondents indicated that bloatware and its attendant problems of performance degradation, lost productivity, and increased network management burdens are the worst security issue in their firms at this time.
- Bloatware slows workstation and server performance an average of 35% to 60% depending on the specific antivirus/antispyware package.
- Bloatware decreases individual end user productivity from 14% to 38% daily depending on the specific application that it impacts.
- Dollar value losses associated with bloatware due to lost end user productivity range on average from \$10 to an estimated \$60 per diem depending on the individual employee's wages.
- Even the newest "slimmed down" antivirus packages are still plagued with bloatware that slows down system performance by an estimated 15% to 20%, according to just over 50% of those polled.
- One out of four businesses of the survey respondents reported that their preferred method of coping with bloatware was to turn off their antivirus software, particularly on large server based accounting and database applications.

The remedy to bloatware is a better, more efficient product that is specifically engineered to scan, detect, and remove the myriad security threats without impacting performance and taking a big bite out of the IT capital expenditure budgets.

Sunbelt Software's new VIPRE Enterprise package is ideally suited to combating legacy and new blended malware threats from traditional viruses to the newest spam and Trojans. It optimizes overall system performance by incorporating antivirus and antispyware protection into a single engine that consumes minimal system resources and costs 50% to 75% less than competing products.

Introduction

Methodology

ITIC conducted primary research in preparing this report. That included the aforementioned survey of 50 SMB businesses and SMB consultants via email and first person interviews. ITIC also interviewed several industry analysts and researched the latest publicly available data on pricing and products obtained directly from vendors and their websites.

The Malware Landscape: Blended Threats Then and Now

Viruses have been an unwelcome fact of networking life since 1988 when Robert Morris Jr. launched his now infamous Internet Worm. Things have changed since then and in some very important respects, not for the better.

Twenty years ago, rogue code meant viruses or worms – period. Twenty years ago, the Internet was in its infancy; networks consisted mainly of unconnected LANs and there were no corporate extranets.

Today, networking technology and security threats have evolved to the point where stealth infections can invade one network and infect thousands of networks, oftentimes with the victims much the worse for wear before they even realize they've been hacked.

“In a 100 person network, a virus or malware can infect the entire corporate network within an hour,” noted Eric Sites, Chief Technology Officer (CTO) at Sunbelt Software in Tampa Bay, Florida and one of the leading architects of the new VIPRE Enterprise product. Depending on the type of malware, (i.e. HTML files) used in a hack attack, the rogue code “can spread outside the corporate extranet to customers, business partners, and suppliers within the next hour,” Sites added.

Malware itself takes many forms. Detection can be difficult, if not impossible until it's too late because malware is often hidden in trusted or legitimate sites or even embedded in something as innocuous as an E-card from a friend wishing a consumer or corporate user “Happy Birthday.” Older style antivirus packages, engines, and email filters are easily fooled and are hard pressed to keep up with the relentless spate of malicious code. Malware also masquerades as a run of the mill spam message. The twist: some infections will employ different links for the various items in the spam message with each link connection to a different legitimate site where the spam author has installed a rogue page. Malware also hoodwinks its victims because the malware sites so closely mirror legitimate, trusted sites when in reality they are near perfect facsimiles hosted by zombies. In this scenario, the malware authors use speed to escape detection. That is, their sites are online for short periods of time – usually no more than a few hours. This makes it nearly impossible for older defensive IP-address blockers and AV packages that only update their definitions once a week or longer simply cannot catch them.

Spam now comes in many forms from traditional advertising spam to PDF and Excel spam files. Additionally, attachment spam is often sent from so called “bots” or zombie computers that have already been compromised by Trojan infections. The spammers themselves are also more highly organized and efficient: they marshal armies of “bots” into super “botnets” which they then use to launch all out malware attacks with worldwide reach, like a high tech version of the popular board game “Risk.”

Corporate enterprises must also contend with an ever menacing array of phishing techniques

and blended threats that infect corporations and consumers from popular online sites like YouTube, Facebook, and MySpace.

The AV arena has also undergone considerable consolidation and commoditization. To more adequately address the threat of blended malware, market leaders like Symantec, McAfee, and Trend Micro purchased smaller security firms with the express purpose of bundling their specialized functionality into their core products.

Andrew Jaquith, principal at Security Benchmarking Advisors, a Boston-based consultancy, acknowledged that many of the leading AV products are bloated and ineffective. "It's a market fundamental that these security suites have gotten bigger," he said.

