



Zimperium

z3A

Machine Learning-Based Mobile App Risk
and Threat Analysis for the Enterprise



Zimperium z3A

Enterprises are growing increasingly aware of the risks posed by mobile devices and apps. In the 2022 Zimperium [Global Mobile Threat Report](#), **42% of respondents reported that mobile devices and web applications have led to a security incident**. Despite the escalating threats, BYOD policies continue to be enabled throughout the enterprise, especially since the distributed workforce has exponentially grown. **Before the COVID-19 pandemic arose, 60% of organizations had no BYOD policies in place**. It is critical and more challenging than ever to strike a balance between enabling mobile access and minimizing the enterprise's exposure to attack.

Enterprises have therefore begun implementing methods to mitigate that risk, but traditional security techniques make it nearly impossible to effectively manage mobile device risk. The apps on those mobile devices can pose an entirely different attack vector that requires on-device analysis.

Nearly half of survey respondents (44%) have added security policies or requirements due to the growing number of cybersecurity incidents as a result of a distributed workforce.

Here's why. Enterprises often have limited visibility into the mobile security apps downloaded by their workforce. Many rely on antivirus solutions for app-focused security, potentially without realizing that some two-thirds of available mobile antivirus solutions have been demonstrated to be ineffective at best and fraudulent at worst.

Moreover, anti-malware solutions do not offer protection against cases where legitimate and malware-free apps nevertheless include code or behave in ways that inadvertently create risk. Also known as riskware, such apps can expose enterprises to data leakage and other threats.

In practical terms, this means that even if you achieve some insight into the mobile apps that users are utilizing in the enterprise via their devices, you still need a method of assessing the risks and threats those apps pose to the security and privacy of the workforce and to the business. Only with valuable insight into risks and vulnerabilities can you set security policies in place to reduce that risk.

56% of technology professionals rely on at least four to eight enterprise applications for productivity.

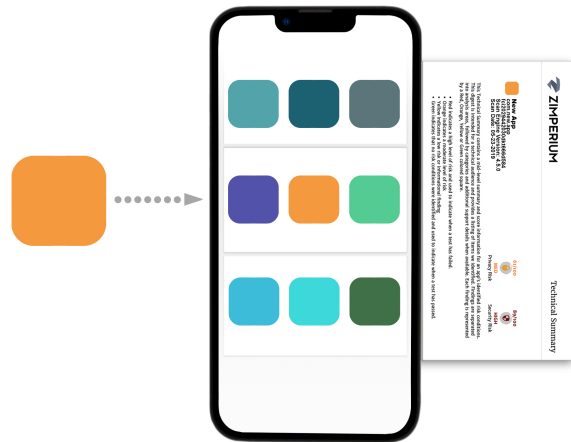
The Number of Mobile Threats is Increasing

Today, the scope of the mobile app market is massive, with over 218 billion app downloads in 2020 alone. IT and security teams will continue to be under increasing pressure to keep up with the growing number of apps on the market. Currently over half of the smartphones within an enterprise are employee-owned with the ability to access unauthorized apps and resources put enterprise data at risk of exposure. The increase in BYO devices in the enterprise leads to a lack of visibility making it difficult for security teams to track and mitigate mobile device risks.

- At the end of 2020, total app downloads for the year reached over **230 billion**.
- By 2023, annual revenue from mobile apps is predicted to reach **\$935 billion**.
- In 2021, **23%** of devices worldwide were exposed to a malicious app and **14%** of iOS and Android apps distributed globally had misconfigurations that exposed users' personal information.

Understanding and managing the risk that mobile apps pose to the enterprise has never been more important.

Zimperium z3A



Security and Privacy Risk Identification with Unprecedented Granularity

Zimperium z3A continually evaluates the risks posed by mobile apps that employees have downloaded to their devices. z3A shows you which apps on a mobile device are safe or risky. For all apps, z3A provides deep intelligence about app behavior with unprecedented granularity, including content (the app code itself), intent (the app's behavior), and context (the domain, certificates, shared code, network communications, and other data). z3A also provides privacy and security ratings, making it easy for you to set effective security policies in to reduce an app's risk.

Automated, Ongoing Detection of Security and Privacy Risks in Installed Apps

Zimperium z3A maintains continual awareness of the apps on mobile devices throughout your enterprise via a parallel processing engine that continuously collects and correlates data from multiple sources. z3A performs multivariate tests and validations to identify mobile app security and privacy risks before they become threats. The z3A engine constantly updates for new threats and the latest app risk behaviors.

The automation and analysis allow you to generate app security and privacy risk summary reports. The reports include app risk scoring giving apps a 'Thumbs Up' or 'Thumbs Down', and details the app behaviors and context so that enterprise security teams can take action. Detailed technical journals in JSON help security teams further understand the Command and Control communications of malicious and risky apps.

Risk Mitigation Actions

Security administrators can set proactive app policies to mitigate app risks and reduce data exfiltration. Policies and risk mitigation are customizable so enterprises can tailor actions according to their risk tolerance. For example, you can restrict user access/privileges if users have installed risky apps on their devices based on criteria defined by you as an administrator. For example, some customers wish to restrict the use of applications that read SMS messages, use self-signed certificates, and send sensitive information about the device over insecure communication channels or to unapproved cloud services. Application risk policies can be crafted to fit specific requirements, with over 100 application characteristics that can be used to create policies. This is powered by z3a's deep insight into application behavior and risks. z3A also allows for risk mitigation through customizable automated actions, such as sending an SMS when a risky app is discovered. Enterprises can also create distinct policies for different groups pulled from the enterprise's MDM solution.

Get Started Today

See how Zimperium z3A can help you manage mobile vulnerabilities across your enterprise.
[Contact us](#) to get a free enterprise trial today.

