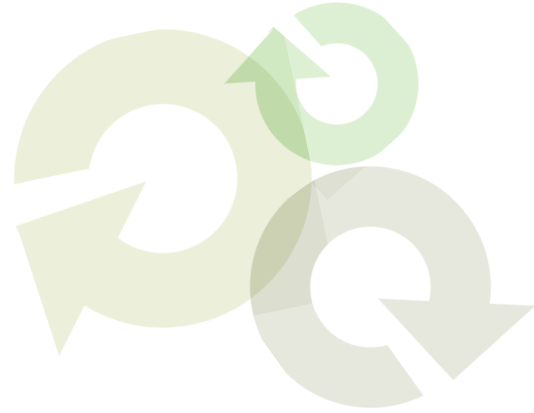




WhitePaper:



Security "Point" Solutions are Not a 4 Letter Word:

*Why Purpose-Built Solutions for Patch and
Configuration Management Continue to be
a Good Thing*



WhitePaper:

Security "Point" Solutions are Not a 4 Letter Word:

In recent years there has been a substantial amount of consolidation in the IT security industry. There were over 20 significant security related acquisitions in 2007 alone. Google acquired both Postini and Green Border, IBM bought Watchfire, HP bought SPI Dynamics, Checkpoint acquired Pointsec, Symantec snapped up Vontu, and there were plenty of others.

Large vendors with a healthy appetite for acquisition would have buyers of security software believe that this consolidation is a good thing; that bigger is better, that *built-in* is tops, and that individual best-of-breed point products are a nuisance to be avoided, a four letter word if you will. While consolidation can be a good thing, flying the same corporate brand doesn't always equate to integration or operational efficiency.

Patch management is a good example where an individual point solution is not only desirable, but may be required. While acquisition-hungry vendors have tried to deliver broader functionality by adding patch management function into their suites, there will always be a need for 3rd party patch management tools. There are a number of reasons why. Consolidation of patch management functions is tough to do correctly. Suites offered by the big guys don't provide best-of-breed patch management capability —they lack patch content, patch-specific targeting or patch reporting.

The same situation exists for security configuration management. Most suites offer patch and configuration management as part of a larger "PC lifecycle management solution." But these suites lack the substance and depth to give you confidence that your systems comply with corporate security policies – or at least that you can "prove" your systems comply. There is certainly a case to be made for solutions that promise to streamline compliance costs and improve your security scorecard. But the false sense of security that results from deploying a suite of "integrated" products can leave you with misconfigured devices that expose data to exploits and internal misuse.

Examples and side effects of consolidation gone wrong include a lack of any real integration, slowing of patch management innovation and new releases, lack of flexibility, diminished focus on actual security issues, big expensive *bloatware* when lightweight focused solutions will do better, and being locked into a specific, inflexible, vendor specific approach. With all of the consolidation and investment in more expensive and larger systems, the end customers are not necessarily seeing any added value. Let's examine some of the issues.

*This document is
provided strictly as guide.
No guarantees can be
provided or expected.*



WhitePaper:

Security "Point" Solutions are Not a 4 Letter Word:

Inherent bugs, weaknesses and security vulnerabilities

All operating systems, applications, and even hardware have inherent bugs and weaknesses that can be exploited if operating systems and applications are not patched or devices are misconfigured. That premise has existed since the beginning of software development. It isn't going to change anytime soon, at least not until developers produce bug free code. Third party patch management products act as back up safety nets and address vulnerabilities that are bound to be present in larger systems.

While security vendors and technologies will continue to be acquired and imbedded within larger systems, new, best of breed patch management, configuration management, and other security solutions will necessarily keep emerging to address the ongoing and ever-changing security threats.

Bigger isn't always better

In the wake of consolidation, some acquiring vendors will have you believe that the best solution is the one that covers the widest range of IT tasks. Yes, breadth is important, but for configuration and (especially for) patch management depth, completeness, and accuracy cannot be sacrificed for system width. A solution that is a mile wide but only an inch deep won't provide the protection needed by organizations that are prime targets for attack.

For instance, vendors that primarily provide network or systems management solutions are not really focused on security, let alone the specific aspect of patch or configuration management. Security is an afterthought or a checklist item only. While they might acquire various patch management technologies and configuration management tools and bolt them on top to give the appearance of security across a wide scope of applications, the companies themselves are focused on other things. Patch and configuration management security features from such vendors tend to languish and fall behind.