Jaquith noted that in order to combat the myriad malware threats, the top AV vendors added features like network access protection, USB port controls, antispyware, personal firewalls, etc. This increased the footprint of the code base. "Many of the legacy AV products grew by acquisition; Symantec bought Sygate and a white listing product, for example. When you jam all this stuff together [in a single product] you'll get software that has multiple agents and a lot of extra and unnecessary code," Jaquith said.

This approach of ladling a new software code or engine on top of a legacy AV engine creates a security Tower of Babel and inevitably results in bloatware.

In this atmosphere, nothing and no one is safe.

"If you look up the definition of Bloatware in the dictionary you'll find a picture of Symantec right next to it," said Drew Sanders, IT Manager at Allpak Container, Inc., a packaging and container company with 300 employees in Renton, Washington.

Sanders said malware and spyware are top challenges for his firm. He appreciates Sunbelt's newest weapon in the war against malware.

"The VIPRE Enterprise approach of a single engine to protect against blended malware, viruses, and spyware is the future," Sanders said. "Right now we're still layering capabilities onto the engine. And that does have an adverse impact on the footprint; it definitely increases consumption of our system resources."

Enter VIPRE Enterprise

VIPRE Enterprise is the successor to Sunbelt Software's CounterSpy product. Unlike traditional AV packages which were developed decades ago, VIPRE Enterprise has been designed from the ground up to deal with blended malware threats. It melds antivirus and antispyware into a single engine, thus conserving valuable system resources to enable corporations to achieve optimal system performance.

In other words, VIPRE Enterprise takes a big bite out of bloatware.

VIPRE Enterprise features include:

- **Real-time monitoring with Active Protection:** Active Protection includes three distinct methods to defend against malware. They are **signature matching** to compare files for an exact match against VIPRE's definition database; **heuristic analysis**, which examines the internal file characteristics to determine if it is malware; and, **behavioral analysis**, which observes and tracks the actions of specific code and program to identify malware.

- **A configurable dashboard:** This provides businesses with a centralized, policy driven malware management. It contains an agent deployment wizard which easily allows IT administrators to pick and chooses their deployment and configuration options.
- **Policy-based management:** This allows IT administrators to schedule quick and deep scans; set scan options for a variety of types such as known locations, the ability to scan running processes or cookies, and whether to allow or exclude specific database threats.
- **Report scheduling capabilities:** This feature gives IT administrators the flexibility to schedule reports to run at designated times; send the reports to specified managers or users.
- **Resource Usage monitoring capabilities:** This function gives IT administrators a detailed representation of VIPRE's low impact on system resources.
- **Extremely high detection rate:** Sunbelt Software automatically processes 40,000 to 50,000 pieces of malware during every 24 hour period. This enables Sunbelt engineers to proactively monitor and respond to new threats and keep their users protected.

Data & Analysis

Companies choose antivirus and antispyware for a variety of reasons beyond the obvious technical features and functions. Other criteria include:

- Ease of use
- Manageability
- After-market technical service and support
- Pricing

Users left no doubt when speaking to ITIC that bloatware, or more precisely, the desire to avoid the adverse effects of bloatware on system resources, dictated their everyday management and subsequent purchasing decisions.

Bloatware is far more than a mere nuisance; it actively drains workstation and server resources by consuming precious compute cycles. This, in turn, degrades desktop and server application performance. The performance impact can range from mild to severe and in extreme cases cause the application to hang. The end result: end user productivity suffers and network managers waste precious administrative time troubleshooting, debugging, and reconfiguring their software.

Bloatware Consequences

In worst case scenarios, businesses may be forced to uninstall their antivirus/antispyware packages or even forego using certain software applications. Consequently, the Total Cost of Ownership (TCO) increases and Return on Investment (ROI) is delayed. This is not mere theory; the issue has become serious enough for some consultants and corporate IT managers to sign up for courses that enable them to calculate and quantify the specific negative impact bloatware has on their systems and the subsequent time and monetary value associated with lost end user productivity.

One of those people is James Farnes, the principal at Farnes Computer a consultancy and training concern in Coconut Creek, Florida.

“Bloatware is a very critical issue .We can’t use or install certain products in certain environments because the performance takes too big a hit,” Farnes said. Though he’s complained to the leading AV vendors like Symantec and they have responded to a degree, their general attitude is not sympathetic.

“They tell us it’s a necessary cost of business and ask us: ‘Would you rather have slower system performance or a secure system?’”

