

SERVICIO GESTIONADO

Nuestro servicio gestionado

Kaseya 365 Endpoint · Datto RMM y Datto EDR

Controlamos por ustedes la plataforma que monitorea, protege y mantiene al día toda su infraestructura. Configuramos cada capa según el riesgo real de su empresa, automatizamos lo que se puede resolver solo y analizamos personalmente cada alerta relevante. El resultado no es una consola prendida y nada más. Es un servicio con reportes concretos, recomendaciones, manuales para su equipo y acompañamiento todos los días.

01 Qué incluye

Monitoreo de infraestructura

Seguimos el estado de servidores, equipos y red en todo momento, para anticipar un problema antes de que se convierta en una interrupción.

Monitoreo de seguridad

Analizamos el comportamiento de cada equipo para detectar actividad sospechosa, incluso amenazas nuevas que un antivirus tradicional no identifica.

Gestión de backup

Seguimiento nativo de las principales soluciones de backup del mercado, para confirmar que cada respaldo se ejecute correctamente.

Configuración a medida

Grupos, roles y políticas de protección pensadas para su empresa, que seguimos ajustando con el tiempo.

Automatización inteligente

Resolvemos solos la mayoría de los inconvenientes menores apenas aparece la primera señal de alerta, sin que su equipo intervenga.

Parches automatizados

Windows según los criterios de su organización, y más de 300 aplicaciones de terceros siempre al día.

Reportes semanales

Informes claros sobre lo que realmente requiere atención, con el motivo y el contexto de cada dato.

Acompañamiento constante

Manuales de uso para su equipo y presencia diaria operando la plataforma, para que ustedes no tengan que hacerlo.

+150

monitores prearmados para configurar alertas a medida

~500

componentes de automatización listos para usar

+300

aplicaciones de terceros con parches automáticos

02 **Cómo trabajamos día a día**

Puesta en marcha

El despliegue se adapta a la forma en la que ya trabaja su organización, ya sea que gestionen los equipos con Active Directory o que necesiten un relevamiento completo de la red desde cero.

1

Relevamiento

Identificamos la cantidad de equipos y los sistemas operativos en uso, para confirmar la compatibilidad con la plataforma.

2

Organización

Ordenamos todo en grupos (notebooks, servidores, estaciones de trabajo, equipos especiales) y definimos roles y accesos.

3

Gestión y después seguridad

La gestión se pone en marcha primero. Con más de la mitad de los equipos incorporados, sumamos la capa de seguridad.

Monitoreo de infraestructura

Vigilamos de forma constante sus equipos y su red, con foco en anticipar un problema antes de que se convierta en una interrupción.

- **Servidores.** Uso de procesador, disco y memoria, y el historial de eventos de Windows, para anticipar caídas o fallas de servicios críticos.
- **Estaciones de trabajo.** Temperatura y salud de los discos, para detectar una falla de hardware antes de que el equipo deje de funcionar.
- **Red.** Switches, routers, impresoras y demás dispositivos conectados.

Cada equipo llega con monitores asignados por defecto, y la plataforma suma más de ciento cincuenta monitores prearmados para configurar alertas a medida de su empresa.

Backup

Hacemos seguimiento nativo de Altaro, Veeam Backup & Replication, Backup Exec, BackupAssist, CloudBerry, StorageCraft ImageManager y ShadowProtect, Windows Server Backup y Dell AppAssure / Quest Rapid Recovery. Detectamos errores en los procesos de respaldo, confirmamos que los servicios estén activos y, si alguno se detiene, intentamos reiniciarlo automáticamente antes de que se pierda información.

Monitoreo de seguridad

Además de la infraestructura, una capa dedicada exclusivamente a la seguridad, con su propio análisis y sus propios reportes.

- **Detección inteligente.** No se limita a virus conocidos. Analiza el comportamiento de cada equipo y detecta amenazas completamente nuevas. Ante un riesgo, el equipo afectado puede aislarse automáticamente de la red.
- **Análisis diario.** Todos los días, alguien de nuestro equipo revisa personalmente cada alerta relevante. No dejamos que la herramienta decida sola qué es importante, y con el tiempo hay cada vez menos ruido.
- **Recuperación ante incidentes.** Si un ransomware u otro incidente grave afecta su información, es posible revertir los archivos comprometidos a su estado previo.

Gestión y configuración a medida

Desde el primer día dejamos una base configurada (grupos, políticas de protección y umbrales de monitoreo) pensada para su empresa, y seguimos ajustando cada parámetro según el riesgo real de su operación.

03 Automatización y parches

Automatización inteligente

La mayoría de los inconvenientes menores se resuelven solos, con automatizaciones que actúan ante la primera señal de alerta. En paralelo ejecutamos tareas programadas de limpieza y mantenimiento preventivo. Contamos con cerca de quinientos componentes listos para usar y creamos componentes propios en PowerShell y Batch cuando hace falta. Por ejemplo, si el disco de una estación se llena, una política puede vaciar la papelería de reciclaje para liberar espacio de inmediato.

Parches automatizados

- **Windows.** Una política de parcheo que administramos por completo y que se activa con la aprobación de su empresa.
- **Software de terceros.** Navegadores, videollamadas, ofimática y más de 300 aplicaciones se actualizan solas con Advanced Software Management, incluido en las licencias. La instalación se puede dividir por área, por ejemplo software de diseño solo para marketing.

04 Reportes y visibilidad

Cada informe está pensado para que su empresa tenga información lista para decidir, no una lista suelta de alertas.

- **Reporte semanal de infraestructura.** Servidores con poco espacio, discos con señales de falla, equipos sin conexión hace más de una semana y equipos nuevos en la red, cada dato con su motivo y contexto.
- **Reporte semanal de seguridad.** Los equipos más expuestos, las alertas por criticidad (alta, moderada y baja) y los pasos sugeridos para cada caso.
- **Reportes a medida.** Consumo de licencias, vulnerabilidades, equipos más vulnerables y alertas más frecuentes.
- **Manuales de uso.** Material propio para su equipo sobre parcheo, monitoreo de servidores y estaciones, y políticas de seguridad.

05 Compatibilidad

PLATAFORMA	COBERTURA
Windows	Windows 10 y 11. Windows Server 2016, 2019, 2022 y 2025.
macOS	Las dos últimas versiones mayores, incluidos los equipos con Apple Silicon.
Linux	Ubuntu, Debian, Red Hat, CentOS Stream y Fedora.

Nuestro trabajo no termina con la puesta en marcha

Seguimos presentes todos los días, operando la plataforma, analizando alertas, ajustando configuraciones y entregando reportes claros, para que ustedes no tengan que hacerlo.

WhatsApp +54 9 11 6150-8969 · Lascano 4864, CABA · pncit.com.ar

Kaseya y Datto son marcas de sus respectivos titulares. PNC IT comercializa, implementa y opera estas soluciones.