ATLASSIAN

Los 5 principales riesgos de seguridad derivados del uso de software no soportado

Moverse a la nube es una gran decisión que requiere una investigación exhaustiva, recursos y la alineación de tu equipo

Y aunque puede resultar tentador seguir utilizando productos de servidor no soportados mientras se elabora un plan, hacerlo podría poner en peligro a tu organización.

La Cybersecurity & Infrastructure Security Agency identifica el uso de software no soportado como la mala práctica de seguridad #1 que las empresas deben evitar a toda costa.

Los 5 principales riesgos de seguridad derivados del uso de productos de servidor no soportados

En el vertiginoso panorama digital actual, mantener la seguridad de los datos de tu empresa es sin duda uno de los retos más cruciales. A medida que la tecnología evoluciona rápidamente, los actores maliciosos adaptan constantemente sus tácticas para explotar las vulnerabilidades de tu software. Según un informe de Forrester publicado en 2022, esta es la principal causa de ciberataques externos. Al confiar en productos y aplicaciones de servidor no soportados, estás introduciendo riesgos innecesarios y evitables, como:

#01 - Las vulnerabilidades sin corregir exponen a tu empresa a amenazas de seguridad

A menudo ya no se proporcionan parches ni actualizaciones de seguridad para los productos de servidor, lo que expone a tu empresa a posibles riesgos de seguridad. Sin parches ni actualizaciones, las vulnerabilidades pueden quedar sin resolver, lo que facilita a los agentes malintencionados atacar y obtener acceso no autorizado a tus datos y sistemas. El uso de software no soportado no sólo aumenta el riesgo, sino que también impone una carga adicional a los equipos de TI. Es posible que tengan que reasignar su tiempo y atención a iniciativas estratégicas que podrían impulsar el crecimiento y el éxito de tu empresa para gestionar, solucionar problemas y proteger tus productos sin el soporte.

#02 - Violación de los requisitos de privacidad y cumplimiento

El uso de productos de servidor no soportados puede tener graves implicaciones para los requisitos de privacidad y cumplimiento, especialmente en sectores muy regulados como la salud y las finanzas. Estos sectores cuentan con medidas estrictas para proteger los datos confidenciales y la privacidad de los clientes. El uso de software no soportado aumenta el riesgo de vulnerabilidades, lo que a su vez aumenta la probabilidad de incumplir la normativa y puede acarrear consecuencias legales y sanciones económicas.

#03 - Tiempo de inactividad y pérdida potencial de datos

Otra consecuencia potencial es el tiempo de inactividad significativo. El software no soportado te expone a riesgos tanto de individuos bienintencionados como de actores malintencionados. Estos podrían perturbar tus sistemas de forma involuntaria o deliberada, provocando potencialmente la pérdida o manipulación de datos, e incluso haciendo que tus sistemas queden completamente fuera de servicio.

#04 - Tecnología de seguridad obsoleta

Además de perder el soporte técnico y las actualizaciones de seguridad, también se pierde el acceso a los últimos avances en tecnología de seguridad. Sin acceso a estas innovaciones, tu sistema se vuelve cada vez más vulnerable a las ciberamenazas.

#05 - Riesgos de las aplicaciones no soportadas del Marketplace

Ya no podrás comprar nuevas aplicaciones para tus licencias de servidor existentes. Y como hemos mencionado anteriormente, los socios de Marketplace ya no tendrán que proporcionar soporte técnico, actualizaciones de seguridad o correcciones de vulnerabilidades, lo que multiplica tu susceptibilidad a las amenazas de seguridad.

Qué puedes hacer para proteger tu empresa

Entendemos lo importante que es para ti mantener tu organización segura y protegida. Para proteger tu empresa, te recomendamos encarecidamente que migres a la nube de Atlassian, que incorpora la protección de datos en la base de nuestra plataforma en la nube. Al compartir la responsabilidad con los expertos de Atlassian, tu equipo ganará en tranquilidad y en tiempo para tener una visión más estratégica de las iniciativas de seguridad, incluido el aprovechamiento de las capacidades nativas de la nube de Atlassian para proteger los datos.