



App Shielding con Protección en Tiempo Real

Combata los ataques a las aplicaciones móviles con una protección completa de su dispositivo desde adentro hacia fuera

NOTAS DESTACADAS

El enfoque holístico de la seguridad de App Shielding de OneSpan incluye:

- **Protección en modo inactivo**
 - Ofuscación del código
 - Prevención del re-empaquetado
 - Criptografía whitebox
 - Almacenamiento local seguro (ALS)
 - ROM de aplicación segura (SAROM)
- **Protección en tiempo real**
 - Jailbreak y root
 - Inyección anti-código
 - Registro anti-clave
 - Lector antipantalla
 - Capturas de pantalla antisistema
 - Anti-duplicación de pantalla y monitores externos
 - Depurador y emulador
 - Comprobación de la integridad y visibilidad para el análisis posterior
 - Varias respuestas diferentes en tiempo real

La mayoría de los usuarios actuales de la banca digital utilizan sus dispositivos móviles para realizar operaciones bancarias. Desgraciadamente, este fenómeno relativamente reciente ha coincidido con un aumento récord del fraude por medio de los equipos móviles. Al mismo tiempo, las aplicaciones móviles son cada vez más importantes para gestionar los procesos de una empresa, y lamentablemente, las mejoras y actualizaciones de las funciones muchas veces han tenido a prioridad sobre la seguridad, la cual tiende a considerarse una carga que solo obstaculiza el desarrollo y la velocidad de implementación.

Por eso es tan importante asegurarse que las aplicaciones estén completamente protegidas, tanto cuando estén inactivas como en el tiempo de ejecución, por medio de una solución fácil de usar que no requiere tiempo ni esfuerzo adicional por parte de su equipo de desarrollo.

Protección en modo inactivo

La seguridad robusta es esencial para cualquier aplicación móvil que contenga información personal identificable (IPI), u otra información sensible y confidencial relacionada con los pagos, los contratos inteligentes, los metadatos o las operaciones de su negocio. Esto es especialmente difícil para las aplicaciones que se ejecutan en dispositivos con jailbreak o rooteados.

App Shielding de OneSpan protege la información personal, las claves de cifrado y los secretos, como las claves de API dinámicas o estáticas, mediante un almacenamiento local seguro respaldado por criptografía whitebox y una ROM de aplicación segura (SAROM). Los datos sólo se descifran cuando son utilizados por la aplicación.



Para aumentar la resistencia a la ingeniería inversa, también ofuscamos el código de la aplicación móvil con técnicas avanzadas. App Shielding aplica la ofuscación de código después de la compilación, proporcionando un enfoque completamente no invasivo sin afectar al rendimiento de la aplicación. Además de esta capa protectora de seguridad, el propio App Shielding está ofuscado lo que hace con esta capa adicional hace que sea imposible eliminar o eludir App Shielding.

Junto con estas técnicas, protegemos la aplicación contra la manipulación y el reempaquetado de manera eficaz. App Shielding detecta si un atacante ha duplicado el código fuente de la aplicación e inyectado funcionalidad maliciosa. Si se detecta un reempaquetado, App Shielding hace que la aplicación dañada no pueda utilizarse.

Protección en tiempo de ejecución

Los dispositivos de los consumidores no están bajo el control de los desarrolladores de aplicaciones móviles, lo que puede poner en riesgo la seguridad de las aplicaciones en tiempo de ejecución.

