

La Apuesta Estratégica por la Gestión de Endpoints en Empresas Medianas.



Introducción

En el mundo altamente digitalizado de hoy, la seguridad y eficiencia de las operaciones de TI (Tecnologías de la Información) son fundamentales para las empresas de todos los tamaños. Para medianas empresas, especialmente aquellas que forman parte de sectores regulados como la banca y la salud, garantizar una gestión de endpoints segura y sin problemas es una necesidad – no un lujo. La gestión de endpoints se refiere a la capacidad de supervisar, gestionar y proteger los innumerables dispositivos conectados a una red, desde ordenadores portátiles y de escritorio, así como servidores de las y los empleados, hasta dispositivos móviles y herramientas IoT (Internet de las Cosas).

El auge del trabajo remoto impulsado por la pandemia, combinado con la creciente sofisticación de amenazas cibernéticas, ha convertido a la gestión de endpoints en una prioridad para directores de Información (CIOs) y directores de Seguridad de la Información (CISOs). La empresa moderna ya no opera dentro de los confines de una oficina tradicional. A medida que incrementan los endpoints, también aumentan los riesgos y los retos operativos asociados a ellos. Para salvaguardar la información, mejorar la productividad y garantizar el cumplimiento de la normativa, es esencial contar con una solución sólida de visibilidad y control de endpoints.

Desafíos de la gestión de endpoints

Mientras que los beneficios de la gestión de endpoints son innegables, las empresas medianas se enfrentan a desafíos únicos que pueden entorpecer sus esfuerzos:



Brechas de visibilidad: Muchas organizaciones tienen dificultades para mantener un inventario en tiempo real de todos los endpoints conectados. TI invisible, dispositivos no autorizados y la falta de herramientas de monitoreo centralizadas generan puntos ciegos que aumentan la vulnerabilidad y el riesgo.



Complejidad creciente: Conforme las empresas adoptan modelos de trabajo híbridos y se expanden globalmente, sus ecosistemas de TI se hacen cada vez más complejos. Gestionar una mezcla de sistemas operativos, aplicaciones y dispositivos dispersos geográficamente puede abrumar a los equipos de TI.



Personal remoto: El aumento del trabajo remoto ha desplazado los endpoints más allá de las capas protectoras de firewalls corporativos. Garantizar la seguridad de los dispositivos que se conectan desde varias redes es un reto importante.



Amenazas cibernéticas: Los endpoints son objetivos prioritarios para la ciberdelincuencia. El ransomware, los ataques de phishing y las amenazas persistentes avanzadas (APT) se aprovechan de los dispositivos mal gestionados, lo que puede poner en peligro los datos confidenciales y la integridad operativa.



Cumplimiento y auditorías: Industrias como la salud y las finanzas están sujetas a estrictos requisitos normativos. Garantizar que todos los endpoints cumplen normas como HIPAA o PCI-DSS requiere visibilidad en tiempo real e informes automatizados.

Mercado de la gestión de endpoints

Para satisfacer la creciente necesidad de gestión de endpoints han surgido diversos actores:

Tanium

Conocido por su información en tiempo real y sus funciones de gestión de endpoints, Tanium es ideal para entornos complejos, pero su costo puede resultar abrumador para las medianas empresas.

Microsoft Intune

Una opción popular para las organizaciones que ya aprovechan el ecosistema de Microsoft, pero puede quedarse corta a la hora de proporcionar compatibilidad multiplataforma.

Axonius

Una herramienta excelente para la visibilidad, pero como tecnología de API/Integración, carece del conjunto completo de funciones de control de endpoints necesarias para una gestión integral.

Aunque estas soluciones ofrecen funciones atractivas, las medianas empresas necesitan una herramienta que equilibre funcionalidad, sencillez, rapidez y rentabilidad.

Beneficios de una gestión eficaz de endpoints

La implementación de una estrategia sólida de gestión de endpoints puede transformar las operaciones de TI, especialmente para las medianas empresas que operan en entornos dinámicos y de alto riesgo.