Farnes doesn’t find that argument to be valid or helpful. “Some of the leading AV and antispyware vendors conveniently ignore the impact on TCO, ROI, IT departments, and end users – in other words, their customers,” Farnes said. According to his calculations, if a single end user’s productivity declines by 33%, the business would lose \$21 per worker per day for each fulltime salaried employee earning \$75 per diem as a direct consequence of bloatware.

“At that rate,” Farnes asserted, “a company would be forced to hire another person to compensate for the productivity loss due to bloatware.”

Michael Klein, lead consultant at Computer Directions, Inc. a New York City-based consultancy specializing in SMBs in the tri-state metropolitan area, agreed.

Security is a top priority for Klein’s corporate customers, but so are performance, reliability and end user productivity.

Klein takes a tough stance against bloatware. He advises corporations to turn off their antivirus and antispyware software if they experience significant performance hits due to bloatware. “It’s a risk, but bloatware is even riskier,” Klein said.

Large applications like accounting and databases are among those hardest hit by bloatware because there are so many reads and writes.

“If the sales, file, and billing files are very large, like 100MB, you may have 100 or 200 files that you’re opening and closing. If every time it opens you do an AV scan, performance takes a big hit,” Klein explained, adding, “and when you add a traditional AV package that now has antispyware included, companies are looking at performance hits of 15% to 20% on smaller applications; it’s even greater on accounting/database software – sometimes as high as 40% or more.”

With bloatware reaching critical mass, many users and consultants are opting to switch. That sets the stage for a new, efficient security tool like VIPRE Enterprise.

All of the businesses interviewed by ITIC, including those corporations that do not currently deploy Sunbelt’s VIPRE Enterprise, gave the product high marks for its overall effectiveness, ease of use, defensive capabilities, and the quality of its definitions. The users also extolled the quick, efficient response they received from Sunbelt’s technical support staff. Some 98% of the respondents told ITIC that they rarely if ever encountered waiting times of more than 10 minutes and got fast callbacks if they chose that option, and the Sunbelt engineers were almost always able to solve any issues during the initial phone call. By contrast, the IT administrators we spoke with said that wait times of an hour or more were commonplace when they called competitors like Symantec.

Finally, given the current economic volatility, corporations, are more cost conscious than ever. Corporations are to pay hefty premiums and upgrades to purchase a brand name

antivirus/antispyware package laden with bloatware, particularly SMBs who have fewer resources and generally smaller IT capital expenditure budgets.

Pricing will vary according to volume purchases as well as an individual customer's relationship with the AV vendor or reseller. Vendors will also offer steep discounts for those customers whose business they are especially keen to keep.

List pricing for Sunbelt Software's VIPRE Enterprise ranges from 33% to 70% less than similar tags for Symantec Endpoint Protection 11. In a 49-user configuration Symantec costs \$2,038 compared to \$1,369 for VIPRE Enterprise. However, several SMBs disclosed that they were able to realize even greater economies of scale – savings of 50% to 70% when they switched or upgraded to VIPRE Enterprise combination of all of the aforementioned factors that has tipped the scale in VIPRE's favor.

The Case for VIPRE Enterprise: Users Speak Out

Access Courier

Aaron Geiger, the lead IT manager at Access Courier, Inc. a logistics and transportation firm with 100 employees in St. Louis, Mo., switched to VIPRE Enterprise because he got fed up. He had had enough of paying a high premium for the bloatware that characterized Symantec's Corporate Edition product over the last six years.

"Each version [since version 7] consumes more memory and is more difficult to deploy for antivirus protection," Geiger said. His firm was already using VIPRE's predecessor, CounterSpy to safeguard against spyware. When he learned that Sunbelt was constructing VIPRE Enterprise he was anxious to test and install it. Access Courier has deployed VIPRE since spring 2008 when the beta version first shipped.

Prior to installing VIPRE, Geiger said bloatware from Symantec's AV software considerably slowed both workstation and server performance.

"The Symantec scanner doesn't optimize the memory footprint or the internal code to make it unobtrusive and more efficient," Geiger said. He conceded that Symantec did the job of protecting his network from malware and noted that Access had not had any viruses or spyware successfully penetrate the network in the last six years. However, that protection "came at the expense of performance and manageability." "If I built a clean Windows XP workstation and installed Symantec it would run 20% slower," he added. Geiger also found it problematic to apply patches in the Symantec environment. As the only IT manager for 100 end users, he didn't have the luxury of backup, so he found himself spending an extra three hours at night to deploy the patches across 40 or 50 machines. Sick of the technical and management challenges, Geiger said he finally told Symantec "flat out that I was not going to renew and was switching to Sunbelt."

