Ivanti Security Controls

Mientras que los departamentos de TI dedican demasiado tiempo gestionando la seguridad por el aumento de dispositivos y los departamentos de seguridad sufren una falta de trabajadores, Ivanti simplifica la seguridad con una solución unificada que se enfoca en los principales vectores de ataque. En Ivanti Security Controls (anteriormente Ivanti Patch for Windows) hemos combinado las herramientas de seguridad que según los expertos crean las mayores barreras contra los ataques cibernéticos (descubrimiento de software autorizado y no autorizado en su entorno para que pueda protegerse y defenderse; gestión de parches para su entorno heterogéneo de SO y aplicaciones de terceros; listas blancas dinámicas y privilegios granulares) y herramientas de parches tradicionales que ayudan a los departamentos de TI y seguridad a trabajar juntos para proteger mejor la empresa.

Parches para Windows y Linux

Ivanti Security Controls es una única solución de parches automatizada que abarca estaciones de trabajo y servidores Windows físicos y virtuales. Y hemos añadido soporte de parches para Red Hat Enterprise Linux a la solución de parches Windows líder en el mercado.

Parchee sus servidores virtuales.

Encuentre estaciones de trabajo y servidores en línea y desconectados, busque parches que no se hayan instalado y despliéguelos. Entonces parchéelo todo desde el SO y las aplicaciones a las máquinas virtuales (VM) e incluso el hipervisor ESXi con una gran integración de productos con VMware.

Es posible mantener imágenes virtuales offline en un estado constante de buena disposición para su despliegue. (No le interesa tener que realizar el proceso de dos pasos de crear una máquina virtual y tener que parchearla. Si las plantillas offline se mantienen actualizadas, usted puede desplegar la máquina sin tener que preocuparse de si está actualizada).

Parchee sin agentes.

La tecnología sin agentes le permite evaluar y desplegar parches a estaciones de trabajo y servidores conectados a su red a la vez que minimiza el impacto en su equipo y las cargas del sistema. Alternativamente, puede usar el agente para crear las políticas de agente necesarias para gestionar su red, que le ofrecen una gran flexibilidad de parcheo, y para proporcionar un alto nivel de precisión en el parcheo en entornos donde los dispositivos no están conectados a la red continuamente. Asigne diferentes configuraciones a diferentes dispositivos en su organización.

Parchee sus equipos Windows y Linux.

Necesita un software de gestión de parches en su caja de herramientas que pueda gestionar los entornos heterogéneos de hoy en día. Extender los parches más allá de Windows es esencial. Y hacerlo de una forma eficiente, mediante una única interfaz y una herramienta automatizada, no solo libera la carga del departamento de TI, sino que reduce el error humano y mejora sus defensas.

Patch your applications.

Las aplicaciones de terceros como Adobe Acrobat Flash y Reader, Google Chrome, Mozilla Firefox y Oracle Java son aplicaciones y complementos del navegador que los hackers suelen atacar.

Proporcionamos el catálogo de parches más grande del sector y nuestro equipo de contenido pone a prueba todos estos parches para que usted no tenga que hacerlo. Podemos ahorrarle tiempo, a usted y a su equipo, para que pueda centrarse en objetivos empresariales fundamentales.

Las listas blancas y la gestión de privilegios bien hechos

Ivanti Security Controls ofrece una opción de listas blancas más dinámica que usa modelos de confianza en vez de listas. Esto reduce el tiempo de preparación, el coste de propiedad una vez en funcionamiento y el impacto en el rendimiento, a la vez que proporciona un gran nivel de seguridad. También permite al departamento de TI recuperar derechos de administrador y permitir a los usuarios hacer lo que tienen que hacer, facilitando también el proceso de añadir los permisos adicionales necesarios.

Simplifique las listas blancas.

Podemos proporcionarle acceso autorizado a aplicaciones, servicios y componentes sin obligar al departamento de TI a gestionar listas extensivas manualmente y sin limitar a los usuarios. Trusted Ownership™, por ejemplo, permite la propiedad NTFS de un archivo para simplificar el proceso de lista blanca. Usar varias cuentas fiables para definir la propiedad de archivos de confianza permite una implementación sencilla de la lista blanca y una continua actualización de las aplicaciones mediante sistemas de gestión, ya que los propietarios de confianza son las cuentas realizando la instalación y las aplicaciones.

Controle las llaves del reino.

Existen muchas vulnerabilidades que, si se aprovechan, proporcionan al atacante los mismos permisos que el usuario actual. Los atacantes pueden usar credenciales robadas y los derechos de administrador de dicho usuario para obtener acceso completo a la información y los sistemas y para extenderse más por su red. Además, proporcionar derechos de administrador en un servidor tiene otros riesgos, como la capacidad de iniciar o detener servicios e instalar o eliminar software por error.

Todavía hay empresas que pueden aplicar una política de bloqueo total de los permisos de los usuarios, pero generalmente los usuarios necesitan inevitablemente ciertos derechos administrativos en su sistema. Microsoft proporciona solo dos niveles de control: usuario o administrador completo. Existen algunas variaciones, pero no son suficientes para que sea una buena experiencia para el usuario o administrador.

Nosotros implementamos los perfiles JEA (Just Enough Administration) y JIT (Just-in-Time Administration), que le permiten recuperar derechos de administrador y a la vez permitir que los usuarios hagan lo que necesitan hacer. También facilitan el proceso de escalar o añadir permisos adicionales en caso necesario. Ahora puede elegir. Reduzca los administradores a simples usuarios y proporcione escalada de privilegios en los momentos en los que sea necesario, como acceso para instalar aplicaciones, instalar una impresora, usar PowerShell o lo que el usuario necesite, pero no más de lo que el usuario deba tener. O puede empezar desde un administrador completo y retirar todas las cosas a las que no deban tener acceso. Quite PowerShell por ejemplo, o el acceso a ciertas características. Limite el privilegio administrativo a consolas, aplicaciones, servicios y comandos específicos, reduciendo así el riesgo de que los administradores introduzcan malware, detengan servicios esenciales o reduzcan el rendimiento de servicios críticos.

Más herramientas para ahorrarle tiempo y dinero

Ivanti Security Controls también incluye las siguientes características que facilitan aún más las actividades de seguridad de su organización a los departamentos de seguridad y operaciones de TI.

Integre y automatice más allá de Ivanti.

La API del parche REST permite que Security Controls se integre con otros productos, automatice procesos compartidos y proporcione acceso y control remotos desde la consola.

Reduzca los huecos entre los departamentos de seguridad y operaciones de TI con vulnerabilidades comunes y creación de listas de parches.

Ivanti Security Controls puede realizar una evaluación de vulnerabilidad de cualquier fabricante que la organización utilice, encontrar todos los parches relacionados con las vulnerabilidades comunes (CVE) y crear un grupo de actualizaciones que se apruebe rápidamente como remedio en el entorno. Ahorra una cantidad enorme de tiempo en comparación con los procesos manuales actuales.

ivanti

ivanti.es
+34 (0)609 64 40 04
contact@ivanti.es