Zscaler SDK At-A-Glance

AT-A-GLANCE

The problem

Countless organizations build mobile apps that provide services to end users and, as such, house sensitive data. From banking and payment platforms to healthcare and citizen portals, these apps must be secured. But mobile app teams face four key challenges to doing so:

1. **APIs are exposed to the web:** Criminals constantly scan, test, and abuse public APIs (application programming interfaces). It's difficult to protect them without breaking access for legitimate users.
2. **Devices are an attack surface:** Devices compromised by rooting/jailbreaking, malware, or malicious apps or instrumentation frameworks enable overlay attacks, injection, and session theft.
3. **Transport security is risky and fragile:** Standard TLS and certificate pinning don't verify who accesses an app, enabling traffic interception; pinning also breaks apps during cert changes.
4. **Point products add complexity:** Using point tools for fraud prevention, device attestation, runtime protection, and observability slows performance and debugging via app bloat.

The solution

The Zscaler SDK (software development kit) is an all-in-one mobile application security SDK that empowers developers to protect both the application and the backend through a single lightweight integration. It combines:

1. Inside-out, zero trust connections that only expose APIs after identity and device verification, rendering APIs invisible to the public web.
2. Runtime application self-protection (RASP) to stop rooting/jailbreaking, emulators, overlay attacks, sideloaded threats, and more.
3. mTLS tunnels with bidirectional authentication to prevent interception and provide enterprise-grade security on unsecured networks.
4. Comprehensive cybersecurity with end-to-end and real-time observability into user connectivity, ISP performance, and cybersecurity posture.

Stated simply, the Zscaler SDK simplifies and enhances both frontend and backend security for mobile apps, all while improving your teams' abilities to troubleshoot and protect user experiences.

Zscaler SDK benefits

API security: Only verified apps and users can access APIs—all other traffic is blocked. There is no public exposure (or whitelisting or WAF tuning).

User privacy: Pre-login and post-login tunnels ensure privacy both before and after authentication, and protect sessions from interception.

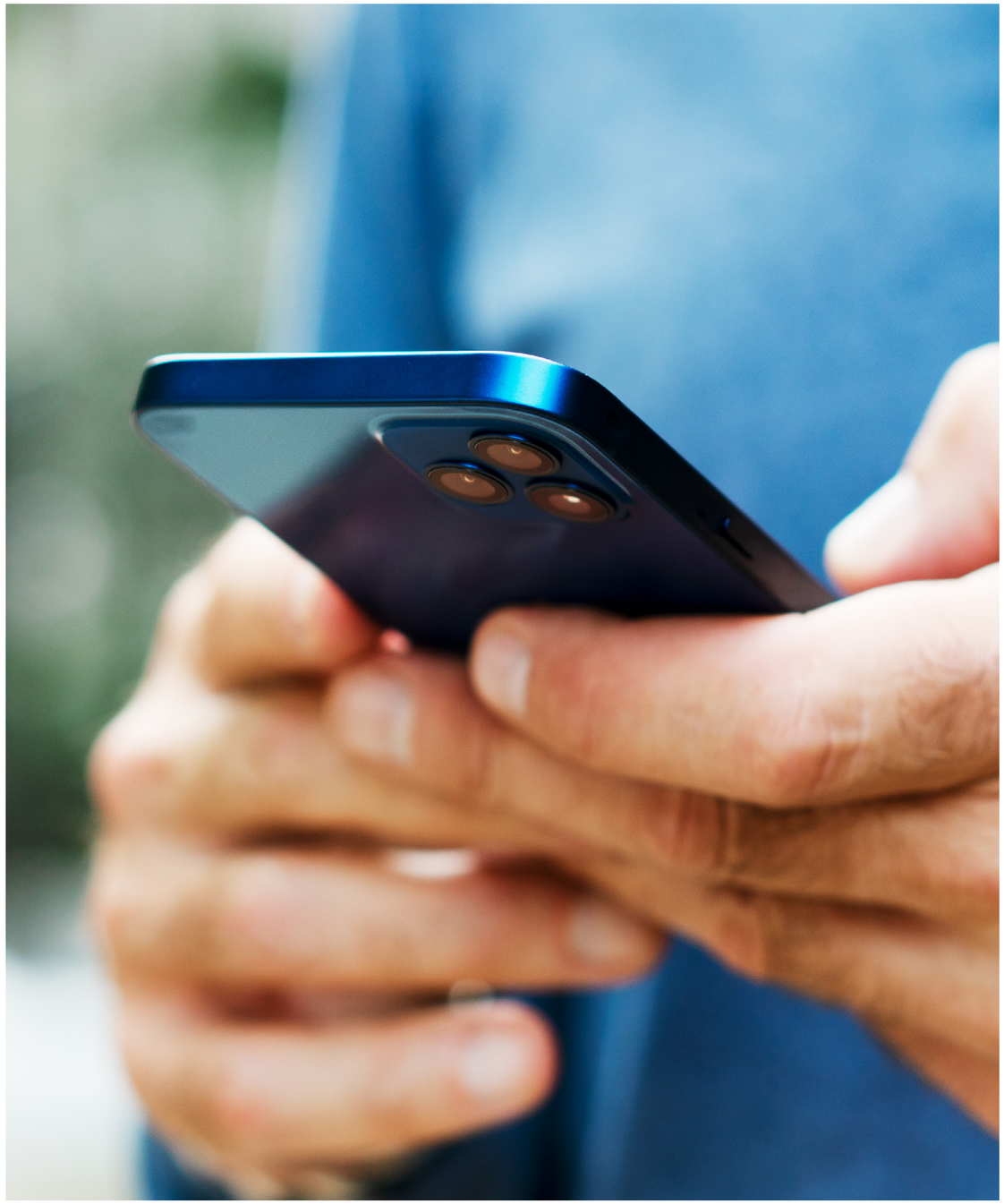
Built-in runtime protection: In-app telemetry and enforcement detect and stop real-time overlay fraud, emulator abuse, app tampering, and more.

Reduced SDK bloat: One solution replaces multiple vendors' SDKs by delivering identity enforcement, traffic protection, RASP, and observability.

No certificate management: Automated, at-scale mTLS with Zscaler eliminates manual efforts around certificate pinning and TLS handshakes.

Faster issue resolution: Integrated diagnostics identify if issues stem from networks, devices, or backends, accelerating mean time to resolution.

To learn more or see the Zscaler SDK in action, reach out to your Zscaler account team.



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere