**Mobile Application Assessment**

**Mobile app** testing reduces risks, tests potential vulnerabilities, and examines software to ensure that an **application** is safe and meets adequate security compliance. **Mobile Application Security Assessment** services provide assurance that your mobile apps are secure. We provide you with a holistic and prioritized approach to testing mobile applications, which reduces your overall risk and remediation costs.

A mobile application security assessment looks at the security and compliance risks of your entire solution from the app on the device, the backend systems, the network the app connects to, and the interaction and data flow between them. Security experts well-versed in application development and coding who know the weaknesses threat actors try to exploit will thoroughly evaluate your security controls and provide actionable steps you can take.

The increased use of mobile devices has made it imperative for organizations to regularly run mobile application security assessments to **mitigate risks and prevent data breaches**.

# 7 Reasons Why Mobile App Security Testing Is Important

### 1. Prevent future attacks by guessing the behaviors of attackers and anticipating their moves

### 2. Going live with the new mobile application without excess worry about security risks

### 3. Change the architecture such as network, components of the mobile application if necessary

### 4. 3rd-party vendors are unfamiliar with enterprise IT environment and specific enterprise security standards and compliances

### 5. Know the skills and experience of the app development agency that builds your mobile applications

### 6. Test the responsiveness of your enterprise IT team

### 7. Meet tough industry security standards and comply with regulations



#### ****What are Mobile application testing essentials?****

Mobile application testing is very different from [software testing](https://www.testbytes.net/) and [web testing](https://www.testbytes.net/web-application-testing/). There are a few specifics that you should consider before performing mobile application testing:

* Screen resolution
* Turning on/off GPS
* Screen orientation (landscape, portrait)
* Different devices’ manufacturers
* OSs
* Type of mobile application

**BENEFITS OF MOBILE APPLICATION SECURITY ASSESSMENT**

* Quick and efficient identification of vulnerabilities in your mobile devices and apps before the damage is done
* Guidance on how to handle future risks
* Guidance on how to improve your mobile security
* Achieve compliance with the regulatory requirement
* We save you the headcount cost of running a full-time team of mobile apps security professionals

## Mobile App Security: Top 5 Security Threats to Mobile Devices

The drastic rise of smartphones in the workplace and everyday situations has made them the prime target for hackers. No computing device is 100% secure, and threat actors continue to explore new ways to exploit vulnerabilities on mobile devices. As reported by Nicholas Fearn, [mobile application attacks](https://www.computerweekly.com/feature/Application-security-more-important-than-ever) increased 63% in 2017, so it's crucial to stay aware of the biggest mobile security threats.



### 1. Unsecured Wi-Fi

Unverified servers and unsecured Wi-Fi networks at coffee shops or bookstores are a hacker's paradise, not to mention one of the biggest mobile security threats. According to CNBC reporter Jennifer Schlesinger, hackers are attempting to compromise enterprises through [mobile vulnerabilities](https://www.cnbc.com/2016/06/17/your-smartphone-could-be-hacked-without-your-knowledge.html) due to a rise of endpoint smartphones in the workplace.

Despite prompts warning smartphone users of potentially harmful and unverified servers, users will continue to connect to dangerous networks. Threat actors can leverage these unprotected networks to access sensitive data directly from phones or apps.

### 2. Apps with Malicious Code

Smartphone users downloaded 197 billion mobiles apps in 2017. However, people can download apps from third-party websites outside the Google Play Store or the Apple App Store. Hackers can use unsecured apps to exploit sensitive data from mobile users.

For instance, a malicious [mobile app malware](https://www.wired.com/2016/12/never-ever-ever-download-android-apps-outside-google-play/) strain called “Gooligan” infected 1.3 million Android users, and threat actors were able to steal user data. Hackers can create copycat apps and plant them on third-party app stores, then — just like phishing schemes — use the malicious software to steal data. You can prevent [mobile security threats](https://www.secureworks.com/blog/security-cost-of-smartphone-apps) by only downloading apps from official app stores.

### 3. Operating System Vulnerabilities

Smartphone manufacturers must continuously update operating software to accommodate technology improvements, new features, and improve overall system performance. A smartphone user is periodically advised to upgrade operating systems (for instance, iPhone users on iOS operating systems).

Software engineers monitor emerging vulnerabilities and adjust operating systems to address threats. However, users may choose to avoid system updates or perhaps their device is no longer compatible with the latest update. The best protection against emerging mobile threats is to update your operating system as soon as possible and upgrade your mobile device if the operating system is no longer compatible with new updates.

### 4. Data Leaks

Mobile apps typically store data on remote servers. Users often download apps and immediately fill out prompts to begin using the application but often do not adequately review the permissions. Advertisers can mine the data to learn more about target demographics, but cybercriminals can also gain access to servers and leak confidential data. Unintended data leaks can come from caching, insecure storage, and browser cookies.

### 5. Cryptography Issues

Mobile cryptography is crucial for security and assures that data and applications operate safely. iOS software must verify the application is digitally signed from a trusted source and then decrypt the app to execute it. Android software simply verifies the application is digitally signed, and doesn't necessarily verify the trustworthiness of the signer. This design of digital trust increases the importance of downloading applications from an official source.

Sensitive data at rest on a mobile device commonly falls victim to unintended disclosure due to poor, or complete lack of, cryptographic implementations. Developers dealing with tight deadlines or trying to cut corners may use encryption algorithms with existing vulnerabilities or not use any encryption at all. Threat actors can use these vulnerabilities or pillage data from a compromised mobile device.

## Mobile Application Security Assessment

Mobile app security assessments are essential cybersecurity measures for any enterprise with publicly available apps. Professional cybersecurity experts can assess the strength of an application against known and potential threats to protect not only your users but also the enterprise from potential disaster. Proper assessments can give you confidence on the security of your mobile apps and APIs. They reduce risks, save time, and implement actionable security measures to not only improve safety but meet mandatory compliance.

A professional security assessment covering this testing is the best practice to assess the security controls of your application. [Data breaches cost enterprises millions](https://www.secureworks.com/blog/data-breach-response-planning-cyber-threat-intelligence), and public reporting of a breach can severely impact a brand's reputation. Since smartphone and mobile app use will only increase in the future, reliable mobile security is an absolute must.

## Mobile App Testing Challenges

### Dependency On Engineering Teams For End-To-End Implementation

### Increased Complexity Of Tests Owing To Nonlinearity Of Mobile UX

### Probable Increase In Time-To-Market Of An App Update

## Top Mobile App Security Testing Tools

Enlisted below are the most popular Mobile App Security Testing tools that are used worldwide.

* ImmuniWeb MobileSuite
* Zed Attack Proxy
* Kiuwan
* Qark
* Micro Focus
* Android Debug Bridge
* CodifiedSecurity
* Drozer
* WhiteHat Security
* Synopsys