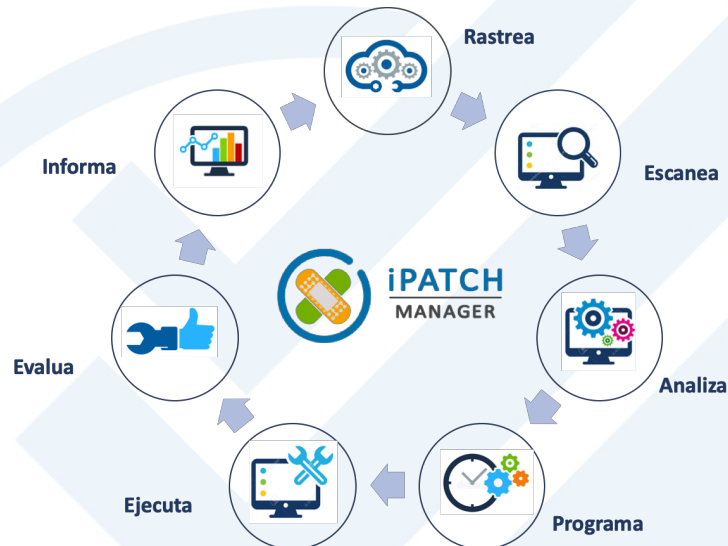


¿ QUÉ ES Y PARA QUE SIRVE LA GESTION DE PARCHES O PATCH MANAGMENT?









La gestión de parches es el proceso de detectar, descargar, probar, aprobar e instalar parches nuevos o faltantes para todos los sistemas operativos y aplicaciones dentro de una red.



La gestión de parches implica tener una vista centralizada de los parches aplicables para los endpoints en una red, a fin de poder clasificar los sistemas vulnerables, altamente vulnerables y saludables de un vistazo. Esto ayuda a detectar los sistemas que necesitan atención para que se puedan tomar las medidas adecuadas para proteger la red ante ataques cibernéticos.

¿Cómo lo hace?

El iPatch Manager esta “escuchando” las actualizaciones liberadas por los fabricantes de Sistemas Operativos, Softwares, Aplicaciones y Hardware, las descarga, las prueba, las aprueba y según reglas predefinidas y configurables las instala. Es como tener un equipo de ingenieros dedicados a realizar estas tareas 24 x 7.

	ACCION	DESCRIPCION
	RASTREA	Sistemas Operativos Windows, Linux, MacOS Soporte para más de 300 aplicaciones de terceros
	ESCANEA	Realice un inventario de todos los dispositivos en la red Detecte las falta de actualizacion de sus Equipos , Sistemas Operativos y Aplicaciones Monitoreo basado en agentes del estado del sistema de los equipos Mantenga actualizados a los usuarios que viajan
	ANALIZA	Revise y apruebe o rechace parches Deshabilite la actualización automática de parches
	PROGRAMA	Pruebe y apruebe los parches antes de la implementación Cree sus propias reglas de actualización Calendarice las actualizaciones
	EJECUTA	Realice las actualizaciones de forma automática
	EVALUA	Revise el resultado de los parches implementados
	INFORMA	Informes personalizados para las auditorías de TI Mensajes emergentes de vulnerabilidad para parches críticos

¿Por qué es tan importante la gestión de parches?

La delincuencia cibernética ha crecido exponencialmente en la última década, además los hackers informáticos cada vez son más creativos y encuentran nuevas formas de explotar las vulnerabilidades. Uno de los puntos de entrada más comunes para estos ataques son los sistemas sin parches. Cada vez que se lanza un parche de seguridad, los atacantes encuentran una nueva vulnerabilidad que se puede explotar (en los sistemas sin parches) y comienzan a explorar las redes para detectar la debilidad.

