

TRUST LIFECYCLE MANAGER MEJORA EL ACCESO DE LOS EMPLEADOS Y GARANTIZA LA SEGURIDAD DE LOS ACTIVOS

Resumen ejecutivo

Nombre de la empresa: DigiCert

Sector: Tecnológico

Sede central: Lehi (Utah)

Requisitos empresariales clave:

- Garantizar que una plantilla global e híbrida tenga acceso a las aplicaciones y los datos corporativos en todo momento.
- Automatizar los niveles de acceso durante todo el ciclo de vida de los empleados, desde su incorporación hasta la finalización de su contrato.
- Minimizar las llamadas al servicio de asistencia técnica para que los equipos de TI tengan menos carga de trabajo y puedan centrarse en proyectos que realmente desarrollen el negocio.

Solución:

- DigiCert Trust Lifecycle Manager con la integración de MDM y SCEP
- DigiCert ONE CA Manager

Principales ventajas:

- Gracias a las plantillas, al equipo de asistencia técnica le resulta sencillo crear certificados que cumplen las políticas de seguridad corporativas.
- Las integraciones de SCEP permiten realizar la inscripción automática de certificados directamente a través de las soluciones de MDM de la empresa.
- La automatización optimiza la gestión de certificados y reduce la complejidad y la probabilidad de que se produzcan incidentes relacionados con los certificados.
- La gestión proactiva del ciclo de vida de los certificados ayuda a evitar las interrupciones de servicio y, por lo tanto, a reducir las llamadas al equipo de asistencia técnica.

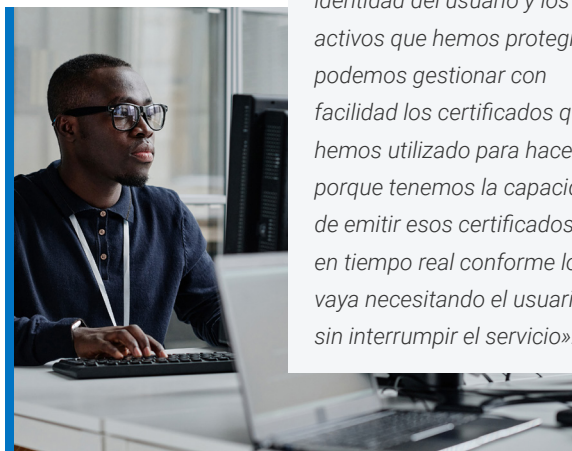
Requisito

Garantizar que los empleados de DigiCert a nivel global tengan acceso a la red corporativa en todo momento

El equipo de asistencia técnica de DigiCert está compuesto por 15 personas que prestan servicio a más de 1600 trabajadores repartidos por todo el mundo. Entre sus responsabilidades se incluye garantizar que los empleados puedan conectarse a la red, las aplicaciones y los datos de la empresa sin interrupciones para hacer su trabajo, ya sea desde la oficina o desde cualquier sitio. También debe asegurarse de que el acceso se otorga exclusivamente a usuarios y dispositivos autenticados, ya que los sistemas de acceso remoto constituyen un vector de ataque de lo más común.

El equipo se enfrentaba a diferentes dificultades a la hora de buscar el equilibrio entre una seguridad de TI férrea y el acceso ininterrumpido de los empleados y sus dispositivos. Para empezar, el aprovisionamiento de todas las cuentas de los usuarios para gestionar el acceso basado en roles era una tarea muy laboriosa. Además, para conseguirlo, era necesario que los endpoints de los usuarios y los recursos de la empresa pudieran conectarse entre ellos con facilidad y se integrasen perfectamente con las soluciones de gestión de dispositivos móviles (MDM) Intune (Windows) y Kandji (macOS e iOS). Por último, el equipo necesitaba gestionar el ciclo de vida de todos los certificados digitales necesarios para autenticar los dispositivos y los usuarios.