Access Courier saw tangible TCO gains and an immediate ROI in terms of actual capital expenditure monies as well as performance and management gains.

The entire upgrade from CounterSpy to VIPRE was less than \$300 for all the machines for a two-year subscription, Geiger disclosed. "This is a 70% savings compared to the approximately \$1,500 annually that Access Courier spent on Symantec renewals," Geiger said, adding, "The management savings are even greater." Since all the updates are automatic he can control everything from his desk and the fact that VIPRE offers the flexibility to customize the

configurations and installation via the Wizard agent is also a great time saver.

“I just changed the policy to allow software updates and everything was completed with all of the new settings within 20 minutes.” In fact, Geiger said, his biggest deployment challenge was “un-installing Symantec which I could only do manually; it took 20 minutes per machine.”

For Geiger, Sunbelt’s superior technical service and support also proved a big incentive. “I haven’t had to come in once off-hours or stay late to do anything extra with VIPRE,” Geiger said. By contrast, he said, he spent an additional three hours every two months or 30 hours per year after hours reconfiguring the Symantec antivirus product. “Not only did I not appreciate working the extra hours but I don’t get overtime since I’m salaried,” he said.

Geiger noted that he’s “never waited more than four minutes on the phone to speak to an intelligent, helpful U.S.-based Sunbelt engineer.” This is in stark contrast to the 45 minutes he usually spent in queue waiting to speak to a Symantec Level 1 technical support person.

Overall, Geiger said, “VIPRE Enterprise has all been upside for us. It makes Access Courier more secure and it makes my life easier and my workday shorter.”

SOJ Consulting

Stanford Jack is manager of Client services at SOJ Consulting, Inc. in Vancouver, British Columbia, a firm which focuses on SMB companies with one to 100 end users. As Jack explains, he’s a one man show, which means he has to be incredibly efficient and get everything right the first time. Sunbelt Software’s VIPRE Enterprise helps him achieve those goals during the eight years he’s been using the company’s security products. Jack had all of his clients standardized on Symantec since 1997 and initially all was well until Symantec released version 10 in the 2005 timeframe. At that point, he began experiencing significant bugs and performance degradation during the installation process. The situation did not improve with the subsequent Symantec version 11 which shipped in 2007, Jack said. Since he was already using Sunbelt’s CounterSpy Enterprise with good results, he decided to try VIPRE Enterprise in his own office.

“I was amazed at how easy and quickly it deployed – in just about 15 minutes – with no problems,” Jack said. He was further impressed when he tested VIPRE Enterprise against some known viruses that Symantec version 10 had trouble removing; specifically, the Antivirus XP2008 malware application that gets sent through as an attachment as a SPAM message from UPS and CNN announcements. “Every customer I have that got hit with it had Symantec 10. When I tested this same piece of malware against VIPRE Enterprise, VIPRE stopped it dead in its tracks and quarantined it,” Jack said. He was also impressed at how quickly VIPRE performs system scans – on average “10% to 15% faster” than competing products from Symantec, Trend Micro, or McAfee, he said.

Jack found the bloatware problem “extremely disturbing.” Jack said he was also perturbed that Symantec’s AV software was not catching all of the malware. “The default for Symantec even after all these years is to do a random once a week check for new updates. Sunbelt does random checks every four hours, so they’re bound to catch a lot more malicious code and in real time,” Jack said.

VIPRE Enterprise’s pricing was also very attractive and 50% less expensive than the roughly \$45 SOJ customers paid to renew their Symantec workstation and Email server licenses per client and server. Such cost savings are a big boon for SOJ micro SMB accounts that have 10 users or less. “A Symantec 10 user license that cost \$400 only costs \$200 for VIPRE

Enterprise,” Jack said.

Like his SMB peers, Jack gives Sunbelt’s technical service and support group high ratings: 9 on a scale of 1 to 10. “Whenever I’ve encountered a glitch with a Sunbelt product, their technical support is very responsive; they stay right on top of things and most of the time, my wait to speak with someone is less than 10 minutes,” Jack said. “I’ve been so impressed with their efficiency that I’ll just leave a message and they call me right back. The only company that has service people as good as Sunbelt is Microsoft,” he asserted.

“There is no incentive for me to go back to Symantec for antivirus/antispyware protection. Sunbelt’s VIPRE is better in every respect; it’s easier to deploy and more efficient at capturing and isolating viruses and malware for half the price,” Jack said.