App Shielding se integra sin problemas en las aplicaciones existentes para detectar, mitigar y proteger contra ataques durante el tiempo de ejecución. Este tipo de ataques incluyen la inyección de código la depuración, la emulación, la duplicación de pantalla, el enlace de aplicaciones y otros. La aplicación permanece protegida inclusive en dispositivos con problemas de seguridad, en caso de ataques novedosos y desconocidos hasta el momento, o bien si un dispositivo está

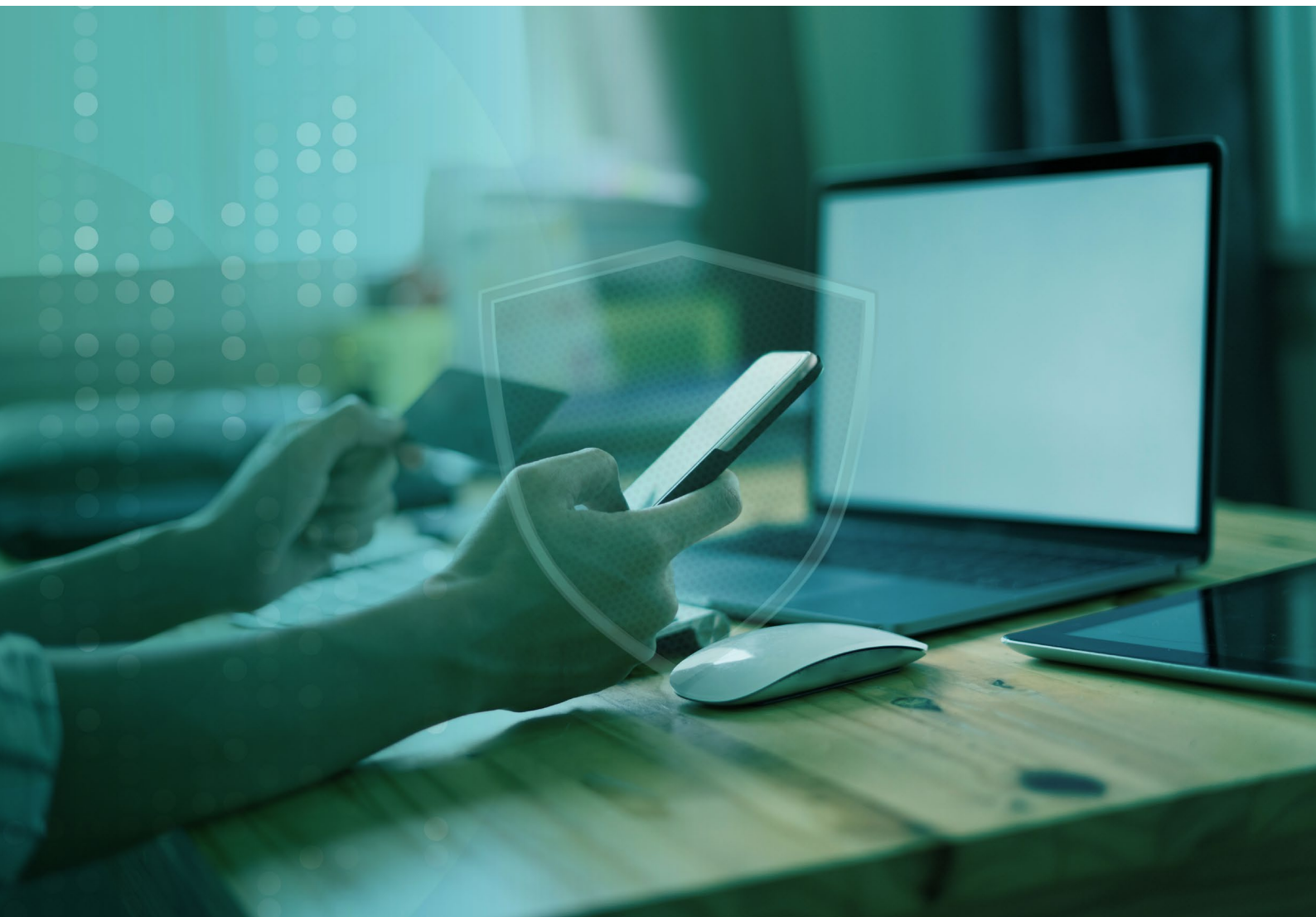
infectado con malware que utiliza teclados fraudulentos con registradores de teclas, capturas de pantalla remotas, capturas de pantalla o superposición de pantallas, la tecnología de autoprotección de aplicaciones en tiempo de ejecución detectará y evitará cualquier comportamiento no autorizado de la aplicación o del entorno.