Algunos beneficios clave son:

- 1 **Seguridad reforzada:** La detección de vulnerabilidades en tiempo real garantiza que los parches y las actualizaciones se desplieguen rápidamente. Al reducir las superficies de ataque, las empresas pueden proteger mejor la información.
- 2 **Mayor eficiencia operativa:** El monitoreo centralizado y la automatización reducen la carga de trabajo de los equipos. Tareas rutinarias como el inventario de activos, actualizaciones de software y la resolución de incidentes pueden gestionarse sin problemas.
- 3 **Cumplimiento regulatorio:** Con informes robustos y comprobaciones automatizadas, las soluciones de gestión de endpoints simplifican las auditorías y reducen el riesgo de sanciones por incumplimiento.
- 4 **Ahorro de costos:** Identificar y abordar los problemas de forma proactiva evita costosos tiempos de inactividad y posibles violaciones de datos, garantizando la continuidad operativa.
- 5 **Escalabilidad:** A medida que crecen las medianas empresas, las soluciones de gestión de endpoints se escalan fácilmente, garantizando un rendimiento y una seguridad uniformes en inventarios de dispositivos en expansión.
- 6 **Mejor adopción y rendimiento de la tecnología:** Las mejoras en la forma en que la tecnología y el software de seguridad se integran en una organización, su eficacia, y la actitud general de los equipos hacia estas tecnologías pueden repercutir en la productividad y la satisfacción.
- 7 **Alineación entre los equipos de TI y Seguridad:** La alineación entre TI y Seguridad mejora significativamente la postura de seguridad, la eficiencia operativa y la gestión de riesgos de una organización. Cuando estos equipos colaboran, combinan sus conocimientos, herramientas y perspectivas para mejorar la visibilidad de la organización.

Cómo aborda la gestión de endpoints necesidades específicas del sector



Banca

Los bancos operan en un entorno muy regulado en el que las brechas de datos pueden provocar graves daños financieros y reputacionales.

La gestión de endpoints para bancos incluyen:

- Detección de activos: Identificación en tiempo real de todos los dispositivos de la red, incluidos los endpoints no autorizados.
- Identificación de vulnerabilidades: Detección proactiva y corrección de brechas de seguridad.
- Informes de conformidad: Documentación automatizada para cumplir requisitos normativos como PCI-DSS y SOX.

Salud

Los proveedores de salud deben garantizar la seguridad de los datos de los pacientes sin perder la eficiencia operativa.

Las soluciones de gestión de endpoints facilitan esta tarea ofreciendo:

- Gestión de inventarios: Seguimiento de dispositivos médicos, estaciones de trabajo y otros endpoints.
- Despliegue de software: Garantía de que las aplicaciones se actualizan para evitar vulnerabilidades.
- Cumplimiento de la HIPAA: Agilizar las auditorías con registros e informes exhaustivos.



¿Por qué escoger Batuta, la plataforma de Metabase Q, para la gestión de la postura de ciberseguridad de endpoints?

La solución Batuta ESPM de Metabase Q se ha diseñado específicamente para abordar los retos específicos a los que se enfrentan las medianas empresas. Con nuestra plataforma podrás:

- ✓ Visibilizar en tiempo real los endpoints, garantizando que ningún dispositivo quede sin gestionar.
- ✓ Automatizar la detección de vulnerabilidades y la aplicación de parches para evitar su explotación.
- ✓ Simplificar el cumplimiento con funciones integradas de auditoría y elaboración de informes.
- ✓ Integrarte con tus infraestructuras informáticas existentes, minimizando las interrupciones.

Nuestra solución ofrece el equilibrio perfecto entre funcionalidad, sencillez y asequibilidad, lo que permite a tu equipo de TI centrarse en iniciativas estratégicas en lugar de combatir los problemas de los endpoints.



Conclusión

En una era en la que las ciberamenazas y los retos operativos son más frecuentes que nunca, la gestión de endpoints se ha convertido en una piedra angular de la estrategia de TI para las medianas empresas. Al garantizar la visibilidad, el control y la seguridad, las empresas pueden proteger sus datos, agilizar las operaciones y cumplir las normativas del sector.

No permitas que los endpoints no gestionados pongan en peligro el éxito de tu empresa. Descubre cómo la solución de visibilidad y control de endpoints de Metabase Q puede transformar tu enfoque de la gestión de endpoints.