Brown University

Rick Smith, network manager at Brown University’s Center for Alcohol & Addiction Studies (CAAS) in Providence, RI, is a tough taskmaster who tests multiple products until he finds just the right combination of performance, efficiency, and price.

“VIPRE Enterprise works well and it doesn’t tax my system,” Smith said, who said he was impressed by the speed and [smaller] footprint of VIPRE.

“Typically, you don’t notice how good something works when it works well and performs as it’s supposed to like VIPRE. I notice when my security software hangs. Anecdotally, at minimum VIPRE is twice as fast as competing products and I’ve never seen it experience a glitch. It just runs all the time,” Smith said.

The Brown University network administrator also praised Sunbelt’s “excellent technical service and support” and VIPRE’s competitive pricing. “Sunbelt has excellent people on the other end of the phone supporting the product. I don’t like to pay for rudeness,” Smith said.

Alternative View

Not all of the customers ITIC spoke with are deploying VIPRE Enterprise – yet.

Sanders at Allpak Container said his firm has used Sunbelt’s Ninja antispam and the CounterSpy products. In head to head benchmark tests between Sunbelt’s Ninja and McAfee’s comparable product, Sanders said his firm found Ninja performance to be 60% more effective and easier to manage. So while he does have some reservations about VIPRE, mainly with respect to its ability to deliver enterprise class management capabilities, the stellar performance of Sunbelt’s other offerings opens the door for VIPRE Enterprise.

“Sunbelt Software has a lot of credibility with us and that bodes well for VIPRE. But I have to conduct more research specifically as to how I’ll easily manage 200 desktop installations,” Sanders said.

Sanders, who describes himself as a “very satisfied McAfee customer,” said that nonetheless, if “VIPRE can provide the same level of enterprise manageability as well as the product functionality [as McAfee], then I would consider using it because then you get to the price and Sunbelt is about 30% cheaper, so that’s the tie breaker.”

Recommendations & Best Practices

Before choosing any new antivirus/antispyware product, ITIC advises corporations regardless of size or vertical market to conduct due diligence in advance. Companies should consider the following criteria when choosing antivirus/antispyware software:

- Features and functionality
- The size of the footprint and the potential impact on system resources
- Types of protection mechanisms
- Manageability
- Ease of use
- Integration and interoperability with legacy and planned infrastructure and devices
- After-market technical service and support from the vendor
- Pricing

As any security professional or security administrator knows, even superlative antivirus, antispam, intrusion detection, authentication, tracking, and other security measures can be defeated by human error or misconfiguration.

ITIC advises customers to strictly adhere to safe computing policies and practices and enforce them. Careful attention to detail doesn't cost anything extra but it will pay off handsomely in both the near and long term, and assist organizations in keeping their corporate data secure.

Sunbelt CTO Sites offered the following "To Do" list to assist corporations with their VIPRE Enterprise deployments. They include:

- **Administrative access should be granted on a strict absolute "need to have" basis.** Sites recommends keeping one account for administrative access and a second account as a working account for installation and configuration. "Giving someone administrative access can be very dangerous. It's all too easy to install a rootkit that steals corporate information and spirits it out of the company," Sites said.
- **Remove all unnecessary communication paths between computers and servers.** The IT administrator should also restrict *what* a computer can communicate. So for example, if there is an employee who has no back end applications installed, simply remove unnecessary communication paths between computers and servers which in turn will limit the scope and the damage of any potential infections.
- **Turn off Auto Run on USB Keys.**
- **Segment the network.** Run some type of Universal Threat Management (UTM) devices at the edge of the network. Companies with more than 100 users should segment the network to minimize the scope of any hack.
- **Ensure that AV signatures are current.**
- **Minimize the footprint on the corporate desktop.**
- **Disable unused features on desktop systems.**

Conclusions

Hackers and rogue code writers will continue to ply their trade and create new, ever more efficient and pernicious viruses and blended malware threats. This will in turn, cause many of the antivirus vendors to continue to expand their code base. Unless or until the leading antivirus/antispyware vendors re-architect their products from scratch, as Sunbelt has done with VIPRE Enterprise, bloatware will continue to abound.

Though the latest version of Symantec is somewhat slimmer than prior releases, ITIC survey respondents noted that it was still approximately 20% less efficient than VIPRE Enterprise.

VIPRE Enterprise has been specifically designed to address today's blended malware threats via its virus intrusion prevention remediation engine, fast scan on boot technology, and kernel level Active Protection.

VIPRE Enterprise is backed by Sunbelt Software's excellent technical service and support team which garnered universal praise from all the users surveyed by ITIC.