Stop Mobile App Threats Before They Impact Your Business

Highlights

- Ongoing Enterprise Mobile Risk Vulnerability Assessment
- Identification and Analysis of Risky Apps Before They Become a Threat
- Real-Time Correlation of App Risk and Device Analysis

Employee use of mobile devices in the enterprise is at an all-time high. There are millions of apps to choose from, and app use is exploding. According to IDC, "mobile device users installed nearly 156 billion mobile applications worldwide in 2015."[1]

Mobile enterprises adopt these apps for competitive advantage, in order to improve business processes, enable employees, partners and customers, and generate revenue. The result, however, is a potentially wider attack surface for cybercriminals and increased risk for the enterprise.

More Mobile Apps, More Risks…

According to a 2016 Netskope report, the fourth quarter of 2015 saw the highest number of cloud apps in use across all enterprises to-date. Employees used, on average, 917 different cloud apps within a given enterprise organization, a 21 percent increase from the previous report. What's more, unsanctioned apps represent the majority of an enterprise's total cloud app footprint at 95 percent.[2]

The June 2016 Netskope report indicates that 11 percent of enterprises have detected malware in their sanctioned cloud apps including mobile malware, spy- and adware. Since unsanctioned apps represent the majority of an enterprise's total cloud app footprint, however, these findings indicate that IT may have an even larger scope of cloud app-based malware in enterprises than initially realized.

> *"82 percent of survey respondents say mobile apps in the workplace has very significantly (50 percent) or significantly (32 percent) Increased security risks"*
>
> Ponemon, The State of Mobile Application Insecurity Study, Feb. 2015

A Ponemon Study found that sixty-five percent of respondents strongly agree or agree that the security of mobile apps is sometimes put at risk because of customer demand or need. The "rush to release" phenomenon challenges an organization's ability to stop the risks of data leakage and malware.

---

[1] IDC Press Release: Mobile App Revenue Outlook Remains Healthy Despite Slowing Download Volumes and Smartphone Growth, According to IDC, 09 May 2016.
[2] Netskope Worldwide Cloud Reports, February 2016 and June 2016.

Mobile apps, in particular, are prone to risky behaviors and surreptitious actions that are often overlooked. This is often due to accidental inclusion of poor coding practice exposing the app to attacks directly, or unsecure collection and handling of personal data.

Performing application risk assessments requires a specialist skill set that includes not only knowledge of the operating system platform but also the public vulnerabilities that are available for any included libraries or code. Human research of individual applications is challenging and a slow process that can take weeks or even months. Apps are often updated during this period, and require restarting the analysis.

These significant skill and scalability challenges call for an automated way of collecting, analyzing and remediating mobile app risks before they become a threat to the business and a breach occurs.

The Business Case for Mobile App Risk Analysis:

According to a survey of 882 respondents from a LinkedIn Information Security community, 72% of organizations say data leakage / loss is the main security concern related to BYOD / Mobile.[3] Loss of employee or customer privacy or company data through mobile apps can result in:

- Brand image deterioration
- Damage to customer trust and retention
- User experience damage
- Unauthorized access and fraud
- Confidential data theft
- Privacy-related data theft
- Revenue loss from piracy
- Intellectual property theft

Business use cases:

- **App Visibility** for understanding an enterprise's mobile app risk posture through a view of the risky apps in the enterprise and the number of users who have risky apps on their devices
- **Actionable Intelligence** for setting app usage policies that whitelist safe apps and blacklist risky non-mission critical apps
- **Security Analysis** of newly developed apps for employees, customers or partners, or that are mandated by business units

Zimperium: a Proven Platform for Enterprise Mobile Protection

Zimperium Mobile Threat Protection is a suite of enterprise security products specifically designed for the mobile environment. It delivers continuous and real-time threat protection to both devices and applications—from a single platform. It provides Security Administrators with a vulnerability assessment of their entire enterprise mobile risk posture so that they can decide which devices can be entitled and which need to be updated to reduce risk.

zIPS is the world's first mobile intrusion prevention system app that protects mobile devices against device, network and application cyberattacks. Its continuous, on-device z9 detection engine uses machine learning to dynamically detect known and unknown threats in real time.

[3] BYOD & Mobile Security 2016 Spotlight Report, by Crowd Research Partners.

It is designed to run efficiently on devices, such as smartphones and tablets, and enables Security Administrators to manage the health of every device running the zIPS app without compromising the user experience or privacy.

- Detects exploits by analyzing deviations to mobile device behavior to identify the specific type of attack
- Identifies and mitigates zero-day attacks
- Prevents a compromised device from gaining access to the corporate network

Expanding Risk Assessment through Comprehensive Mobile App Analysis

Zimperium's z3A Advanced App Analysis provides risk assessment capabilities to its continuous and real-time Mobile Threat Protection solution. It identifies risky apps before they become a threat. Advanced App Analysis provides comprehensive mobile app risk intelligence, including privacy and security ratings along with contextual analysis, for each risky app identified. Arming security teams with this detailed insight can help them set policies to reduce company data exfiltration risks and prevent breaches before they happen.