«Además de conocer la identidad del usuario y los activos que hemos protegido, podemos gestionar con facilidad los certificados que hemos utilizado para hacerlo porque tenemos la capacidad de emitir esos certificados en tiempo real conforme los vaya necesitando el usuario sin interrumpir el servicio».

Asimismo, había una situación que se repetía con demasiada frecuencia: el equipo de asistencia técnica no sabía que un certificado de cliente había caducado hasta que el empleado perjudicado se ponía en contacto con él porque había dejado de tener acceso a la red corporativa. «Cada llamada al servicio de asistencia técnica nos lleva unos 10 minutos como mínimo, pues diagnosticamos los problemas mediante una lista de comprobación de prácticas recomendadas para la solución de problemas. Esto era muy frustrante, sobre todo cuando veíamos que, cada dos por tres, el origen del problema era un certificado caducado», explica Rob Carnesecca, director de TI de DigiCert.

Solución

DigiCert Trust Lifecycle Manager proporcionó funciones de CLM automatizadas que se integraban con las plataformas de MDM

Por suerte, el equipo de Rob Carnesecca tenía acceso a DigiCert Trust Lifecycle Manager (TLM), una sólida plataforma de gestión del ciclo de vida de los certificados (CLM) e infraestructura de clave pública (PKI) diseñada para la empresa. A diferencia de otras soluciones de la competencia, Trust Lifecycle Manager podía generar y gestionar los certificados de cliente que se utilizaban para autenticar los dispositivos y los usuarios. Además, ofrecía integraciones listas para usar con diferentes soluciones de MDM.

Trust Lifecycle Manager permitía automatizar todos los aspectos del ciclo de vida de los certificados, desde la emisión hasta la renovación o la revocación.

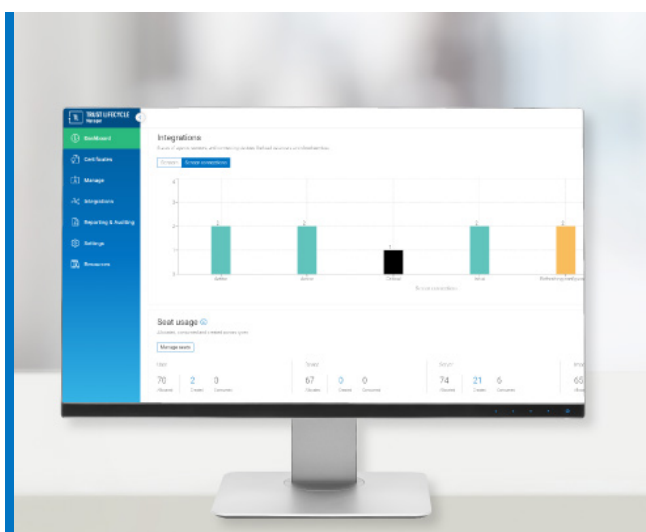
«Gracias a Trust Lifecycle Manager, podemos saber qué certificados están a punto de caducar y renovarlos automáticamente durante todo el tiempo que el usuario esté activo en nuestro sistema —explica Rob Carnesecca—. Además de conocer la identidad del usuario y los activos protegidos, podemos gestionar fácilmente los certificados que hemos utilizado para hacerlo porque podemos emitirlos en tiempo real conforme necesite el usuario sin interrumpir el servicio».

Uso de las integraciones y los perfiles para optimizar la CLM

Para instalar los certificados que autentican los dispositivos correctamente, el equipo de asistencia técnica requería procesos que pudieran ejecutarse en las soluciones de MDM de la empresa. La integración de SCEP de Trust Lifecycle Manager permite inscribir los certificados automáticamente, por lo que un certificado privado emitido desde DigiCert ONE CA Manager se puede administrar mediante Kandji o Intune sin tener que configurar o gestionar de forma manual los múltiples procesos que deben ejecutarse sobre la marcha.

