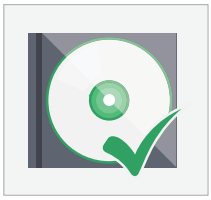
Aumente la seguridad con NetSupport DNA

NetSupport DNA es un conjunto de aplicaciones para la gestión de activos de TI. Con una diferencia: aparte de las funciones estándar de inventario, licencias de software y distribución de software que caben esperar, y además de sus innovadoras funciones de impresión y supervisión del consumo energético, NetSupport DNA incluye también una serie de herramientas diseñadas para funcionar en conjunción con la planificación general de escritorios y seguridad de redes de una organización.

¿Cómo ayuda NetSupport DNA a aumentar la seguridad de sus escritorios? Estas son ocho maneras:

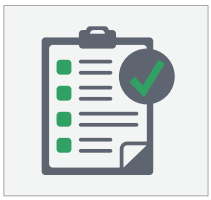
Seguridad de terminales

NetSupport DNA incorpora una función flexible de seguridad de terminales que permite controlar el uso de llaves de memoria, restringiendo el acceso de cada llave a un usuario o departamento específico. También se puede realizar el seguimiento y la elaboración de informes de cualquier llave de memoria, y la seguridad de terminales de DNA puede ayudar a evitar tanto la pérdida de datos como la infección con virus presentes en dispositivos multimedia portátiles.



Control de USB/DVD

NetSupport DNA ofrece también control del acceso a dispositivos de almacenamiento USB y unidades de CD/DVD por parte del usuario, bien evitando completamente su uso, limitando su acceso a solo lectura, o permitiendo su uso pero evitando que se ejecuten archivos desde ellos. Esta función permite a una empresa controlar y (en conjunción con los módulos de Internet y apps) evitar que se instalen o ejecuten nuevos programas en cualquier PC.



Listas blancas de aplicaciones

NetSupport DNA también permite supervisar e informar del uso de todas las aplicaciones y, al mismo tiempo, crear listas blancas de aplicaciones autorizadas por la organización que pueden asignarse a usuarios o departamentos específicos. El uso de las aplicaciones puede limitarse a solo las autorizadas por la empresa; y puede evitarse el uso de aplicaciones desconocidas que puedan causar problemas de seguridad posteriores.

Seguridad de Internet

Al igual que sucede con el control de aplicaciones, NetSupport DNA incluye el uso de listas de URL autorizadas y restringidas, además de la supervisión y el registro de toda la actividad en Internet. El acceso en los equipos de una empresa puede limitarse únicamente a sitios web autorizados específicos, para así evitar el acceso a sitios no seguros que puedan suponer un riesgo de transmisión de malware o virus.

Exploración proactiva y alertas

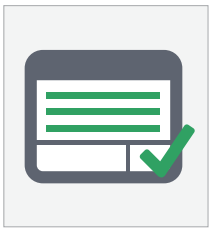
NetSupport DNA features a powerful alerting suite with many alerts designed to help maintain security. Alerts can be triggered instantly: for example, if a key service such as anti-virus is stopped, or a new application is installed, or the size of a known file changes – and much more. Alerts are designed to operate in combination to highlight potential security risks and prevent systems from becoming compromised.

Detección automática

Al igual que sucede con el control de aplicaciones, NetSupport DNA incluye el uso de listas de URL autorizadas y restringidas, además de la supervisión y el registro de toda la actividad en Internet. El acceso en los equipos de una empresa puede limitarse únicamente a sitios web autorizados específicos, para así evitar el acceso a sitios no seguros que puedan suponer un riesgo de transmisión de malware o virus.

Supervisión de SNMP

El módulo SNMP de NetSupport DNA permite detectar y supervisar los datos clave de dispositivos de red como conmutadores de redes y cortafuegos. Las alertas pueden activarse en decenas de situaciones distintas, por ejemplo si el tráfico entrante en el cortafuegos de la empresa excede un cierto porcentaje durante un período de tiempo predefinido, lo que podría indicar un ataque por denegación de servicio.



Políticas de uso aceptable

El módulo SNMP de NetSupport DNA permite detectar y supervisar los datos clave de dispositivos de red como conmutadores de redes y cortafuegos. Las alertas pueden activarse en decenas de situaciones distintas, por ejemplo si el tráfico entrante en el cortafuegos de la empresa excede un cierto porcentaje durante un período de tiempo predefinido, lo que podría indicar un ataque por denegación de servicio.

Para ampliar información, visite www.netsupportdna.com