

HIGHLIGHTS

App-Shielding mit Runtime-Protection umfasst:

- Overlay-Erkennung
- Jailbreak- und Root-Erkennung
- Verhindern von Code-Injektion
- Verhindern von Key-Logging
- Verhindern von Screenreadern- Verhindern von System-Screenshots
- Verhindern von Screen-Mirroring und externen Monitoren
- Schutz vor Repackaging
- Debugger- und VM-Debugger-Prävention
- Laufzeitschutz – Integritätsprüfung
- Emulator-Erkennung
- Verschleierung

MOBILE SECURITY SUITE: APP-SHIELDING MIT RUNTIME- PROTECTION

Abwehr von Angriffen auf mobile Anwendungen mit komplettem Schutz von innen heraus

In fieberhaftem Tempo entwickeln und vermarkten Unternehmen eigene Mobilapplikationen, vergrößern damit aber auch erheblich die Angriffsfläche für Betrug. Im Mittelpunkt dieser Bedrohung stehen Hacker, die mit Schadsoftware die Schwachstellen mobiler Betriebssysteme ausnutzen. Durch App-Shielding mit Runtime-Protection stattet OneSpan Unternehmen mit starker, nativ integrierter Applikationssicherheit aus, sodass diese Angriffe dynamisch erkannt und eingedämmt werden können.

Sichern sensibler Daten

App-Shielding durch OneSpan schützt proaktiv vor Zero-Day- und anderen gezielten Angriffen, damit mobile Business-Applikationen sicher laufen und die Ausführung fremder Codes blockiert bzw. die Applikation abgeschaltet wird, wenn Daten bedroht sind. Durch die Integration von App-Shielding mit Runtime-Protection in mobile Anwendungen wird deren Integrität vollständig gesichert und sensible geschäftliche sowie persönliche Daten werden vor Cyberkriminellen geschützt.

Integrierter Schutz

App-Shielding mit Runtime-Protection umschließt den Anwendungscode und schützt ihn so vor einer Injektion von fremdem Codes. Selbst wenn Geräte mit Schadsoftware infiziert sind – auch bei Systemkomponenten wie Screenreadern oder Key-Logging auf Android, erkennt die Runtime-Protection-Technologie diesen Code und verhindert dessen Ausführung.

Stärken der Anwendungssicherheit

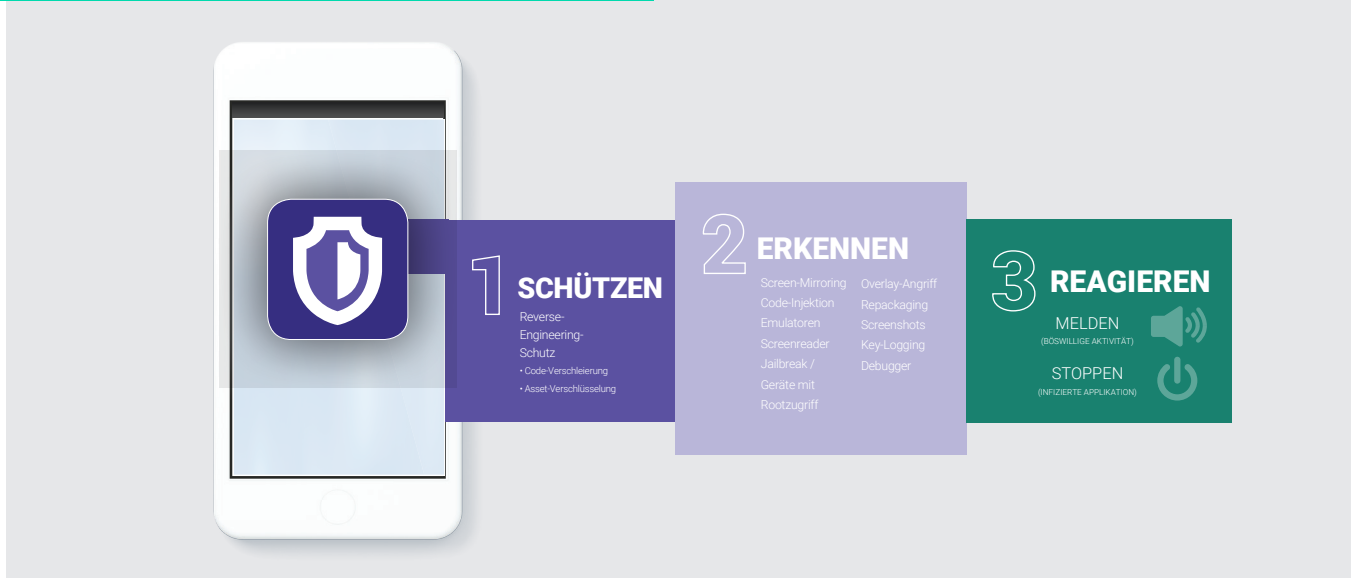
App-Shielding stellt eine umfassende Liste von Funktionen bereit, die leicht zu integrieren sind und für den Endnutzer unsichtbar bleiben. So können Unternehmen mit App-Shielding die Anwendungssicherheit ausbauen und stärken, Kunden schützen und auch anspruchsvolle Zeitpläne für die Entwicklung von Applikationen einhalten.

