TECHNICAL ARCHITECTURE REVIEW

Project Name:	**Desktop Virus and Spyware Protection**
Requestor:	**Jim Matsumura and Michael Casey**
Date of Initial Request:	**October 31, 2007**
Request Description:	Enterprise Security is working with Administration and Contracts to develop or renew the purchasing vehicle for Virus Protection and Spyware. Currently there are three or four major packages in use. Do we need purchasing mechanisms for all of these products or should be developing an enterprise standard?
Agency or Agencies:	**Enterprise**
Reviewers:	**Bob Woolley**
ARB Acceptance Date:	
Agency Requestor Acceptance Date:	

Introduction

Trojans, viruses, worms, and other types of malicious code continue to be the most serious threats facing the State. There is a need for more proactive virus-detection techniques because of the rising number and severity of threats entering networks. Reactive signature-based antivirus (AV) technology alone does not provide an adequate level of threat protection. Real-time behavior analysis, using heuristic algorithms, is emerging to complement signature-based antivirus products.

The digital threat environment is rapidly changing not only in the motives of malware writers but also in the vulnerabilities they target. E-mail borne viruses were the most attractive weapon of hackers who sought to damage or disrupt business operations. The Web has now become the preferred vector for malware attacks.

IDC indicates that Trojans, viruses, worms, and other malicious malware continue to dominate as the number one the threat for enterprises of all sizes. Spyware has been identified as the number two threat. Bots are becoming more prevalent as a threat environment, using the Web as a distribution and propagation tool and are almost undetectable.

In a separate IDC survey, 35% of respondents reported successful attacks against their enterprise, while 24% reported 10 or fewer successful attacks. Additionally, 27% of respondents from very large companies stated that they had 10 or fewer successful attacks on their enterprise.

While no antivirus or spyware method is foolproof, something is clearly better than doing nothing.

Objectives and Scope of Review

This review looks at antivirus and anti-spyware solutions for desktop deployment. The objective is to consider the advisability of an enterprise standard that incorporates antivirus and spyware detection, and analyze the economic value of such a standard to the State.

Baseline of Current Architecture

Baseline data has been derived from a data summary by the Security Office and by a direct query of the ZenWorks database. From a numbers perspective, the data in Table 1 shows a large installed base of McAfee products which appear to represent a defacto standard. Table 2 reflects the installed base by agency. ZenWorks data was collected based upon a sample of 14,532 desktop and laptop devices, and reveals some interesting additional information and concerns.

Table 1. Security Office Virus Protection Information—Summary Data

Vendor	Licenses	% of Total
McAfee	17,044	82.1%
Symantec	1,912	9.2%
CA	1,750	8.4%
F-Protect	60	0.3%
	20,766	100.0%

The summary in Table 1 would lead one to conclude that McAfee is a de facto standard. While this is true in an aggregate sense, a closer look at these figures reveals diverse installed versions of McAfee including versions 4.51, 7.0, 7.1, 8.0, and 8.5, with significant quantities in all of these categories. The McAfee installed base primarily represents Virus scan and does not include the full security suite.

The Symantec installed base is primarily limited to virus scanning software. The CA installed base represents 402 installations of the integrated security product and the balance are e-Trust virus scanning software. Other vendors also represented with installed AV solutions include ALWIL, BigFix, Cheyenne, Grisoft, and H+BEDF GmbH.

The level of AV implementation is suggested by a detailed analysis of 351 DTS desktops, largely on Capitol Hill. Detailed analysis reveals the following:

- Desktops with November AV Signatures: 49, or 14.0%.
- Desktops with the most current AV Signature: 12, or 3.4%.
- McAfee Installed Base (All Versions): 153, or 43.6%.
- Norton Installed Base (All Versions): 197, or 56.1%.
- Other: .3%.

DTS data does not appear to be any better or worse that the State at large, so this data should be representative of what can be expected on a State-wide basis.

Virus definition currency is generally very dated. Of the 14,532 workstations scanned by ZenWorks, it is estimated that less than 14% are using current November 2007 virus definitions. Hundreds of the virus definition files are older than one year, and range to three years behind current versions. There are also hundreds of workstations that have multiple virus protection products installed. Given the version diversity and dated virus definition files, the level of protection is somewhat limited. The Tax Commission appears to be the only agency that has a significant installed base of integrated threat detection products, which represents a best practice for AV and related threat protection. There are few instances of any AV products that rely on advanced behavior detection. The vast majority of the AV base relies solely on virus signature files.