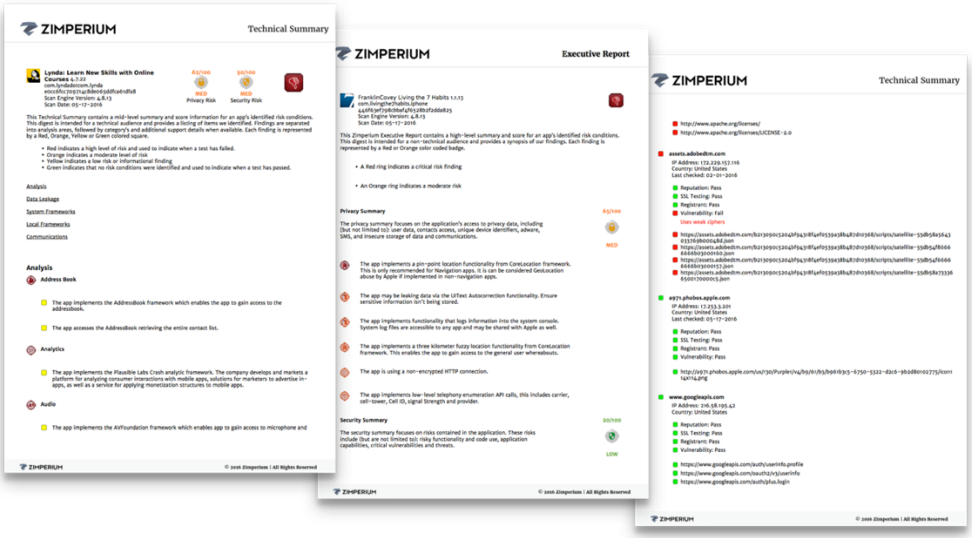
Unlike standalone app risk or app reputation solutions, Zimperium's Advanced App Analysis capability uniquely correlates app risk analysis with its device analysis. It delivers a holistic view of the risk posture of the device covering operating system exploitation, network attacks and apps from malware, security risk and privacy perspectives.

Leverage the Power of Data

z3A Advanced App Analysis provides Security Administrators with deep insights so they can determine which apps in use in their enterprises are safe or risky. At the heart of its purpose-built, fully-automated and cloud-based mobile risk assessment platform, is a parallel processing engine that continuously collects intelligence from multiple sources applying multivariate tests and validation to identify security and privacy risks in mobile apps before they become threats. The engine uses a comprehensive array of processes running asynchronously in parallel to produce deep and accurate investigation and analysis.

Analysis	Intelligence Collection	Tests/Validation
Dynamic Analysis (D.A.S.T.)	Registrant History	OWASP Mobile Top 10
Static Analysis (S.A.S.T.)	Communications	Chain of Trust
Cross Application Correlation	URL Reputation	SSL Certificate Validation
3rd Party Code inspection and identification	Data Leakage	Vulnerabilities
Payload Inspection	Privacy Violations	Certificate Pinning
Various Threat Engines	Security Violations	Repacking Detection
	Distribution Footprint	Developer Reputation

z3A gathers everything from malware to data manipulation instances, providing detailed quantitative and qualitative results to match the specific needs of any enterprise for app security and privacy risk analysis. Customers benefit from a vast and large database of dynamically updated app knowledge. As an autonomic computing engine, z3A's parallel processing engine is self-learning. It continuously builds upon its intelligence base, adapting to change and reassesses apps to determine if their risk posture has changed.



z3A App Risk Reporting

Deep App Analysis in Minutes

z3A Advanced App Analysis lets Security Administrators know what each and every app is doing. Its deep app analysis provides them with insight into:

- *Content:* The app code itself
- *Intent:* The app's behavior
- *Context:* The domains, certificates, shared code, network communications

z3A doesn't just stop at static code analysis. It also performs dynamic analysis, running the app in a virtual machine, so that it can compare how the app actually behaves for increased accuracy. Using machine learning and artificial intelligence, Zimperium's Advanced App Analysis correlates its findings in a vast and multivariate database to predict an app's activities and provide security teams with clear actionable intelligence.

App Security and Privacy Risk Summary Reports include app risk scoring, giving apps a Thumbs Up or Down, as well as the app behaviors and context so enterprise security teams can take action. Detailed technical journals in JSON help security teams further understand the Command & Control communications of malicious apps.

These reports are near real-time and generated in minutes, saving application testers six to eight hours of research time. Reports can be generated for an initial app inventory risk assessment when a device is activated for zIPS and thereafter as apps are installed and updated.

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, user access/privileges can be restricted if risky apps are installed on their devices.

z3A also allows for risk mitigation through customizable automated actions, such as sending an SMS when a risky app is discovered.

Why Zimperium?

Zimperium provides the first mobile threat management platform that delivers continuous and real-time cyberthreat protection to **both** mobile devices and applications:

- *Continuous* on-device monitoring and detection of known and unknown mobile cyberattacks in real time.
- *Comprehensive* visibility across all mobile devices to assess enterprise risks, identify security gaps, and update policies to adapt and improve mobile device and application protection.
- *Complete* management with configurable end-user and admin notifications, and automated policy action recommendations.

ZIMPERIUM

Zimperium is a leading enterprise mobile threat protection provider. Only the Zimperium platform delivers continuous and real-time threat protection to both devices and applications. Through its disruptive, on-device detection engine that uses patented, machine learning algorithms, Zimperium generates “self-protecting” apps and protects against the broadest array of mobile attacks.

CONTACT US

101 Mission Street
San Francisco, CA 94105
Main: (1) 844.601.6760
info@zimperium.com

www.zimperium.com