Mobile Security Suite

App-Shielding mit Runtime-Protection ist als optionales Feature der OneSpan Mobile Security Suite erhältlich. Die OneSpan Mobile Security Suite bietet eine umfassende Liste von Funktionen, mit denen Identität/Authentifizierung, sicheres Speichern und Kommunizieren, Verschleierung, Whitebox- Kryptografie, Runtime Protection und weitere Features nahtlos in nahezu alle mobilen Anwendungen integriert werden.



FUNKTIONSWEISE



App-Shielding mit Runtime-Protection sichert die Integrität mobiler Applikationen in drei Schritten: Schützen, Erkennen und Reagieren. Es schützt die vertrauenswürdige mobile Applikation, indem Reverse-Engineering-Techniken durch Code-Verschleierung und Anti-Repackaging-Technologie verhindert werden.

Böswilliges Key-Logging, Screenreader, Repackaging, Debugger und Emulatoren sowie Geräte mit gehacktem Dateisystem oder Rootzugriff werden aktiv erkannt. Das System kann mittels Konfiguration reagieren und böswillige Aktionen durch das Ausschalten der Applikation oder die Aktivierung bestimmter Benutzer-Aktionen basierend auf Geschäftsvorgaben verhindern.



OneSpan trägt zum Erfolg von Finanzinstituten und anderen Organisationen bei, indem wir sie auf ihrem Weg zur Digitalisierung begleiten und unterstützen. Kernfokus ist das Vertrauen in die Identität von Personen, in mobile Apps und in Finanztransaktionen. Wir sind überzeugt, dass dies die Grundlage für mehr Wertschöpfung und Wachstum ist. Mehr als 10.000 Kunden, darunter mehr als die Hälfte der 100 weltweit führenden Banken, vertrauen bereits auf Lösungen von OneSpan, um ihre wichtigsten Beziehungen und Geschäftsprozesse zu schützen. Vom digitalen Onboarding über die Betrugsbekämpfung bis hin zum Workflow-Management – die einheitliche, offene Plattform von OneSpan reduziert Kosten, beschleunigt die Kundenakquise und erhöht die Kundenzufriedenheit.



Copyright © 2020 OneSpan North America Inc. Alle Rechte vorbehalten. OneSpan™, Digipass® und Cronto® sind eingetragene oder nicht eingetragene Marken von OneSpan North America Inc. und/oder OneSpan International GmbH in den USA und anderen Ländern. Alle anderen Marken oder Markennamen sind Eigentum ihrer jeweiligen Besitzer. OneSpan behält sich das Recht vor, jederzeit und ohne Vorankündigung Änderungen an technischen Daten vorzunehmen. Die von OneSpan in diesem Dokument bereitgestellten Informationen werden als richtig und zuverlässig erachtet. OneSpan kann jedoch nicht für deren Nutzung oder die Verletzung von Patenten oder anderen Rechten Dritter durch ihre Verwendung haftbar gemacht werden.

Letztes Update im Dezember 2020

KONTAKT

Weitere Informationen:
info@OneSpan.com
www.OneSpan.com