The 2024 PKI & Digital Trust Report

Tendencias y amenazas que impactan en la confianza digital en 2024

Atención CISOs:

¡Bienvenidos al Año de la Disrupción Digital!

Aquí están los puntos destacados del nuevo estudio global de Keyfactor que descubre lo que realmente está afectando la confianza digital: una gestión incorrecta de la infraestructura de clave pública (PKI), una proliferación de certificados digitales y los cambios inminentes en la criptografía moderna.

La PKI es la base de la confianza digital para las organizaciones, proporcionando autenticación y cifrado para todo, desde sus sitios web y aplicaciones hasta dispositivos IoT y procesos de trabajo en la nube. Pero el aumento del uso de la PKI está llevando a los equipos y herramientas al límite.

Qué pueden hacer los líderes de seguridad...

Es hora de evaluar tu infraestructura de PKI y determinar si puede soportar los casos de uso actuales y, más importante aún, si está preparada para adaptarse a cambios significativos que están por venir.

98% dicen que necesitan modernizar su PKI

La PKI es una infraestructura crítica, pero se está volviendo compleja

+5 Hrs para identificar y remediar caídas de servicio causadas por los certificados

Las caídas de servicio disminuyen los ingresos (y la confianza).

KEYFACTOR

Las organizaciones están implementando más claves, certificados e identidades de máquinas que nunca, un 91% en comparación con el 74% en 2023 y el 61% en 2021. Los equipos de seguridad deben preocuparse constantemente de si otros miembros pueden cometer errores o ignorar políticas. El informe muestra que, en promedio, los equipos tardan más de 5 horas en identificar y remediar una interrupción por certificado. Es hora de invertir en visibilidad y automatización. Afortunadamente, los encuestados indicaron que esta es una prioridad principal para el próximo año.

Qué pueden hacer los líderes de seguridad...

Las caídas de servicio causadas por certificados caducados afectan seriamente la confianza del cliente, los ingresos y la productividad de los empleados, especialmente cuando afectan a sistemas orientados al perímetro externo. Los líderes de seguridad deben comprender la gravedad y frecuencia de estas caídas y priorizar la capacidad de su equipo para prevenir y responder a estos incidentes.

95% encuentra obstáculos al prepararse para la criptografía post-cuántica

El futuro cuántico se vislumbra en el horizonte

Listos o no, la computación cuántica está llegando, y las organizaciones deben prepararse adoptando la criptografía post-cuántica (PQC). Los perpetradores de amenazas ya han comenzado a recopilar y almacenar datos encriptados con el objetivo de descifrarlos cuando esté disponible un ordenador cuántico lo suficientemente potente como para romper el cifrado moderno.

Qué pueden hacer los líderes de seguridad...

Es hora de comenzar a planificar tu hoja de ruta hacia la seguridad cuántica — lo que empieza con obtener visibilidad de tus datos y activos criptográficos.

¿Quieres aprender aún más sobre las principales tendencias y amenazas?

Descarga el "The 2024 PKI & Digital Trust Report" de Keyfactor y obtén nuevas frescas para mejorar la seguridad, fiabilidad e integridad de las interacciones digitales de tu organización.

Download now ↗