Most consolidated solutions lack real integration

It is very difficult to correctly integrate multiple technologies and products into a cohesive solution, or suite. Although there are exceptions, the "integrated solutions" offered by most vendors today are not really integrated at all. The features and technologies were developed by different companies with differing objectives, using different development teams, for different threats. The various packages have a myriad of dissimilar interfaces and administration styles.

*This document is
provided strictly as guide.
No guarantees can be
provided or expected.*



WhitePaper:

Security "Point" Solutions are Not a 4 Letter Word:

As any vendor who's attempted it will testify, it's incredibly difficult to take multiple point security products and piece them together into a cohesive whole without losing a substantial portion of the features and benefits.

In those rare cases where a supplier will actually spend the resources to properly integrate security features such as patch management, it usually takes a number of years to pull it off. Unfortunately, by then new solutions are needed to meet the new and ever changing security threats and the process must be repeated. It's a vicious cycle to maintain and get right. More often than not a number of diverse security products are merely *bundled* together as a "package." This kind of consolidation hurts more than it helps.

Need patch management depth & application coverage

Another critical issue for patch management is depth and completeness of application coverage. Microsoft's WSUS and any vendor's offering that relies on the Windows Update APIs only addresses Microsoft systems and applications. Unfortunately Mozilla Firefox, QuickTime, Adobe, Realplayer, to name just a few non-Microsoft applications are realities in most networks today. While custom scripts can be created to help manage these non-Microsoft applications, it's a very complicated task to do without the right tools. To manage non-Microsoft systems in a cost effective manner requires a separate point solution like Shavlik NetChk Protect.

Likewise, Microsoft WSUS and technologies that deploy agents can't easily manage systems that are offline. This is a particular challenge for large enterprises where at any given moment there are potentially thousands of devices that are not connected to the network. Extraordinary steps must be taken to patch previously offline machines as they go-online. Again, it takes a best of breed point product like Shavlik NetChk Protect to effectively administer the patch management of offline systems.

Simple, sustainable patch and configuration management are keys to success

Another important consideration regarding a sustainable patch and configuration management solution is the time to implement and manage large systems. A large scale Tivoli, Openview, or other large network management system can easily take 9 to 18 months to implement, and several full time administrators to keep it going. Good point products like Shavlik NetChk Protect and Shavlik NetChk Compliance

*This document is
provided strictly as guide.
No guarantees can be
provided or expected.*



WhitePaper:

Security "Point" Solutions are Not a 4 Letter Word:

on the other hand can be deployed and maintained in a fraction of that time, produces benefits immediately, and requires minimal staffing.

Simplicity and ease of use means that you should be able to manage your environment in ways that support your business goals. Unless your patch management and configuration management solutions are comprehensive yet simple enough to manage and sustain in a cost effective manner, they are not serving your needs.

Here are some important administration issues to consider when evaluating patch management and configuration management solutions:

- ◆ *Simple, quick installation and configuration. With a reasonable knowledge of your network and its assets, you should be able to complete the installation and configuration of a patch management or configuration management solution without having to hire professional services from the vendor to be successful. If you cannot download, install, and perform the simplest assessment – scanning a local machine – in 30 minutes, a red warning flag should be raised.*
- ◆ *Policy establishment and compliance reporting. You must be able to easily establish your patch management policies or configuration baseline and assess how well you meet those policies. A continuous, sustainable, ongoing process is the only way to prevent erosion of your security status.*
- ◆ *Automated discovery and assessment. The administration interface should discover new systems on your network and quickly determine if the latest security bulletins or vendor patches are needed and applicable for your organization. The solution should also provide you with an easy but effective way to judge the priority of vulnerabilities and devices that are out of compliance.*
- ◆ *Quickly determine risk level. The system should be able to quickly ascertain risks and level of security or conformity with corporate policies for patch deployment and configuration baselines.*
- ◆ *Accuracy and trust. The right solution needs to provide an accurate assessment without displaying false positives or false negatives. It should also perform a deep assessment of patches to ensure accurate results, and it should be able to identify patches that have been reverted as well as understanding supersedence so it only displays what is needed. A solution that can be fooled by incomplete patch installations or faulty registry key settings cannot be trusted.*

This document is provided strictly as guide. No guarantees can be provided or expected.