Table 2. Security Office Virus Protection Information—Customer Detail

Agency	Software Solution	Installed Base	Expiration Date	Renewal Year
ABC	McAfee/ePO	150	12/5/2007	1
Commerce	McAfee/ePO	450	12/5/2007	1
DAF	McAfee/ePO	355	12/5/2007	1
DAS (General Services)	McAfee/ePO	25	12/5/2007	1
DAS (Purchasing)	McAfee/ePO	20	12/5/2007	1
DAS (State Finance)	McAfee/ePO	125	12/5/2007	1
DTS (DET) DHRM	McAfee/ePO	1,607	12/5/2007	1
DHS	McAfee/ePO	4,021	6/30/2008	1
DNR	McAfee/ePO	1,200	Nov-08	2

DOH	McAfee/ePO	1,500	Dec-08	2
DPS	McAfee/ePO	1,502	2/14/2008	1
DWS	McAfee/ePO	3,001	11/21/2008	2
Governor's Office	McAfee/ePO	150	Sep-08	2
UDOT	McAfee/ePO	1,500	12/5/2007	1
DCC	Symantec	287	Apr-08	1
Insurance	Symantec	125	3/3/2008	1
UDC	Symantec	1,500	Jan-08	1
DEQ	CA eTrust	500	Jun-08	1
Labor Commission	CA eTrust	150	3/6/2008	1
USTX	CA eTrust	1,100	12/4/2007	1
DFI	F-Protect	60	7/31/2008	2
Executive Branch Totals		19,328		
Attorney General State Auditor Crime Victim Reparations State Treasurer	McAfee/ePO	498	12/5/2007	1
State Totals		19,826		
SWUT Public Health Utah County Weber County Library	McAfee/ePO	940	12/5/2007	1
Total Licenses		20,766		

By contrast the desktops being billed to agencies for desktop support total 22,087 as of November 2007 based upon data provided to the Office of Planning and Budget (OPB) for rate impact calculation purposes.

Market Overview

The three main leaders in the enterprise marketplace are Symantec, McAfee, and Trend Micro. Gartner points out that the leaders have been slow to respond to new threat profiles, and slow to release new signatures for evolving threats. They are just beginning to consider behavior based approaches. Symantec and McAfee have both been criticized by customers for products that are overly intrusive and have unacceptable performance impacts.

Gartner places these three vendors in the leader portion of the magic quadrant. Most of the smaller and more innovative companies are not included in this analysis. Companies like CA are characterized as “niche players.” Some of the most interesting antivirus solutions are from smaller, and in many cases, non-USA based providers, such as F-Secure from Finland.

There is a substantial gap in the review literature on the effectiveness and capability of many of these leading products. Gartner rates them highly, but in the consumer space Symantec and McAfee have relatively weak ratings.

A variety of smaller vendors have released products with less impact and a number use behavioral detection technology. Large market share does not necessarily equate to the best products in this space. Customers are asking for an antivirus layer with enhanced behavioral protection, firewall, and antispam protection to create a unified antithreat security suite, with centralized management capability.

Best Practices Review

Best practices in this area are sometimes divergent from an operational perspective (e.g., use a wide variety of solution products to ensure detection but manage centrally), which is pretty difficult to do. Given the trend away from product specific solutions toward security suites, new best practices include the following:

- Implement a security suite from a vendor that provides:
    - virus and spyware protection using both signature based and behavioral detection methods;
    - an effective personal firewall for each workstation, with capabilities for allowing centralized software distribution and updates;
    - central management of the security suite across the enterprise;
    - Network Access Control (NAC) capability that denies access to network computers that do not meet defined antivirus, spyware, and firewall policy requirements;
    - aggregated threat detection reports across the enterprise; and,
    - security policy based implementation capability.

- Select security suites based upon reliability, manageability, and economic benefits for standardization across the enterprise.

- Ensure that network computers have a single updated instance of antivirus, spyware, and personal firewall software that imposes minimal performance impacts on end user computers.

- As a matter of operational policy, do not allow end users to turn off antivirus, spyware signature, and operating system updates.

- Use Web security gateways and XML firewalls to minimize security risks from the Web and Web services as malware payload carriers.

- Establish security policies that mandate antivirus, spyware, and personal firewall implementations on all network computers and enforce the policy.

Emerging Technologies and Trends

The antivirus market seems to be evolving from product to suite and will ultimately shift toward more comprehensive security solutions. Antivirus will be increasingly sold as a feature of endpoint security, messaging security, Web security, and network security solutions. For example, antivirus and antispyware have already converged into effective single solutions on the endpoint. Effective firewall solutions for desktops are available from many vendors.

