La empresa de servicios públicos Fortune 500 establece una infraestructura de clave pública de alta disponibilidad en un entorno distribuido geográficamente

La manera como la experiencia de Entrust y los Módulos de Seguridad de Hardware (HSMs) de alta garantía ayudaron a una de las empresas de servicios públicos más grandes del país a brindar una seguridad sólida y al mismo tiempo habilitar nuevos servicios al cliente.

EL OBJETIVO: PREPARARSE PARA EL FUTURO

El equipo de TI de una de las empresas de servicios públicos más grandes del país estableció un objetivo ambicioso para sí misma y para su infraestructura de seguridad.

A medida que la tecnología en el sector energético evolucionaba, la empresa seguía decidida a permanecer a la vanguardia. Necesitaban asegurarse de poder brindarles a sus clientes un servicio continuo y al mismo tiempo preparar su infraestructura para tecnologías nuevas y exigentes, tales como la medición inteligente y la red inteligente. Querían cumplir y superar los altos requisitos en materia de seguridad que habían establecido sus auditores y Seguridad Nacional. Y querían habilitar nuevos servicios tales como permitirles a los empleados y clientes usar tabletas y teléfonos inteligentes para acceder a la red.

> **«Sabíamos que necesitábamos una solución de hardware certificada. Teníamos que asegurarnos de que todas nuestras claves privadas tuvieran la protección más sólida disponible; habíamos leído demasiadas historias sobre el robo de claves privadas que comprometían PKI completas. Nuestra prioridad más importante es brindar servicios al público y teníamos que asegurarnos de poder brindar la mayor fiabilidad posible.»**
>
> – Analista principal de seguridad de la empresa de servicios públicos Fortune 500

Empresa de servicios públicos Fortune 500

Para cumplir con estos objetivos, el equipo de seguridad de la empresa de servicios públicos planeó migrar a una versión actualizada del software de infraestructura de clave pública (PKI) y a plataformas de servidor central. Su PKI existente, que ahora tiene casi una década de antigüedad, había funcionado bien para autenticar servidores internos y computadoras portátiles. Pero necesitaría de una nueva solución si fuera a emitir certificados para estos dispositivos móviles y acomodar otras nuevas tecnologías, al tiempo que garantizan los más altos niveles de seguridad.

Una nueva PKI permitiría nuevos servicios como la firma de código y el sellado de tiempo para garantizar la integridad y la gobernanza adecuada de sus procesos internos de desarrollo de software, así como "traiga su propio dispositivo" (BYOD), donde la inscripción certificada permitiría que los dispositivos móviles y tabletas accedan a la red de forma controlada y segura.

EL RETO: ENTORNO COMPLEJO Y DISTRIBUIDO

El verdadero desafío de esta implementación estaría en trabajar con el entorno único de la empresa. Para lograr la funcionalidad de alta disponibilidad, redundancia y recuperación ante desastres que la empresa necesitaba, el equipo tendría que implementar la PKI junto con una compleja infraestructura de agrupación de servidores que residía en varios sitios. De tener éxito, la infraestructura de la empresa de servicios públicos podría satisfacer fácilmente las demandas de la próxima década. Pero se disponía de poca información sobre la configuración de una PKI en este entorno exigente; algunos expertos sugirieron que era posible, pero claramente se trataba de una tarea abrumadora.

Dados sus requisitos de seguridad, el equipo sabía que la solución tendría que incluir módulos de seguridad de hardware (HSMs).

"Sabíamos que necesitábamos una solución de hardware certificada", informa el analista de seguridad líder de la empresa. "Teníamos que asegurarnos de que todas nuestras claves privadas tuvieran la protección más sólida disponible; habíamos leído demasiadas historias sobre el robo de claves privadas que comprometían PKI completas. Nuestra prioridad más importante es brindar servicios al público y teníamos que asegurarnos de poder brindar la mayor garantía disponible".

LA SOLUCIÓN: HSMs NSHIELD Y ASESORAMIENTO EXPERTO DE ENTRUST

Para implementar esta innovadora solución, la empresa eligió un conjunto de soluciones de Entrust que incluían los HSMs nShield® Connect y nShield Edge y nShield Time Stamping Option Pack. Con un legado de experiencia con los productos Entrust y el reconocimiento de su combinación superior de seguridad sólida con facilidad operativa, el equipo de seguridad sabía que sus soluciones Entrust brindarían la configurabilidad y flexibilidad necesarias para trabajar en este entorno exigente.

