Ensuring User Privacy While Enabling A Safe Bring Your Own Mobile Device Strategy

MTD™

ZIMPERIUM®

More enterprises are realizing that a bring-your-own-device (BYOD) policy has many benefits including lowering operating costs, improving employee productivity, and allowing workers the comfort and convenience of using their own personal devices. Permitting use of BYOD in today's workplace presents the security team with the solvable challenge of employee concerns about the privacy of their personal data and device use vs the reduced cost and benefits provided by an employee owned device. User acceptance and confidence in the protection of their personal activity and identity, as well as adherence to privacy regulations, is imperative to a successful adoption of mobile security in a BYOD environment.

It is common for security teams to implement a solution to protect an employer-provided mobile device from attacks and limit application use to trusted applications only. However, mobile access via BYOD can also be implemented that secures access to corporate resources and data while addressing employee privacy concerns. This is accomplished by implementing a mobile security solution built with a privacy-first methodology.

Securing the Device:
Zimperium MTD is a Privacy-focused Security Solution

Zimperium can easily be configured so that no personal information or data is collected without compromising mobile device security. Zimperium protects against known and zero-day threats, protecting the workforce from malware, mishing (mobile-targeted phishing), network, and app vulnerabilities. Configuring Zimperium for privacy is accomplished by administrative settings, user settings and compliance with *GDPR Right to be Forgotten* requirements.

Managing the Device:
EMM or non EMM Managed

Organizations have the choice to implement a BYOD strategy via either a managed (EMM/MDM) process or an unmanaged approach. In both use cases, mobile threat defense (MTD) can be deployed to secure the devices and data without compromising employee privacy. If an Enterprise Mobility Management (EMM) approach is employed, Zimperium MTD provides integration for ease of management; however, user name and email information is easily configured to not be collected or stored by MTD based upon customer requirements.

Administrative Privacy Settings

Administrators set privacy policies based on corporate standards such as protecting BYOD user privacy.

Figure 1 shows the configuration screen for privacy policies. These settings control what data in these areas are transmitted to the Zimperium console. Granular policy can be set for Location, Application, Network and Device data. These policies can be global or by policy group. ***A policy group can be created for BYOD users so that their information never leaves their device.*** This means that neither Zimperium nor the administrator ever see the information as it is never transmitted from the user's device.