OneSpan App Shielding protege contra los ataques de día cero y otros ataques dirigidos de forma proactiva, bloqueando la ejecución de código externo, cambiando dinámicamente la pantalla de la aplicación en función del riesgo o incluso cerrando la aplicación si existe una amenaza grave. Estas técnicas aseguran la integridad de la aplicación y protegen totalmente los datos personales y empresariales sensibles, evitando que caigan en manos de los delincuentes cibernéticos.

Reforzar la seguridad de las aplicaciones

App Shielding ofrece una amplia lista de funciones fáciles de integrar e invisibles para el usuario final. Estas funciones no afectan la experiencia del usuario ni ralentizan la ejecución de las operaciones en la aplicación. Como resultado, las empresas pueden ampliar y reforzar la seguridad de las aplicaciones, proteger a los clientes y desarrollar aplicaciones en cortos períodos de tiempo.

La solución también ayuda a aumentar la productividad operativa, ahorrándole tareas y trabajo manual al equipo de seguridad, eliminando errores y agilizando la certificación y las auditorías de aplicaciones. Esto no solo mejora la eficiencia del desarrollo, sino que también reduce el costo total.



Mobile Security Suite

App Shielding con protección en tiempo de ejecución está disponible como solución independiente, y también como una función opcional en OneSpan Mobile Security Suite. Mobile Security Suite es la solución de protección de aplicaciones móviles más completa de su clase. Integra perfectamente una serie de funciones de seguridad en cualquier aplicación móvil, como la identidad/authenticación, el almacenamiento y las comunicaciones seguras, la ofuscación, la criptografía whitebox y la protección en tiempo de ejecución, entre otras.

Cómo funciona

App Shielding tiene un triple enfoque para asegurar la integridad de las aplicaciones móviles: Proteger, detectar y reaccionar.

Primero, protege la aplicación móvil esquivando las técnicas de ingeniería inversa a través de la ofuscación del código, la criptografía whitebox y la tecnología anti reempaquetado.

En segundo lugar, detecta el registro de claves maliciosas, los lectores de pantalla, las aplicaciones reempaquetadas, los depuradores y emuladores, y los dispositivos con jailbreak o rooteados.

Por último, puede configurarse para reaccionar y eludir las actividades maliciosas, cerrando la aplicación o activando acciones personalizadas basadas en la política empresarial.



Sobre OneSpan

OneSpan, "The Digital Agreements Security Company™", ayuda a las organizaciones a acelerar su transformación digital respaldando la creación de acuerdos con clientes y experiencias de transacciones seguras, compatibles y muy fáciles. Las organizaciones que requieren altos niveles de seguridad, incluida la protección de los usuarios finales y la fidelidad de los registros de las transacciones para cada acuerdo, eligen OneSpan para simplificar y proteger los procesos comerciales con sus socios y clientes. OneSpan, que cuenta con la confianza de empresas líderes mundiales, incluido más del 60% de los 100 bancos más grandes del mundo, procesa millones de acuerdos digitales y miles de millones de transacciones cada año, en 100 países.

Visite [OneSpan.com](https://www.onespan.com)

Contáctenos www.onespan.com/es/contactenos



Copyright© 2022 OneSpan North America Inc., todos los derechos reservados. OneSpan®, el logo "O", Digipass®, Cronto® y "The Digital Agreements Security Company™" son marcas comerciales registradas o no registradas de OneSpan North America Inc. o sus filiales en Estados Unidos y otros países. Cualquier otra marca comercial citada en este documento es propiedad de sus respectivos dueños. OneSpan se reserva el derecho a hacer cambios en las especificaciones en cualquier momento y sin previo aviso. La información proporcionada por OneSpan en este documento se considera precisa y confiable. Sin embargo, OneSpan no se hace responsable de su uso, ni de la infracción de patentes o de otros derechos de terceros que puedan resultar de su uso.