El equipo también se basó en la experiencia de los consultores del equipo de servicios profesionales de Entrust para ayudar a estructurar la implementación. "El equipo de Entrust fue increíble", dice el analista de seguridad líder. "Recuerden que esto nunca se había hecho antes. Había documentos técnicos que decían que se podía hacer, pero algunas de las tecnologías más avanzadas y complejas no se habían comprobado en una implementación real. Entrust proporcionó los HSMs empresariales, nos enseñó cómo configurarlos y utilizarlos correctamente en nuestro entorno específico y nos ayudó a unir todas las piezas con la capacitación. Sus consultores tenían un gran conocimiento y experiencia en tecnología PKI, y su dedicación para garantizar un proyecto exitoso era insuperable".

Empresa de servicios públicos Fortune 500

¿Los resultados? “Nuestra solución de Entrust ha tenido un impacto fenomenal en las operaciones. Nuestra infraestructura ahora puede soportar una serie de proyectos adicionales que se encontraban pendientes. Y nuestra PKI está realizando la labor para la que fue creada: no solo emitir certificados de servidor, sino realmente habilitar muchos tipos diferentes de servicios. Dependemos de la PKI para muchas cosas. Y cuanto más depende de ella, más imprescindible se vuelve la seguridad basada en hardware”.

HARDWARE DE ENTRUST

Los productos implementados en esta solución incluyen:

HSM nShield Connect de Entrust

Este HSM conectado a la red de alto rendimiento proporciona servicios criptográficos seguros como un recurso compartido para instancias de aplicaciones distribuidas y máquinas virtuales. Los HSMs nShield Connect ofrecen una forma rentable de garantizar los niveles adecuados de control físico y lógico para los sistemas basados en servidores. Con los HSMs nShield Connect, las organizaciones pueden:

- Minimizar los costos operativos con una potente arquitectura de administración de claves
- Maximizar la utilización y la escalabilidad con una plataforma centralizada compartida
- Proporcionar protección criptográfica para la arquitectura de red en implementaciones tradicionales, virtualizadas y en la nube
- Superar las vulnerabilidades inherentes de la criptografía basada en software

HSM nShield Edge de Entrust

Este HSM conectado por USB proporciona una forma rentable para que las organizaciones implementen criptografía de alta seguridad. Con una mayor portabilidad y conectividad USB, los HSMs nShield Edge son especialmente adecuados para computadoras portátiles y en entornos de estaciones de trabajo o de escritorio, y su diseño compacto y lector de tarjetas inteligentes integrado los hace perfectos para implementaciones con espacio limitado o donde los HSMs se usan solo en ocasiones.

nShield Time Stamping Option Pack de Entrust

Esta solución llave en mano y de alta seguridad para el sellado de tiempo mantiene la hora exacta y proporciona sellos de tiempo seguros para la creación de registros, el archivo y la sincronización de otros eventos asociados con registros y aplicaciones electrónicos. nShield Time Stamping Option Pack de Entrust protege las operaciones de sellado de tiempo por medio de un hardware resistente a manipulaciones indebidas certificado de forma independiente y ofrece una precisión de tiempo y una auditabilidad superiores.

Empresa de servicios públicos Fortune 500

BENEFICIOS: DISPONIBILIDAD, SEGURIDAD Y SERVICIOS MÁS AMPLIOS

La solución de Entrust ofrece varias ventajas fundamentales:

Alta disponibilidad

La configuración en clúster y las funciones de resistencia de los HSMs nShield permiten una mayor redundancia, incluida la conmutación por error automatizada que proporciona una recuperación ante desastres más sólida y una disponibilidad continua.

Mayor seguridad

A medida que la empresa abre la red a más dispositivos, los HSMs nShield de Entrust permiten una autenticación más sólida mediante la emisión de certificados de dispositivos. La PKI puede emitir certificados para todos los dispositivos, y los dispositivos personales solo tienen acceso limitado a la red.

Múltiples factores de forma para HSMs

El uso de HSMs nShield de Entrust le permite a la empresa comprar hardware del tamaño adecuado para computadoras portátiles y servidores y no verse obligada a "comprar de más".

Soporte de medición inteligente

A medida que la empresa implementa tecnología de medición inteligente, la solución garantizará la integridad y confidencialidad de los datos transmitidos.

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.

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com