Zscaler Mobile Security

The proliferation of mobile devices and platforms, and the BYOD movement has heightened the threat of security attacks and malicious mobile apps. With Zscaler Mobile Security Solution—you can harness the power of your mobile workforce without compromising on mobile security!

Zscaler Mobile Security is an enterprise grade solution custom built to address the evolving challenges of mobile data and app security for both employee-owned and corporate-issued mobile devices. Using Zscaler Mobile Security, IT administrators can detect and block against advanced web-based threats and malicious apps, apply consistent, user-based policy controls across multiple devices, and get instant visibility into all mobile traffic in the enterprise.

The Zscaler Advantage

- Modular solution format supports BYOD, corporate-issued and hybrid environments
- Provides multiple traffic forwarding options - Global HTTP proxy, GRE and IPSec VPN
- Protects browser and app traffic across all network types - 3G/4G/LTE and WiFi

LEARN MORE at **www.zscaler.com/mobile**
Speak with a specialist: **1-866-902-7811**

Key Benefits

Advanced Protection for Mobile Devices

By scanning every byte of inbound and outbound mobile traffic—browser and app–Zscaler provides comprehensive protection against malware and advanced security threats. *Zscaler Mobile App Profiler™* profiles apps for security and privacy risks, and identifies and blocks malicious apps.

Zscaler Analytics provides IT administrators instant and detailed traffic visibility through a 'single pane of glass'—allowing them to view transaction logs, run reports for instant analysis and cross-correlate user behavior across platforms, devices and locations. It also enables centralized policy control, including comprehensive data loss prevention (DLP) across devices to help meet compliance mandates for HIPAA, PCI, FISMA.

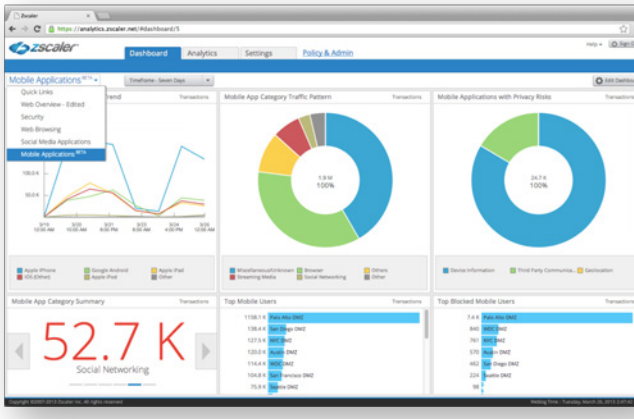
Simple, Low Touch Deployment

Zscaler Mobile Security provides a modular and scalable solution for varied deployment models - BYOD, company issued devices or hybrid environments. As a 100% cloud-based solution, it is low-touch, easy to deploy (via leading mobile device management solutions) and scales to address the needs of growing organizations. For the user, the solution is transparent and unobtrusive – applying the user's corporate security policies automatically across locations and network types, while maintaining a near-zero traffic latency.

Align with Changing Business Needs

The rapidly evolving mobile landscape necessitates security solutions to be agile in addressing changing technology and business initiatives. By focusing on protecting the data and providing multiple forward traffic mechanisms, Zscaler is able to effectively address the security requirements across current and emerging mobile hardware and OS platforms.

The modular solution format allows companies to pick features that are best suited to their mobile environment and business objectives. The subscription-based pricing model ensures that organizations only pay for what they need, eliminating the expense of investing in hardware and software capacity for future growth.



Product Components

Zscaler Mobile App Security and Control

By forwarding all mobile traffic to the Zscaler Security Cloud and inspecting it in real time, Zscaler protects against malicious apps, browser exploits, cross-site scripting, phishing and other advanced threats. *Mobile App Profiler™* fingerprints apps based on traffic patterns to detect any malicious behavior or suspicious activity such as apps leaking sensitive device or user specific information and classifies them as security or privacy risks to the Zscaler cloud.

IT administrators have complete traffic visibility via the Mobile Insights dashboard on the Zscaler Analytics portal. They can apply the user's corporate browsing policy (including DLP policies) across multiple devices, irrespective of location or network type. The in-depth classification of mobile apps by category, and risk profile empowers IT administrators to understand app-level threats and security incidents, and apply policies to minimize the risks.

Traffic forwarding to the Zscaler cloud can be done in multiple ways. All traffic from an office location can be forwarded via GRE or IPSec VPN. For Apple iPhones and iPads traffic can be forwarded to Zscaler by configuring the Global HTTP Proxy on supervised devices.

Zscaler SafeBrowser

A standalone browser, *SafeBrowser* can be deployed as the sole default browser (for corporate issued devices) or as the corporate compliant browser (for BYOD environments). SafeBrowser maintains a persistent proxy connection to the Zscaler Security Cloud across all mobile network types (3G/4G/LTE and WiFi) protecting the users' from web-based malware and advanced persistent threats.

SafeBrowser provides all critical browser functions such as customizing security and privacy settings, and supports rendering content using modern technologies like HTML5 and embedded videos or audios on web pages.

Zscaler SecureAgent

SecureAgent authenticates the user to the Zscaler Security Cloud and provides user notifications for any protective action taken by the Zscaler Mobile Security service. Protective actions include blocking access to content prohibited by company policy, blocking malicious apps, or blocking apps from stealing sensitive information from the device.

For Apple iPhones and iPads, SecureAgent enables the deployment of the Global HTTP Proxy configuration, allowing the user to authenticate to the Zscaler service. Once authenticated, the user's specific policies are applied to protect all traffic from the device. SecureAgent also allows shared usage of the device amongst multiple users, such as in school labs or hospital kiosks.

With trusted security, innovative app protection, and scalable deployment options, Zscaler Mobile Security provides organizations with the key capabilities they need to securely enable mobile users on any device, anywhere in the world.