IT organizations are requiring fewer agents on the desktop, less performance impact, and a less intrusive kind of solution. Organizations increasingly want to be able to manage endpoint security with a single console for consolidated administration, policy, and reporting. IDC and Gartner suggest that behavior analysis technologies, such as advanced heuristics, with traditional signature based antivirus technologies, will allow for a greater degree of accuracy in detecting both known and unknown threats.

Financial Analysis

Moving to an integrated security suite approach will increase costs to the State, but will also provide consistent protection from spyware, a personal firewall for each workstation, and a consistent approach to deploying AV signature files to the enterprise. Security office analysis suggests a four year current cost assumption of $205,583 to $240,000 for maintaining the current approach using nothing but AV signature files with a current vendor such as McAfee. This approach effectively provides the same level of detection the State has today. If a best practice security suite approach is taken for a broader range of threat detection, Gartner and IDC suggest that costs would approximately double. Even if the same approach is maintained with no added value, a different automated method is necessary for maintaining virus definition files. From an enhanced security perspective, the integrated approach has more actual security value and provides a common management and monitoring approach potential across the enterprise.

Security Review and Analysis

The current AV environment provides only limited AV protection and spotty protection at best for spyware and other types of intrusion that could be implemented with a personal firewall approach. A more comprehensive and single vendor approach would seem to be in the best interest of agencies and the Security office.

Operational and Infrastructure Analysis

Workstations, as currently managed, represent a threat to the enterprise. There is too much variability in the installed base to guarantee a reliable method of protection. From a network perspective, it would be much more secure if Network Access Control could restrict access from inadequately protected devices. This becomes feasible if the State implements a common standard across the enterprise, and could be implemented on an automated policy level.

Solution Delivery Impact and Analysis

There is no significant impact for solutions delivery from an AV perspective. The greater risk is with viruses, bots, and SQL injection issues that can be placed into Web services payloads with little or no possibility of detection. An XML firewall should be considered to mitigate this risk.

Agency Services Impact and Analysis

An enterprise AV standard impacts agencies significantly in terms of existing business practices. A single standard can add value in terms of reduced costs, but the greatest value is in the area of enhanced manageability of the threat environment. A great deal of coordination will be required with LAN administrators to gain management benefits, and to ensure that workstation firewalls don't hamper LAN staff ability to use push technologies for software updates and distribution.

Summary and Recommendations

Recommendation 1: **Implement an enhanced AV solution with integrated threat detection.** Enhanced AV solutions can bring a lot of security. When they include personal firewalls, host-based IPS, content filters, phishing filters, and more, referring to these packages as anti-virus solutions is misleading. Layering on all of those security capabilities and managing them through a consolidated console can significantly improve enterprise security. Enhancements increase the cost of basic AV-only packages.

Recommendation 2: **Multi-platform coverage improves efficiency.** While almost the majority of workstation users use Windows platforms, the environment is getting more diverse. Diverse platform environments should focus on solutions that support them all. Deploying multiple AV solutions within the enterprise increases cost and management requirements, decreasing operational efficiency.

Recommendation 3: **If all else is equal, buy the cheapest solution.** AV is essentially a commodity capability. The baseline functionality between the providers is essentially equivalent. If two products exist that equally meet the needs of the enterprise, go with the cheapest. McAfee, from an installed base perspective, is an adequate solution, especially if the security suite approach is chosen.

Recommendation 4: **Leverage volume procurement to reduce cost and simplify deployment.** Implement an overall solution that brings all agencies under a single procurement timeline. Do not hesitate to replace an incumbent solution. Implementation of a new solution will be easier and the cost savings can be significant.

Recommendation 5: **Adopt a management plan that enhances existing security.** Be sure business processes are in place that ensure consistent implementation across agencies, and automated update methodologies for AV and spyware signature files. From a network security perspective, ensure that workstations logged into the network meet minimal AV standards. Do not allow virus software to be disengaged at the user level.

Recommendation 6: **Minimize the AV and spyware impact on workstations.** Avoid deployment of AV and Spyware solutions as separate vendor applications because of the performance impact on the user's computer. Most leading vendor detection suites are now combining both capabilities.

Implementation and Migration Considerations

- ***Procurement:*** Establishing a single AV vendor would be in the best interests of the State. Competitive pricing could be accommodated with a request for bid. Pricing assumptions need to consider staggered contract due dates that currently exist among agencies with provision for a consolidated State-wide renewal date.

- ***Migration and Configuration:*** Once a vendor is selected based upon competitive bid responses, an implementation and rollout plan must be developed that includes:

    - Removal of existing installed AV and spyware software, including necessary automated registry cleansing, prior to installation of the approved product will be necessary.

