ZIMPERIUM

Zimperium Mobile App Vetting

Mobile App Risk and Threat Analysis

Cybercriminals have adopted a mobile-first attack strategy to exploit the expanded and often unsecured mobile attack surface. Mobile threats go beyond operating system vulnerabilities and mishing (mobile-targeted phishing) exposure. The apps running on our mobile devices represent an equally, if not more effective, entry point for attackers. While organizations are increasingly aware of the risks mobile devices pose to enterprise data and user privacy, many remain unaware of the risks associated with the apps installed and running on mobile devices. These risks include data transmission to foreign entities; apps accessing unnecessary device permissions (such as the camera, microphone or device keyboard), app vulnerabilities that can be exploited by malware, and noncompliance with local and global regulations like MITRE, HIPAA, PCI, etc.

There are two main types of apps running on mobile devices that may access your data and systems:

- **Business apps:** External third party apps used by employees for work-related productivity as well as internally developed apps created in-house or contracted by third party developers for your organization.
- **Personal apps:** Apps installed by employees on the company device or their BYO device for their own purposes

Mobile App Vetting addresses the security and risk of third party apps and personal apps

Ensure Third-party Business Apps Keep Enterprise Data Safe

To foster workplace productivity, public and private organizations heavily rely on third-party apps for critical functions like CRM, collaboration, messaging, bug tracking, clinical trials, expense management, and more. The challenge lies in the limited visibility into the security posture of these apps, posing risks to the sensitive data they process and critical backend systems to which they connect. More due diligence is needed to ensure third-party apps are built to keep data safe, defend against attacks and comply with industry regulations and compliance standards.

Ensure that Personal Apps Installed on Employee Devices Don't Pose a Threat

Allowing Bring Your Own (BYO) or Enterprise or Government Furnished Equipment (EFE or GFE) devices to download apps for personal use is often important for employee satisfaction, but it may put your organization at risk. Organizations quickly find themselves lacking control over which personal apps employees download, leaving them with a tough choice: to restrict enterprise access from mobile devices which compromises productivity, **or permit personal app use with no restrictions which increases risk of potential data leakage or breach due to security vulnerabilities.** Navigating this delicate balance requires thoughtful strategies and robust security measures.

If third party and personal apps are not properly vetted, organizations are exposed to significant risks, including:

- Unsecured data transmission and storage - exposing sensitive enterprise data to attackers
- Security vulnerabilities - making the app susceptible to exploitation
- Malware & malicious code - can be used for hijacking credentials including 2FA codes and complete device compromise

Users and organizations assume that apps, whether for work or personal use, that are downloaded from an approved app store such as Google Play and Apple App stores, have been thoroughly vetted for security and **will keep their data safe.** The reality is very different. Most mobile app stores generally scan all newly available apps for known malware. However, not all mobile app updates are scanned for potential additions of malicious code or risky or dangerous permissions. This provides a window of opportunity for attackers to leverage insufficient mobile app security.

> CISOs evaluate all business web applications as part of their cyber risk and privacy efforts. They must apply the same rigor for mobile apps that run on user devices.

Zimperium App Vetting: Your Response to Mobile App Threats

Zimperium's App Vetting solution empowers enterprises with the critical visibility needed to assess the privacy and security risks of mobile applications used across their workforce. App risks are not limited to malware alone—everyday applications used for productivity, business, and finance can also introduce security vulnerabilities, excessive data collection, and compliance risks among other concerns. Without proper vetting, these apps can unknowingly expose sensitive enterprise data, including login credentials and even two-factor authentication codes, potentially becoming entry points for attackers.

By analyzing app behaviors, permission usage, data handling practices, and security vulnerabilities, Zimperium helps organizations identify potential threats before they compromise devices or corporate assets, while also ensuring employee privacy. With comprehensive risk intelligence and in-depth security assessments, enterprises can make informed decisions about the applications they allow within their environment. Proactively vetting mobile applications strengthens compliance efforts, reduces data breach risks, and ensures a safer mobile ecosystem for both employees and business operations. Zimperium App Vetting enables an organization to implement its own policy for risk tolerance on 23 app behavior categories.

APP VETTING™

Bolster Your Organizational Risk Program and Privacy Initiatives

Supports Organizational Cyber Risk Programs:
Zimperium Mobile App Vetting (MAV) provides Security Assessments & Ratings – This security summary focuses on risks contained in the application. Coupled with your enterprise app risk policy, Zimperium identifies non-compliant apps based on your unique predefined rule-driven policies.

Visibility is provided into risks that include, but are not limited to:

- **Security risk summary and details:** Risky functionality, code use, application capabilities, critical vulnerabilities, and threats
- **Third-party vulnerabilities and unauthorized behaviors:** Identification of embedded libraries or SDKs that may introduce risk
- **Compliance risk summary:** Evaluation against standards such as MITRE, OWASP, NIAP, CWE, MASVS, ADA, GDPR, HIPAA, PCI, CVE, and more
- **App features and permissions:** Visibility into potentially risky app functions and permission requests
- **Network communications:** Details on network behavior by country and domain

- **Data protection controls:** Identification of insufficient measures for data encryption, access, and handling
- **Unsecured transmission methods:** Alerts on unencrypted communication or insecure storage
- **Malicious code detection:** Alerts if malicious or suspicious code patterns are identified

Supports Privacy Requirement Compliance:
Zimperium MAV provides Privacy Assessments & Ratings: A privacy summary focused on the application's access to privacy data, including (but not limited to): user data, contacts, user identifiers, adware, SMS, and insecure data storage or communications.

About Zimperium

Zimperium is the world leader in mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank.

www.zimperium.com

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244