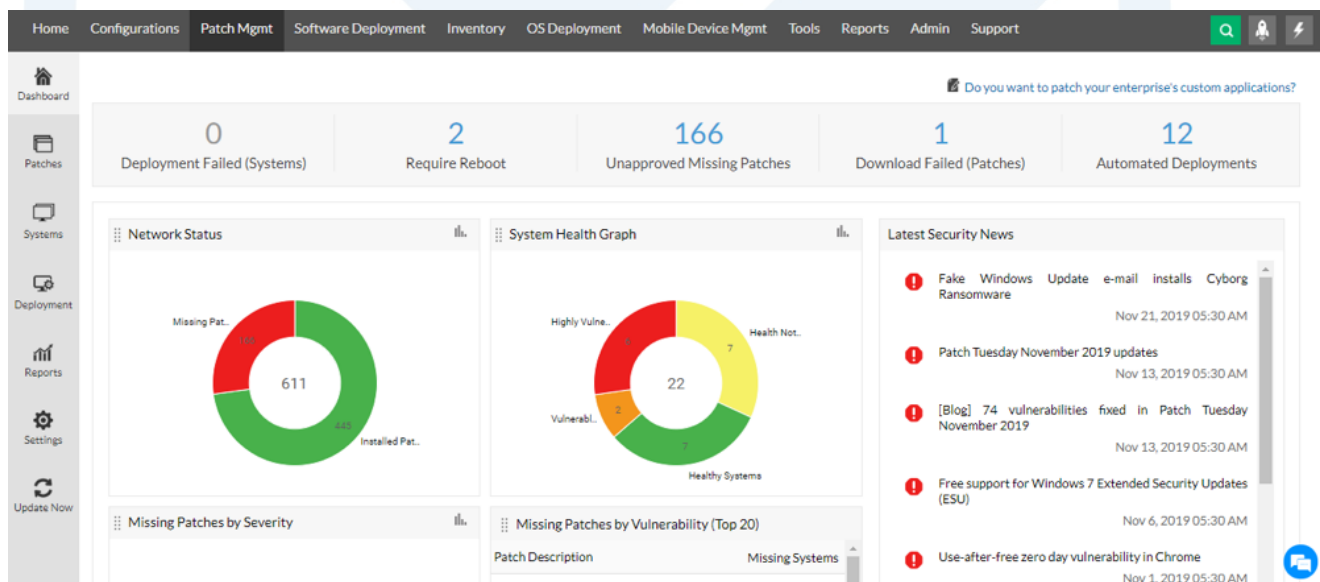
Dado que solo el 38% de las organizaciones están preparadas ante un ataque cibernético, es fácil encontrar y explotar las redes vulnerables. Esta es la razón por la que se requiere un software de gestión de parches efectivo, para proteger las redes ante ataques cibernéticos y evitar las violaciones de datos.

Si no se aplican parches a los Endpoints en una red:

- Se perderá de nuevas funciones y recursos
- Se reducirá el rendimiento
- Los sistemas serán vulnerables a los ataques

Gestión de parches con iPatch Manager

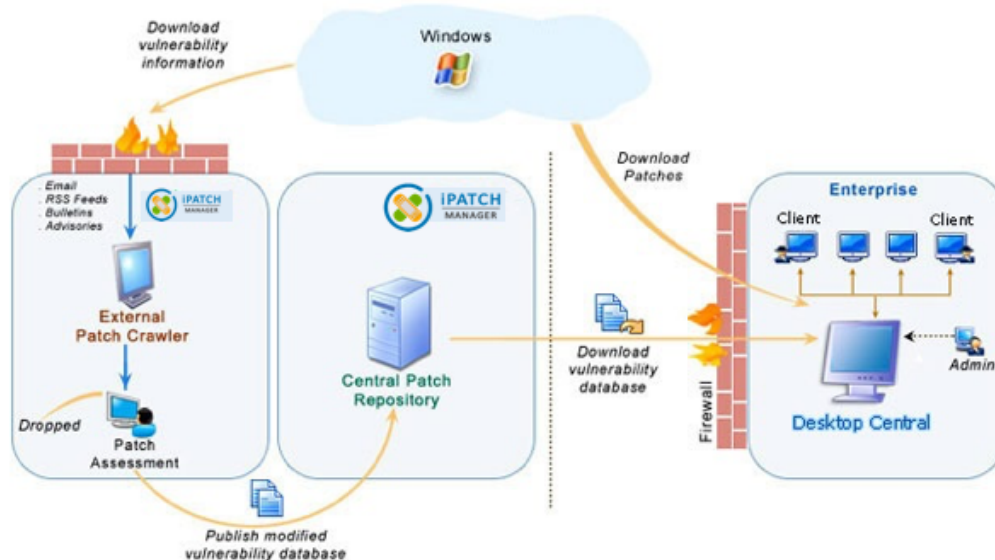
Para estar informado respecto a la gran cantidad de parches que se lanzan todos los días, necesita un software de gestión de parches efectivo. Desktop Central ofrece una solución de gestión de parches totalmente automatizada para las aplicaciones de Windows, Mac, Linux y aplicaciones de terceros (vea la lista completa de las aplicaciones compatibles aquí). Las siguientes funciones y características le brindan un control granular sobre todo el proceso de gestión de parches y le permiten proteger y actualizar sus endpoints:



Funciones clave de gestión de parches

- Actualizar la base de datos de vulnerabilidades
- Actualizar la base de datos de vulnerabilidades
- Establecer una política de salud del sistema
- Actualizar el antivirus automáticamente
- Rechazar parches para aplicaciones específicas
- Deshabilitar las actualizaciones automáticas
- Probar y aprobar automáticamente los parches para su implementación
- Programar la implementación de parches
- Implementar los parches automáticamente
- Gestionar parches usando la aplicación móvil

Actualizar la base de datos de vulnerabilidades



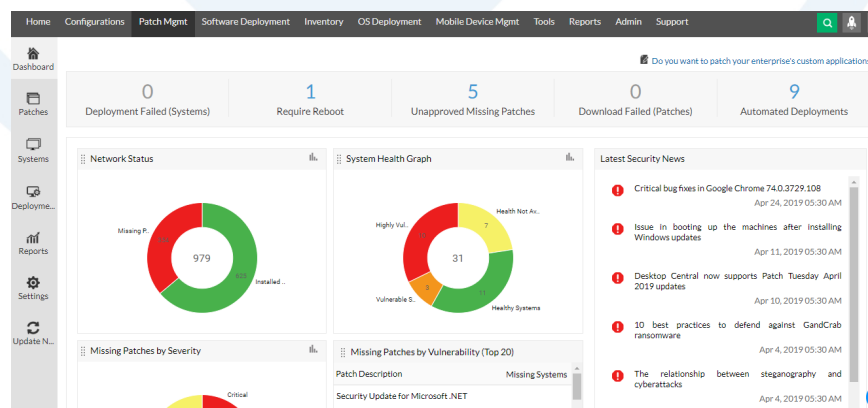
iPatch Manager busca continuamente en Internet los parches y vulnerabilidades recientemente lanzados. Una vez que se descubre un nuevo parche, se agrega al repositorio central de parches de **iPatch Manager** después de realizar un extenso proceso de verificación y prueba. Se puede acceder a este repositorio mediante el servidor de Desktop Central instalado dentro del entorno de un cliente y además se utiliza para evaluar las vulnerabilidades dentro de la red. En el sitio del cliente, el servidor de Desktop Central mantiene una base de datos de vulnerabilidades que se sincroniza periódicamente con el repositorio central de parches. Esta sincronización se realiza de dos maneras:

- **Sincronización diaria:** El servidor sincroniza la base de datos de vulnerabilidades con el repositorio central de parches todos los días. Puede establecer la hora en la que se realizará la sincronización.
- **Sincronización bajo demanda:** La base de datos de vulnerabilidades se puede actualizar en cualquier momento al iniciar una sincronización bajo demanda.

Analizar los parches de forma periódica

Cada vez que se actualiza la base de datos de vulnerabilidades se inicia automáticamente un análisis de parches. Se analizarán todos los sistemas de la red para buscar los parches faltantes en los próximos 90 minutos y esta información se publicará en el servidor de Desktop Central.

Establecer una política de salud del sistema



iPatch Manger le permite clasificar el estado de salud de los sistemas dentro de su red a través de la política de salud del sistema. Puede especificar la cantidad de parches faltantes necesarios para que los sistemas se clasifiquen como saludables, vulnerables y altamente vulnerables. A partir de esta clasificación, podrá filtrar los sistemas que necesitan atención inmediata y tomar medidas efectivas

Actualizar el antivirus automáticamente

iPatch Manger también ayuda a automatizar las actualizaciones de definiciones de antivirus. Dichas actualizaciones son bastante frecuentes y pueden realizarse varias veces al día, lo que puede resultar en un alto consumo de ancho de banda. Para evitarlo, puede programar estas actualizaciones para que se realicen una vez al día y a una hora conveniente.

