



TotemGuard

Principales diferencias entre Shavlik NetChk Protect y WSUS



¿Sólo puede desplegar parches Windows? ¿Y las demás aplicaciones?

Este documento detalla las principales diferencias entre Shavlik y WSUS en los siguientes aspectos:

- > [Velocidad y precisión de la información](#)
- > [Soporte para aplicaciones](#)

- > [Selección de máquinas de destino](#)
- > [Despliegue de parches y opciones de reinicio](#)
- > [Informes](#)
- > [Auditoría](#)

Velocidad y precisión de la información

Shavlik es una de las pocas empresas que no depende del fichero mssecure.cab de Microsoft para determinar la relevancia de un parche, sino que ha desarrollado su propia lógica. Esta lógica de detección de parches propietaria no tiene rival en el mercado, y es utilizada por más fabricantes que cualquier otra alternativa, incluyendo Symantec, Marimba, Bindview and Bladelogic.

Shavlik determina la aplicabilidad de un parche para una máquina determinada en base a un detallado examen de sus ficheros y dlls. En muchas ocasiones Microsoft ha marcado un parche como requerido o no requerido para una situación concreta, mientras que Shavlik ha indicado lo concreto: en cada una de estas ocasiones, y tras una investigación exhaustiva, la indicación de Shavlik ha resultado ser la correcta. Sirva como ejemplo el caso del parche MS05-001, aplicable a sistemas NT4 con IE6: Microsoft introdujo el parche 05-001 para NT4 y lo asoció al producto "NT4 SP6a".

Esto causó falsos positivos, dado que todas la máquinas NT4 SP6a eran evaluadas independientemente de su nivel de service pack de IE. Shavlik actualizó su motor hfnetchk para incluir un nuevo producto, que introdujo la dependencia de IE, y lo llamó "IE6 SP1 for Windows NT4". Este nuevo producto permitió que Shavlik escaneara solamente las máquinas NT4 con IE6 SP1. Shavlik asoció el parche 05-001 NT4 al producto "IE6 SP1 for Windows NT4", proporcionando resultados más precisos que los del fichero MSSecure.cab y por tanto más precisos que los del propio fabricante Microsoft.

Por otra parte, WSUS no puede escanear bajo demanda. Por defecto se escanea cada 22 horas, y se requiere un Administrador con derechos de Política de Grupo (y un profundo conocimiento de AD) para cambiar esta política. Si se incrementa la frecuencia de los escaneos, por supuesto, se incrementa también el tráfico de red de los agentes entre hacia el servidor WSUS.

