digicert®

Evaluación del software de firma y adopción de una política de firma de código

Las mejores prácticas que hay que tener en cuenta para lograr una seguridad más robusta en el proceso de publicación de software sin ralentizar el ciclo de CI/CD.

GUÍA DE COMPRA

Introducción

Los ataques a la cadena de suministro de software y otras formas de propagación de malware pueden hacer que las empresas pierdan la confianza de los clientes, además de mucho tiempo y dinero intentando corregirlos. Estos ataques de gran repercusión pueden traducirse en violaciones de datos, peticiones de rescate y sistemas completamente paralizados.

Paralelamente, los puntos de vulnerabilidad en la seguridad del software se han multiplicado por varios motivos: el desarrollo ágil ha aumentado la frecuencia de los ciclos de compilación, la implementación y la orquestación en la nube han cambiado «el centro de mando» de la entrega de software y el número de dispositivos conectados se ha disparado, lo que exige actualizaciones de firmware y comunicaciones seguras.

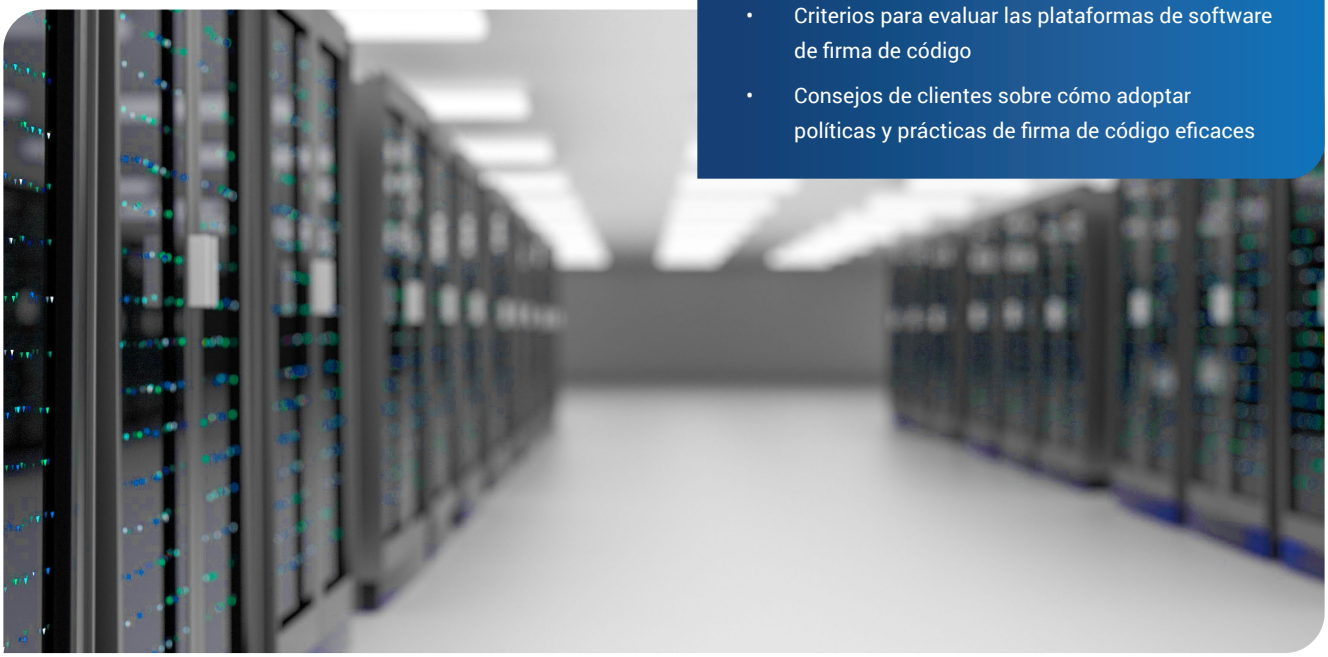
Ahora más que nunca, las empresas necesitan mejorar la seguridad de sus ciclos de vida de desarrollo de software. El software de firma de código centraliza la gestión de la actividad de firma de código, además de normalizar y aplicar las políticas y prácticas de firma de código que reducen las vulnerabilidades en el software.

A la hora de evaluar e implementar soluciones de software de firma de código, asegúrese de basar sus decisiones en estos criterios:

1. Configuración flexible
2. Métodos exhaustivos de almacenamiento y gestión de claves
3. Integración y automatización de los flujos de trabajo
4. Informes centralizados y flexibles
5. Controles para el proceso de publicación
6. Implementación flexible y ampliable

Esta guía de compra está dirigida a clientes que desean mejorar la seguridad de su proceso de publicación de software. En ella, encontrará:

- Criterios para evaluar las plataformas de software de firma de código
- Consejos de clientes sobre cómo adoptar políticas y prácticas de firma de código eficaces



Configuración flexible

La posibilidad de establecer configuraciones detalladas para las estructuras de las cuentas y los roles y permisos de los usuarios permite a las empresas adaptar las funciones del sistema a sus necesidades corporativas específicas.