Además, Trust Lifecycle Manager proporciona diferentes perfiles que el servicio de asistencia técnica pudo configurar utilizando plantillas sencillas para optimizar la integración. «Dada mi limitada experiencia con los certificados, no habría sabido ni por dónde empezar de no ser por las plantillas que ofrece TLM para configurar los enlaces SCEP —confiesa Jordan Wilcox, administrador de sistemas de DigiCert—. Configurar perfiles con TLM es extremadamente sencillo: basta con seleccionar la plantilla de SCEP para Intune y responder unas cuantas preguntas, y TLM se encarga de hacer el resto».

Trust Lifecycle Manager también ofreció al equipo perfiles basados en plantillas para automatizar otras integraciones con recursos de la red y diferentes niveles de acceso basado en roles, entre otras opciones. «Incluso hay plantillas para configurar el periodo de validez de un certificado y renovarlo antes de que caduque», añade Jordan Wilcox.



Gestión y escalabilidad totalmente automatizadas

La capacidad de automatizar tantos aspectos de la gestión de los certificados permitió al equipo de Rob Carnesecca aprovechar de verdad las ventajas que brinda la PKI para gestionar todos los aspectos de la seguridad de los usuarios y los dispositivos con rapidez y sin apenas sobrecarga. «TLM es una solución muy completa: por un lado, podemos establecer un certificado para aprobar un dispositivo e indicar que pertenece a DigiCert. Por otro lado, podemos establecer otro certificado que se comunica con nuestra infraestructura de red y valida el acceso de dicho dispositivo a un recurso específico. De ese modo, conseguimos proteger las aplicaciones mediante un certificado —explica Rob Carnesecca—. Además, sabemos que tenemos las herramientas necesarias para confiar en que la automatización de TLM se encargue de realizar todos esos procesos».

Como señala Rob Carnesecca, los trabajadores de DigiCert se encuentran repartidos por todo el mundo, por lo que habría sido difícil que su equipo pudiese satisfacer todas las necesidades empresariales sin la ayuda de una plataforma como Trust Lifecycle Manager. «Me parece importante destacar que TLM es una solución global que abarca cualquier región geográfica. Esto es especialmente importante en los casos en los que nuestros recursos no coinciden exactamente con nuestras zonas horarias —apunta—. Como muchas de estas tareas pueden automatizarse, no solo somos capaces de garantizar la seguridad de nuestros usuarios, sino que también sabemos que los recursos de la empresa están protegidos y que siempre podemos ampliar capacidades para gestionar más recursos y usuarios sin sobrecargar al equipo».

«Como muchas de estas tareas pueden automatizarse, no solo somos capaces de garantizar la seguridad de nuestros usuarios, sino que también sabemos que los recursos de la empresa están protegidos».



«Saber que TLM se encarga de renovar automáticamente los certificados para que no haya interrupciones en el servicio me da mucha tranquilidad. Puedo configurarlo y olvidarme del tema, algo que se agradece cuando tienes que estar pendiente de que todo funcione de forma ininterrumpida».



Seguridad y accesibilidad mejoradas y reducción drástica de la sobrecarga

Trust Lifecycle Manager ha puesto fin al doble reto que suponía proteger los recursos de DigiCert con una alta disponibilidad y garantizar la facilidad de uso para los empleados de la empresa. Y, lo que es mejor, ha reducido drásticamente la sobrecarga de los equipos de TI para que los trabajadores que antes invertían gran parte de su jornada en responder las llamadas al servicio de asistencia técnica ahora dediquen ese tiempo a proyectos que maximizan las oportunidades comerciales.

«Saber que TLM se encarga de renovar automáticamente los certificados para que no haya interrupciones en el servicio me da mucha tranquilidad. Puedo configurarlo y olvidarme del tema, algo que se agradece cuando tienes que estar pendiente de que todo funcione de forma ininterrumpida», añade Jordan Wilcox.

Empiece a disfrutar de las ventajas de DigiCert® Trust Lifecycle Manager hoy mismo. Envíe un correo electrónico a sales@digicert.com.