



ENTRUST



Entrust ayuda a Zerto a establecer la integridad de sus aplicaciones comerciales

Zerto

Fundada en 2010, Zerto se ha basado en una visión única de que la tecnología de recuperación de desastres no debe ser una póliza de seguro, sino una ventaja competitiva.

Zerto ayuda a los clientes a acelerar la transformación de TI al eliminar el riesgo y la complejidad de la modernización y la adopción de la nube a través de la resiliencia de TI. Al reemplazar múltiples soluciones heredadas con una única IT Resilience Platform™, Zerto combina recuperación de desastres, respaldo y movilidad en la nube en una solución simple y convergente. Con escala empresarial, la plataforma de software de Zerto ofrece disponibilidad continua para una experiencia de cliente siempre activa, al tiempo que simplifica la movilidad de la carga de trabajo para proteger, recuperar y mover aplicaciones libremente entre nubes híbridas y múltiples.

Zerto ha revolucionado los mercados de TI y ha superado los límites de la recuperación ante desastres. La compañía ha desarrollado su producto innovador sobre tecnología de protección de datos continua y, en un mundo donde la tecnología ininterrumpida no es negociable para las empresas, se ha convertido en mucho más que una simple herramienta para la recuperación de desastres.

« En comparación con otros proveedores, la implementación y el soporte de Entrust son mucho mejores. Los HSMs nShield de Entrust son más fáciles de usar y respaldar y también nos gusta la interfaz gráfica de usuario (GUI). »

- Nadav Svirsky, líder de infraestructura de TI corporativa, Zerto

DESAFÍO DEL NEGOCIO

Como proveedor líder de resiliencia de TI, Zerto necesitaba la seguridad de que sus propios sistemas comerciales no fueran vulnerables a compromisos. La estrategia más eficaz para hacerlo fue asegurarse de que se confiara en su infraestructura de clave pública (PKI).

Una infraestructura PKI es un conjunto de hardware, software, políticas, procesos y procedimientos necesarios para crear, gestionar, distribuir, usar, almacenar y revocar certificados digitales y claves públicas. Las PKIs ayudan a establecer la identidad de las personas, los dispositivos y los servicios, permitiendo el acceso controlado a sistemas y recursos, protección de datos y contabilidad de transacciones. A medida que los modelos comerciales en evolución se vuelven más dependientes de las interacciones electrónicas, que requieren de la autenticación en línea y del más estricto cumplimiento de las regulaciones de seguridad de datos, las aplicaciones comerciales de próxima generación se han vuelto más dependientes de la infraestructura de clave pública (PKI) para garantizar una alta seguridad.

Para vincular claves públicas con su usuario asociado (propietario de la clave privada), las PKIs utilizan certificados digitales. Los certificados digitales son las credenciales que facilitan la verificación de identidades entre los usuarios y una transacción. Así como un pasaporte certifica la identidad de

alguien como ciudadano de un país, el certificado digital establece la identidad de los usuarios dentro de un ecosistema. Puesto que los certificados digitales se usan para identificar a los usuarios a los que se envían datos cifrados, o para verificar la identidad de quien firma la información, es de vital importancia proteger la autenticidad y la integridad del certificado para mantener la confianza del sistema. Esto era esencial para el modelo comercial de Zerto como proveedor confiable.

DESAFÍO TÉCNICO

Las autoridades de certificación (AC) emiten las credenciales digitales que se utilizan para certificar la identidad de los usuarios. Las AC respaldan la seguridad de una PKI y los servicios que admiten y, por lo tanto, pueden ser el foco de sofisticados ataques dirigidos. A fin de mitigar el riesgo de ataques en contra de las AC, se han vuelto necesarios los controles físicos y lógicos, así como mecanismos de fortalecimiento tales como los Módulos de Seguridad de Hardware (HSMs), para garantizar la integridad de una PKI.

Zerto usa una plataforma de Microsoft y TI sabía por trabajar con Microsoft que la mejor práctica para proteger sus AC era usar un HSM. Al ofrecer un entorno certificado de forma independiente y a prueba de manipulaciones indebidas, los HSMs son una parte integral de la protección de claves y procesos comerciales confidenciales.

« La implementación de HSMs nShield de Entrust para proteger nuestras AC nos proporciona tranquilidad. Nuestra gerencia cree que la reducción de riesgos bien vale la inversión. »»

- Nadav Svirsky, líder de infraestructura de TI corporativa, Zerto

SOLUCIÓN

El equipo de TI de Zerto tenía experiencia con varios proveedores de HSMs y eligió los nShield® Solo de Entrust para su implementación. Según Nadav Svirsky, líder de infraestructura de TI corporativa, Zerto eligió a Entrust sobre otros proveedores porque “en comparación con otros proveedores, la implementación y el soporte de Entrust son mejores, los HSMs nShield Solo de Entrust son más fáciles de usar y respaldar y también nos gusta la interfaz gráfica de usuario (GUI).”

RESULTADOS

Zerto no comparte sus resultados cuantificables de la instalación de HSMs nShield de Entrust para proteger sus AC. En referencia a contar ahora con las mejores prácticas de seguridad de AC, que era el objetivo inicial del proyecto,

Svirsky señala: “Nuestros clientes deben estar seguros de que nuestros sistemas son seguros y confiables. Desafortunadamente, con frecuencia no puede ver el valor de la seguridad de los datos hasta que algo sale mal. Entonces ves la reputación, las ventas y el precio de las acciones de una empresa. Por lo tanto, la implementación de HSMs nShield Solo de Entrust para proteger nuestras AC nos brinda tranquilidad. Nuestra gerencia cree que la reducción de riesgos bien vale la inversión”.

RENDIMIENTO, CONFIABILIDAD Y PROTECCIÓN

Necesidades del negocio

- Reducir el riesgo de problemas internos de seguridad de datos

Necesidades tecnológicas

- Raíz de confianza segura para los servidores de AC a un costo razonable

Solución

- HSMs nShield Solo de Entrust

Resultado

- Reducción de riesgos
- Tranquilidad para la gestión de Zerto

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.