TOTEMGUARD

902 360 645

www.totemguard.com

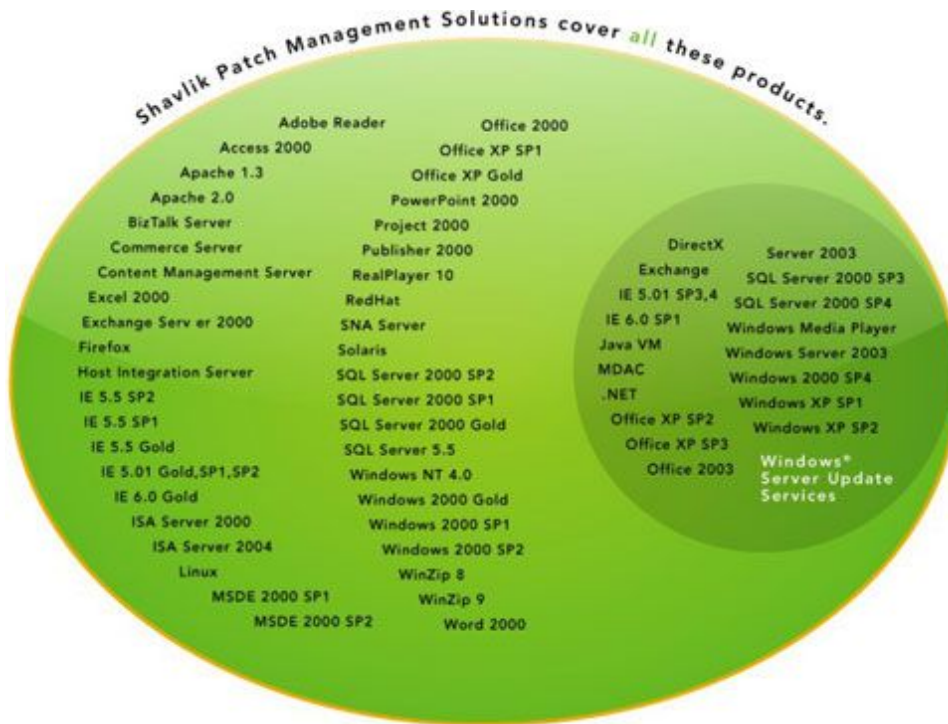
info@totemguard.com



TotemGuard

Principales diferencias entre Shavlik NetChk Protect y WSUS

Soporte para aplicaciones



WSUS no soporta aplicaciones "no-Microsoft" como Adobe, Firefox, Real Player o Winzip, mientras que Shavlik sí lo hace. Además, no soporta algunos productos Microsoft antiguos como NT4 y Office 2000. El problema es claro, al no poder proteger una parte de su red de las vulnerabilidades conocidas, ese tanto

por ciento de su infraestructura debe ser considerada como vulnerable. Con WSUS puede tener hasta el 35% de sus equipos sin los parches necesarios, por lo que tendría un 35% más de probabilidades de verse comprometido por un ataque que si estuviera utilizando Shavlik.

Selección de máquinas de destino

Shavlik permite seleccionar grupos de máquinas de destino por OU, IP, nombre de máquina name o una combinación de criterios. Los grupos que defina pueden recibir todos o un subconjunto de parches que usted elija, incluyendo aplicaciones específicas de servidor

o de escritorio, o incluso números de MS0 específicos. Con Shavlik USTED es quien define la importancia de los parches y cómo deben desplegarse. WSUS sólo permite aceptar o rechazar parches, sin ningún otro tipo de refinamiento.

TOTEMGUARD

902 360 645

www.totemguard.com

info@totemguard.com



TotemGuard

Principales diferencias entre Shavlik NetChk Protect y WSUS

Despliegue de parches

Lo más importante en este aspecto es que Microsoft no evalúa el posible impacto de los parches antes de liberarlos. Por el contrario, Shavlik comprueba los parches en 150-200 configuraciones distintas antes de liberarlo, e informa de los posibles problemas cuando un parche se muestra como requerido, para que esté informado de cualquier posible impacto antes de proceder al despliegue. Aun así, Shavlik libera los parches el mismo día que lo hace Microsoft, y no ha incumplido en ninguna ocasión este compromiso autoimpuesto.

En términos de despliegue, como ya se ha comentado puede elegir entre desplegar automáticamente o manualmente. Estos parches pueden distribuirse a todas las consolas y posteriormente distribuidos a los clientes a través del punto más cercano. Las soluciones Microsoft requieren acceso a su centro web de descargas, aunque los parches pueden ser aprobados localmente.

WSUS no tiene ningún mecanismo de roll-back, por lo que si necesita desinstalar algún parche que ha desplegado deberá hacerlo manualmente, máquina por máquina. Por ejemplo uno de los parches más recientes, 06-042 resultó contener un bug que afectaba directamente a IE. Los administradores que lo desplegaron mediante WSUS tuvieron un día muy largo.

Cuando los parches requieren un reinicio, WSUS ofrece muy poco control, mientras que Shavlik ofrece la gama de opciones más amplia del mercado. Los reinicios pueden ser programados para que ocurran en una fecha y hora determinadas para coincidir con paradas programadas de mantenimiento, con o sin interacción del usuario y tomar en consideración si existe o no un usuario con sesión iniciada. Estas características permiten que el despliegue de parches sea a la vez eficiente y transparente para al usuario.

Informes

WSUS sólo genera informes simples en formato html, y no puede exportarlos a ningún otro formato. Shavlik ofrece 23 informes personalizables y exportables a 8 formatos. Los informes pueden ser organizados gráficamente y mostrar específicamente la información

que necesite alguien en concreto. Los resultados de escaneo y despliegue pueden ser enviados manualmente o automáticamente a los usuarios que defina el administrador de Shavlik. Los informes pueden ser generados a nivel de consola global o local.

Auditoría

No sólo es importante detectar qué parches se requieren y desplegarlos de forma eficiente, sino también disponer de un registro completo de qué parches han sido desplegados, cuándo y quién los ha desplegado. Esto es vital para cualquier organización que quiera cumplir

con estándares de calidad internos o externos, y es una funcionalidad inherente a Shavlik pero no disponible en WSUS.

TOTEMGUARD

902 360 645

www.totemguard.com

info@totemguard.com