Objetivos

- Centralizar la gestión del entorno de certificados y claves de firma de toda la empresa
- Adaptar las estructuras y funciones de las cuentas a las necesidades de seguridad
- Limitar el acceso a los sistemas a los usuarios autorizados
- Eliminar los puntos de vulnerabilidad únicos de las funciones críticas
- Aplicar una política Zero Trust para el acceso a las cuentas
- Mejorar la eficiencia de la asignación y revocación de privilegios del sistema

En qué fijarse

- Importación de claves y certificados para consolidar todo el entorno de claves y certificados
- Configuración de cuentas centralizada y estructuras de usuarios, incluida la configuración de ICA y atributos de ICA
- Roles y permisos de usuario detallados con controles de políticas de acceso
- Permisos de quorum para funciones que requieren la aprobación de dos partes
- Compatibilidad con la autenticación multifactor
- Perfiles a nivel de grupo

Consejo n.º 1 sobre la política y las prácticas de firma de código

Los clientes utilizan diferentes métodos para aplicar la política de firma de código mediante software de firma de código. Algunos crean un documento de política formal, otros basan sus prácticas de firma de código en consejos y formación y otros confían en el uso de software para la aplicación centralizada de la política.

Consejo n.º 2 sobre la política y las prácticas de firma de código

Los aspectos que más preocupan a los clientes en materia de gestión de claves son: quién gestiona las claves, dónde se almacenan y la definición y aplicación de los permisos de firma.

Métodos exhaustivos de almacenamiento y gestión de claves

Los controles detallados de almacenamiento y gestión de claves permiten a las empresas eliminar incoherencias en las prácticas de gestión de claves y evitar accesos y usos no autorizados o inadecuados.

Objetivos

- Seleccionar el método de almacenamiento de claves que mejor se adapte a las necesidades de seguridad (por ejemplo, confianza pública o privada)
- Establecer controles más estrictos para los proyectos delicados
- Limitar el acceso durante las investigaciones de posibles amenazas
- Utilizar diferentes prácticas de uso de claves para los entornos de producción y de pruebas
- Aplicar el modelo de uso de claves adecuado según los requisitos de la plataforma de software de destino
- Reducir el uso de claves que contengan elementos criptográficos obsoletos, poco seguros o no conformes
- Aumentar la eficiencia y reducir el error humano

En qué fijarse

- Opciones de almacenamiento de claves para módulos de seguridad de hardware (HSM) o almacenamiento cifrado
- Perfiles de acceso a las claves que estipulen quién puede acceder a qué claves y cuándo Modos de claves de firma en línea y fuera de línea, para permitir una respuesta rápida
- Tipos de claves de firma para entornos de producción y de pruebas
- Modelos de uso de claves estáticas, dinámicas y rotatorias
- Controles detallados de los perfiles de pares de claves
- Plantillas de perfiles de certificados con flujos de trabajo de generación de un solo clic

Consejo n.º 3 sobre la política y las prácticas de firma de código

Según los clientes, los principales motivos para el desarrollo de políticas y prácticas de firma de código son el cumplimiento de la normativa empresarial y oficial y los requisitos de los clientes y las plataformas.

Integración y automatización de los flujos de trabajo

La integración y la automatización evitan que se produzcan errores manuales, mejoran la eficiencia, favorecen la coherencia de las prácticas de firma y contribuyen a los objetivos del desarrollo ágil en materia de plazos de salida al mercado.

Objetivos

- Ofrecer seguridad sin ralentizar el proceso de desarrollo
- Alcanzar mayores niveles de seguridad y cumplimiento de las normativas corporativas de manera más cómoda para los usuarios, en comparación con los procesos de firma manuales
- Minimizar el riesgo de que se produzcan interceptaciones del código fuente durante el proceso de firma

En qué fijarse

- Integración con ciclos de CI/CD, con opciones de línea de comandos, consola o API
- Compatibilidad con diferentes plataformas de CI/CD
- Accesos y privilegios centralizados y preconfigurados para desarrolladores y servidores de compilación
- Generación de certificados y plantillas de certificados preconfiguradas
- Firma de hash, que elimina la necesidad de transferir el código fuente

Consejo n.º 4 sobre la política y las prácticas de firma de código

Los clientes consideran que su política de firma de código —que se aplica a través de software de firma de código y está gobernada por un departamento de seguridad o TI designado— es muy eficaz.

Consejo n.º 5 sobre la política y las prácticas de firma de código

Los clientes señalan que tanto los equipos de seguridad como los de TI son participantes clave en la creación de sus políticas de firma de código. Entre los colaboradores que mencionaron se incluyen el CISO , el departamento de gestión de riesgos y cumplimiento , DevOps, SecOps, el departamento de gestión de productos y los equipos de ciberseguridad y TI.