Deshabilitar las actualizaciones automáticas

Puede deshabilitar las actualizaciones automáticas con Desktop Central con solo unos pocos clics. Esto le permite tener control total sobre cualquier actualización que esté instalada dentro de su red.

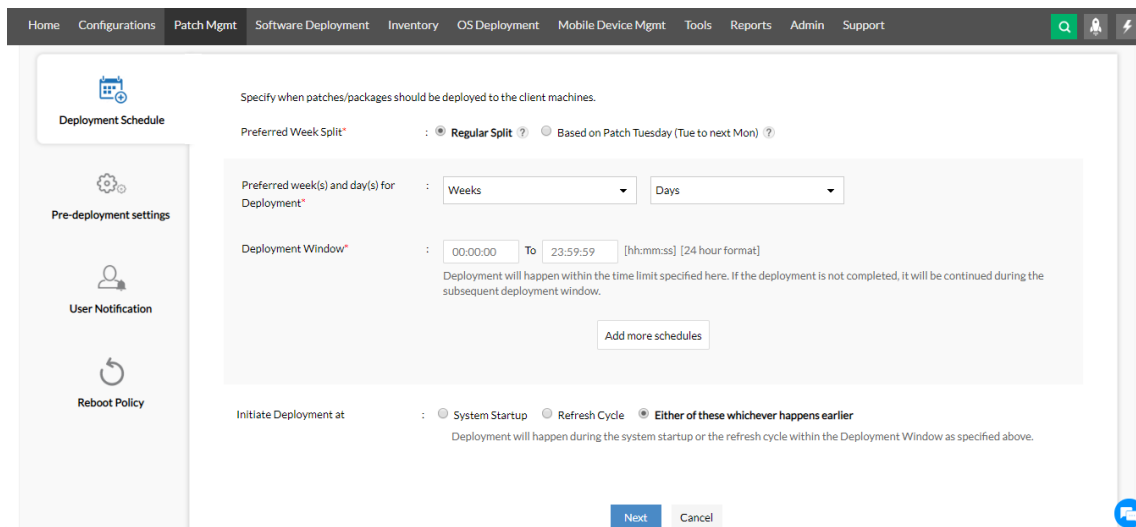
Probar y aprobar automáticamente los parches para su implementación

Siempre se recomienda probar los parches antes de instalarlos en todos los sistemas de la red para asegurarse de que no se genere un tiempo de inactividad debido a parches defectuosos. Con Desktop Central, puede formar grupos de prueba y automatizar la instalación de parches en los sistemas de prueba antes de implementarlos en toda la red. También puede especificar el número de días después de los cuales se deben aprobar los parches automáticamente para instalarlos en los demás sistemas.

Rechazar parches para aplicaciones específicas

Puede optar por rechazar parches para ciertas aplicaciones (aplicaciones heredadas) o en caso de que un parche cause inestabilidad al instalarlo en los sistemas de prueba. Desktop Central le permite rechazar los parches que no son graves, así como los parches para un grupo de equipos específico.

Programar la implementación de parches



Para evitar los problemas relacionados con el ancho de banda y garantizar la disponibilidad del sistema, los administradores del sistema pueden programar la instalación de parches en un día y hora convenientes al establecer una política de implementación. En la política de implementación, puede configurar las semanas y días en los que se realizará la implementación, el intervalo de tiempo dentro del cual se instalará el parche y la política de reinicio. También puede permitir al usuario omitir la implementación. Desktop Central permite encender los computadores por medio de la LAN antes de la implementación, si los computadores están apagados en ese momento.

Implementar los parches automáticamente

Desktop Central le permite automatizar la implementación de parches en cualquier momento y ahorrar tiempo, recursos y esfuerzo. Puede automatizarla para aplicaciones o departamentos específicos dentro de su red, en el día y la hora deseados, con una frecuencia conveniente. Solo necesita programarla una vez y todo el proceso se automatizará y recibirá notificaciones en cada fase. Visite esta página web para obtener más información.

Gestionar parches usando la aplicación móvil

Puede gestionar parches desde cualquier lugar con nuestra aplicación móvil. ¡Con tan solo unos toques podrá instalar parches, aprobar / rechazar parches, ver informes detallados de parches, iniciar el análisis de parches y mucho más! Lo mejor es que ni siquiera tiene que hacerlo usted mismo, **Zia**, la asistente de TI de **iPatch Manager**, puede hacerlo todo por usted.