



SICHERN SIE DEN DATENVERKEHR IHRER MOBILEN APPS VOR NEUEN BEDROHUNGEN

Mobile SDK | Link11 WAAP

Mobile API-Endpunkte sind schwer vor Angreifern zu schützen. Viele herkömmliche Web-Sicherheitstechnologien basieren auf einer Browserüberprüfung, die darauf ausgelegt ist, die von Angreifern typischerweise verwendeten Headless-Browser und Emulatoren zu erkennen. Bei mobilen Apps gibt es jedoch keinen Browser, der verifiziert werden kann.

Link11 WAAP ist eine umfassende All-in-One-Cloud-Sicherheitsplattform, die über ihr proprietäres Mobile SDK vollständigen Schutz für den mobilen Datenverkehr bietet: Ein einzigartiger Client-Zertifizierungsmechanismus für mobile Anwendungen. Unternehmen können ihre iOS- und Android-Apps mit dem integrierten SDK veröffentlichen.

Das SDK signiert die Anfrage, authentifiziert das Gerät und überprüft die Identität des Benutzers. Es signiert alle Anfragen, die von legitimen Apps stammen, und fügt jeder Anfrage eine kryptografische HMAC-Signatur hinzu. Die Signaturen sind nicht reproduzierbar, nicht erratbar und nicht wiederholbar.

Diese einfache Methode bietet einen zuverlässigen und sicheren Mechanismus, um zu bestätigen, dass der Datenverkehr von einem legitimen App-Benutzer und nicht von einem Bot oder Emulator stammt. Eingehender Datenverkehr, der nicht vom SDK verifiziert wurde, kann sicher abgelehnt oder mit anderen benutzerdefinierten Antworten konfiguriert werden.

Erweiterter Schutz für mobile Anwendungen



Einfache Verwendung

Das SDK wird auf der Client-Seite mit wenigen Zeilen Code aktiviert. Es kommuniziert direkt mit der Link11 WAAP-Instanz und deshalb sind keine Änderungen am Ursprungsserver erforderlich.



Hardened Software

Auf dem Client-Gerät wird das SDK unter anderem durch eine eindeutige App-Signatur kontinuierlich überprüft. Außerdem ist es in C++ verschleiert, um Reverse Engineering zu verhindern.



Flexible

Das SDK funktioniert sowohl in iOS- als auch in Android-Apps, unabhängig davon, ob der Zugriff über nativen Code, WebView oder Frameworks wie React Native erfolgt.



Zusätzliche Sicherheitsebene

Zusätzlich zum SDK schützt Link11 WAAP mobile Endpunkte mit seiner Next-Gen-WAF, fortschrittlicher Ratenbegrenzung, DDoS-Schutz und vielem mehr.



Geschützter Code

Selbst wenn Angreifer die Software irgendwie dekompileieren könnten, sind die Authentifizierungsmechanismen nicht zu kapern.



Mit dem Mobile SDK von Link11 erhalten Unternehmen eine leistungsstarke und ressourcenschonende Lösung zum Schutz des mobilen Datenverkehrs vor sich ständig weiterentwickelnden Bedrohungen. Link11 WAAP stellt sicher, dass nur legitime App-Anfragen Ihr Backend erreichen, und stärkt so die mobile Sicherheit, ohne die Komplexität zu erhöhen. In Kombination mit unserer umfassenden WAAP-Plattform können Unternehmen ihre mobilen APIs zuverlässig schützen, unbefugten Zugriff verhindern und eine nahtlose, sichere Benutzererfahrung bieten – ohne Leistungseinbußen.

Die Link11 WAAP -

Vier Lösungen in einer einzigen innovativen Plattform



Web Application Firewall (WAF)

Unsere Web Application Firewall (WAF) schützt vor allen Schwachstellen, die in den OWASP Top 10 aufgeführt sind, sowie vor Bedrohungen wie: Code- und SQL-Injektion, Cross-Site-Scripting und bösartige Payloads (Malicious Payloads). Im Gegensatz zu herkömmlichen Ansätzen, die sich nur auf die Erkennung von Signaturen und IP-Blockierung verlassen, umfasst die WAF von Link11 fortschrittliche Abwehrmechanismen wie die Auflistung der erlaubten Anwendungen und granulare Zugriffskontrollen (Access Controls, ACLs).



Web DDoS Protection

Link11 bietet umfassenden Schutz vor Layer-7-DDoS-Angriffen. Die Web DDoS Protection bietet Schutz vor einer breiten Palette von DDoS-Angriffsmethoden, einschließlich HTTP Floods, Slowloris-Angriffen, anwendungsspezifischen Angriffen und Zero-Day-Schwachstellenausnutzung.



Bot-Management

Link11 bietet eine Plattform mit einem leistungsstarken Bot-Management, das unerwünschten Bot-Traffic filtert, bevor er Ihre Anwendungen oder APIs erreicht. Unsere Lösung verhindert Datendiebstahl, Scraping, Credential Stuffing, Brute-Force-Angriffe, Anwendungsmissbrauch, Schwachstellen-Scans und Inventardiebstahl und schützt Ihre Systeme vor unerwünschtem Zugriff und Störungen.



API Security

APIs sind aufgrund ihrer weit verbreiteten Nutzung und der oft inkonsistenten Wartung häufige Ziele. Der API-Schutz von Link11 schließt diese Sicherheitslücken und bietet umfassenden Schutz für Ihre internetbasierten APIs. Unsere Lösung schützt vor einer Vielzahl von API-Angriffen, einschließlich der OWASP Top 10 API-Sicherheitsrisiken.

Über Link11

Link11 ist ein Cybersicherheitsunternehmen, das Lösungen für Netzwerksicherheit, Webanwendungs- und API-Schutz sowie Anwendungsleistung mit umfassendem Schutz für verschiedene Branchen, in Enterprise-Qualität, anbietet. Unsere Dienstleistungen reichen von vollständigem Netzwerk-DDoS-Schutz bis hin zu einer All-in-One-WAAP-Lösung, die Web Application Firewall, Web DDoS Protection, Bot Management (einschließlich ATO), API Protection und Secure CDN & DNS umfasst.

Als führender Anbieter von Cybersicherheitslösungen schützen wir Kunden weltweit vor sich ständig weiterentwickelnden Bedrohungen durch sorgfältige Detailarbeit und die frühzeitige Integration modernster Methoden.

Link11 WAAP - Vier umfassende Produkte in einer einzigen hochmodernen Plattform

BUILT TO DEFEND. ALWAYS AT YOUR SIDE.