Controles para el proceso de publicación

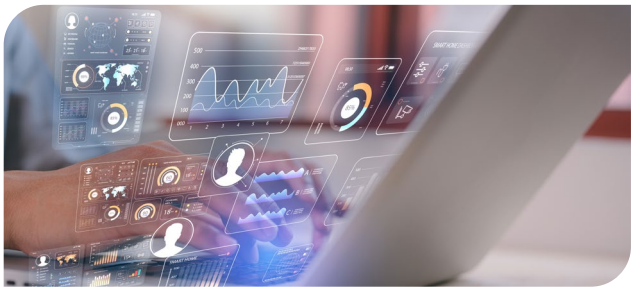
Los controles para el proceso de publicación proporcionan comprobaciones adicionales que pueden ayudar a evitar la inyección de malware durante el propio proceso de compilación.

Objetivos

- Reducir el riesgo de que se produzcan actividades maliciosas durante el proceso de publicación

En qué fijarse

- Atributos y controles del período de publicación que definan el acceso de los usuarios, los plazos programados y otros criterios que limiten el acceso a los usuarios autorizados
- Funciones de comparación de versiones que utilicen el principio de las compilaciones reproducibles para definir un referente con el que comparar las compilaciones posteriores



Informes centralizados y flexibles

Los informes centralizados ayudan a acelerar la corrección, cumplir los requisitos de auditoría e identificar posibles problemas o amenazas.

Objetivos

- Obtener visibilidad y control totales de las actividades de firma de código
- Saber quién firmó qué y cuándo, para agilizar la corrección
- Garantizar el cumplimiento de las auditorías

En qué fijarse

- Registro e informes centralizados que faciliten la auditoría y el seguimiento de la actividad
- Filtros para los informes, con exportación como archivos con y sin formato

Consejo n.º 6 sobre la política y las prácticas de firma de código

Los clientes consideran importante normalizar el proceso de firma de código —de manera que quede documentado sea rastreable y seguro y facilite la asignación de responsabilidades— y garantizar el origen y la integridad de los paquetes de software de la empresa a los clientes finales.

Implementación flexible y ampliable

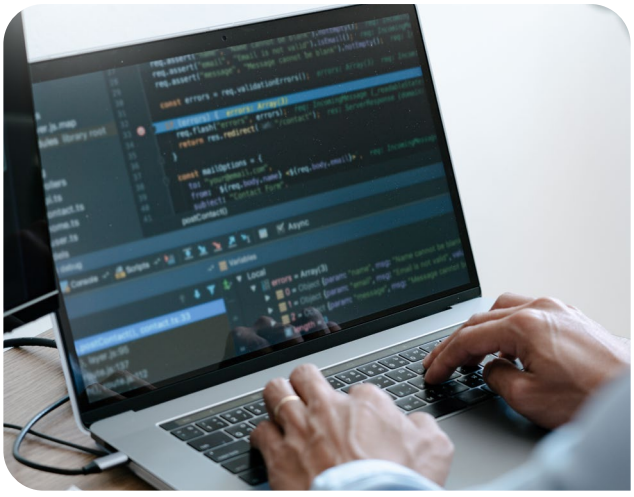
Las empresas deben, por un lado, buscar modelos de implementación flexibles que les permitan cubrir sus distintas necesidades de implementación y, por el otro, evaluar la escalabilidad de las soluciones en función de sus requisitos de firma previstos.

Objetivos

- Capacidad de elegir el modelo de implementación que la empresa prefiera
- Capacidad de hacer frente a grandes cantidades de actividades de firma que se producen a gran velocidad
- Configuración eficiente con escalabilidad bajo demanda

En qué fijarse

- Opciones de implementación local, en la nube o híbrida para abordar de principio a fin las necesidades de entrega en toda la empresa
- Configuración rápida y eficiente de ICA para divisiones con requisitos de configuración de seguridad específicos
- Arquitectura basada en contenedores con orquestación para facilitar la escalabilidad rápida y eficaz



Resumen

El software de firma de código puede reducir considerablemente los puntos de vulnerabilidad en los procesos de publicación de software. Las soluciones de nivel empresarial que ofrecen una configuración flexible y un conjunto de funciones completo son las más adecuadas para ayudar a las empresas a cumplir los objetivos de sus políticas y prácticas de firma de código. Estas soluciones brindan:

Protección

- Eliminan los puntos de vulnerabilidad que pueden dar lugar al robo o uso indebido de las claves
- Evitan la inyección de malware en el proceso de publicación

Gestión

- Favorecen una seguridad y un cumplimiento coherentes en todos los equipos implicados en el proceso
- Centralizan la visibilidad y el control de la actividad de firma

Productividad

- Mejoran la eficiencia y reducen el error humano
- Crean agilidad para responder a los cambios relativos a la criptografía y el cumplimiento

¿Empezamos?

DigiCert ofrece soluciones de seguridad SSL, PKI e IoT de gama empresarial a algunas de las mayores organizaciones del mundo, quienes a cambio disfrutan de la tranquilidad de saber que sus datos están a salvo en todo momento. Hable de sus necesidades con nuestros expertos.

Para obtener más información, llame al (+1) 801 770 1736, envíe un correo electrónico a pki_info@digicert.com o visite digicert.com/es/software-trust-manager