WhitePaper:

Security "Point" Solutions are Not a 4 Letter Word:

- ◆ *In depth reports. The user interface and reports should provide real-time indications of the latest patch status. You should be able to quickly get a list of top offending machines or machines with unauthorized configurations, applications, or out of date patches or software.*
- ◆ *Automated remediation. Sustainable patch management and configuration management must automate routine, mundane tasks such as remediation and give you visibility into how well those tasks have been accomplished.*
- ◆ *Security Focused. Is the solution secure by default? Is all necessary traffic encrypted? Can the solution be subverted by malicious users? The right solution needs to ensure that all sensitive data is encrypted while in transmission. It also needs to employ multiple security checks to ensure the process cannot be tampered with.*

Defense in depth

Another leading reason for deploying purpose-built point solutions is to provide *defense in depth*. Deploying multiple, varying security countermeasures has become standard practice for most high profile organizations that are subject to specific targeted attacks. Not only can 3rd party point security products provide backup defenses for other systems, they can be used to audit or validate that systems are correctly configured and that the security is actually working.

Quick response time to new security threats is crucial

Operating systems and many applications that are so large and have such long development and release cycles that they can't possibly respond to the ever changing security landscape. Since IT security threats are constantly emerging, often rapidly, it's not feasible for large systems such as operating systems to respond to every new and emerging threat. Independent patch management and security configuration products that can emerge and adapt quickly must fill that role.

Innovation is driven by small, point solution providers

While mature and unchanging patch and configuration management features and technologies will continue to be acquired and imbedded within larger systems, new point security solutions will keep emerging to address the ongoing and ever changing security threats. Most of the innovation in the IT security industry comes from smaller companies such as Shavlik Technologies that are focused exclusively on patch and vulnerability management solutions.

This document is provided strictly as guide. No guarantees can be provided or expected.



WhitePaper:

Security "Point" Solutions are Not a 4 Letter Word:

Security developers who were acquired by larger IT companies indicate that the larger IT focused organizations see security as merely a checklist item that they can provide for their customers. In that environment innovation becomes an expense rather than an asset and therefore takes a back seat to other activities. This however is opposite for smaller companies who thrive only on innovation. They tend to lead with innovative ideas and products, continuously bringing new point patch management solutions to the marketplace.

Filling the gaps left by network management systems

Point products like Shavlik NetChk Protect and Shavlik NetChk Compliance fill the gaps left by other network management systems. Point patch management products may not always replace other solutions like Tivoli, SMS, or WSUS, but they are great companion products, complementing and providing important security benefits otherwise not available.

While products like Tivoli or Openview do a lot to manage the patching of critical systems, because they are not focused on security they can't go as deep as pure point security products. For example, network management or operating system products rarely if ever cover patch management needs for 100% of an organization's applications. There is almost always a percentage, typically between 5 to 20 percent, of applications that don't get managed. Point products address these areas.

*This document is
provided strictly as guide.
No guarantees can be
provided or expected.*

Don't get locked into an inflexible, vendor specific approach

Relying solely on a single, comprehensive PC lifecycle management solution locks you into an inflexible, vendor specific approach. Effective security solutions require a lot of flexibility.

There are times when an agent-less solution is best, just as there are situations where an agent-based solution is the right solution. For maximum flexibility, a combination of agent and agent-less architecture allows you to protect servers, desktops, and laptops whether they are connected to a LAN, connected over VPN, or are on the Internet.

You should also have the flexibility of scanning from either a distributed or from a centralized source. Large enterprises will frequently need to use both approaches in order to meet their security and management needs.



WhitePaper:

Security "Point" Solutions are Not a 4 Letter Word:

Summary

While the consolidation trend will continue as redundant security vendors combine and the more mature technologies get embedded within the general IT infrastructure, it doesn't mean that a bigger, more expensive solution is a better solution. With all of the consolidation and investment in more expensive and larger systems, the end customers are not necessarily seeing any added value as far as patch management is concerned. Unless consolidation results in a more secure product, and one that is easier to administer and sustain over the long haul, the consolidation is of no benefit to end organizations.

Customers seeking quality and complete solutions for their patch management and configuration management needs will continue to augment their network management systems and operating system tools with 3rd party, best of breed point products. In spite of how nice it would be for the operating system or other large applications to handle all security efficiently and transparently, it cannot be. Third party point security products will always be necessary, and to a significant extent.

Not all point security products are four letter words. In your time of need they just might become your best friend. If you required specialized medical care, you wouldn't want to rely on a generalist. You would want a certified point specialist who does nothing but focus on solving the particular threats to your health. The same holds true when it comes to patch management and security configuration management and protecting the health of your organization's infrastructure. A point solution will be your best option.

*This document is
provided strictly as guide.
No guarantees can be
provided or expected.*