    - Configuration profiles for AV and other integrated software (e.g., personal firewalls) that will ensure automated AV signature updates and provision for software distribution within the personal firewall environment.

    - Timelines for each agency installation that respects existing contractual obligations.

    - Evaluation of NAC control options that ensure that AV is present with network connected computers and other mobile devices.

- ***Other Issues:*** Spyware detection is variable at best, through existing suites, although detection is improving rapidly. Spyware vendors such as WebRoot also supply other security solutions, such as AV, so major spyware vendors should also be included in the AV bid process.

- ***Cost Recovery:*** An integrated approach to AV, spyware, and personal firewalls may be more costly than separate AV and spyware approaches. A plan to recover increased costs needs to be developed.

A final product recommendation is primarily a consideration of cost and related security value. AV is a commodity product and should be procured with that in mind. Taking a more comprehensive approach, from the perspective of endpoint security, seems to be more productive than just considering AV and spyware in their existing context.

Summary of Agency Review Comments

Comments and questions were received from the Department of Insurance as follows:

Question 1: What is considered minimal impact on a system? 5% ...10% of resources? Experience shows that these all-in-one products are resource intensive.

Question 2: Have other forms of system protection been considered (or even tested), such as BufferZone (http://www.trustware.com/index.html) and EyeBlink (http://www.eeye.com/html/consumer/products/blink/index.html)?

Comment 1: Some thought should be given to proper configuration of a workstation. Allowing users to have administrative rights is not a best practice, and though it will not eliminate spyware/adware it does greatly reduce the number of incidences. To what extent are agencies allowing users to have administrative access? How many agencies mandate that, if users are allowed administrative access, applications (if possible) run with reduced access using such tools as Privbar, PolicyMaker, MakemeAdmin, and Sandboxie? Some reference needs to be made in this regard.

Comment 2: How big is the problem of spyware, adware, and viruses in the State? Is it pervasive, or just limited to a few users or agencies? Can implementing system restrictions eliminate the issues caused by a few?

Comment 3: What is most important to the agencies? Is it management and system performance, or is it having the best protection out there?

Comment 4: Do the desktops in the State have the same incident rate as mobile users with laptops? If laptops, would it be better to enhance the protection of these devices rather than for the whole State, which may not need it?

Comment 5: The report mentions different systems in use within the State. What are these systems? What are the options for these other systems?

Comment 6: Can the proposed solution integrate with NDS or Active Directory for efficient policy based management?

Comment 7: Implementing a single security suite is against best practices of multi layered security. Putting the State on a single security suite may lower acquisition costs, but it does not take into account incident costs. Separate vendors need to be at each level if possible: at the gateway, at the server, etc., due to the fact that different vendors react at different levels and rates. If a type of malware is able to bypass the security suite the whole State is affected. If, however, half of the State is on a second security suite, that second security suite may be able to block the malware that the first suite let through. What would be best is a single management console that can manage the diversity of security of products.

Comment 8: Since spyware/adware is highly resistant to signatures based protection, more emphasis should be placed at the perimeter where e-mail and Web content can be managed to exploit the ability to natively understand content. This scenario would catch the majority of malware before it even reaches the user. With a properly configured workstation the products installed on the client would essentially be protection against each other and for the malware that gets through perimeter defenses.

Observations

- The Insurance Department, for the past three to four years, has limited all users to "User" access on windows desktops. Only a handful of users have administrative rights, and only due to the fact that the users need to be able to change network settings on the fly, though we are testing a solution now to eliminate this need.

- The Insurance Department also has used, for the past four years, Symantec's client security product which includes a desktop firewall (which, by the way, has maintenance costs essentially the same as for just having A/V protection).

- The Insurance Department also utilizes the auto update feature of Windows for workstations to ensure that desktops (not servers) are up to date.

- The Insurance Department also has had, for the past four to five years, a modified policy applied to each desktop to enhance security on the desktop.

As a result of these changes we have had no instances worth noting involving spyware or adware, as well as virus outbreaks.

References

Beyond Signature-Based Antivirus: New Threat Vectors Drive Need for Proactive Antimalware, Adapted from Worldwide Antivirus 2006–2010 Forecast Update and 2005 Vendor Analysis by Brian E. Burke, IDC #204715, July 2007

Protection Hallawell, Arabella, and Peter Firstbrook, *Magic Quadrant for Enterprise Antivirus, 2006,* Gartner RAS Core Research Note G00141873, August 31, 2006.

Roiter, Neil, *Web Security Gateways Meet Rising Malware Threats*, Security News: SearchSecurity.com, July 12, 2007.

Vendor Landscape: Inject the Right Anti-Virus Solution, InfoTech Research Group, October 3, 2007.