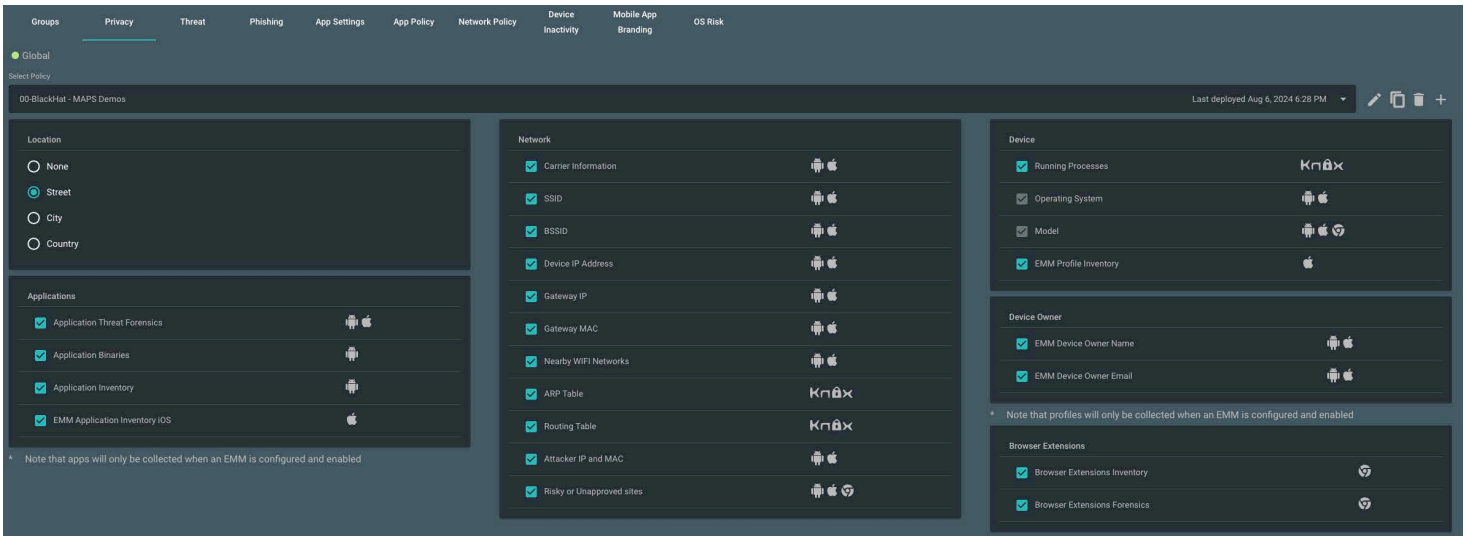


Figure 1

User Privacy Settings

The end user and the administrators may each adjust policies of the MTD app that determines what data that they will allow to leave the device. See Figure 2 where the displayed privacy summary screen is dynamically updated based on the configured policy settings. Some personal data, however, is never collected from the device, regardless of policy including:

- Personal emails, documents, contacts, or calendar
- Passwords
- Pictures and videos

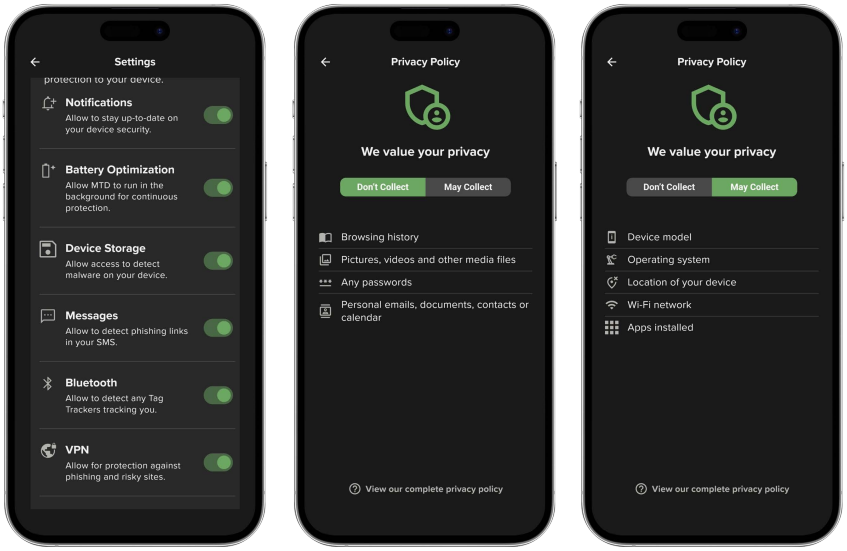


Figure 2

User Data and Rights

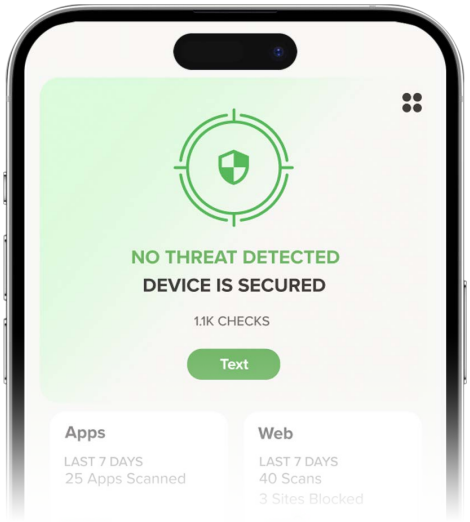
If a user's data is stored and the user decides later to have it deleted, Zimperium fully supports the GDPR right to be forgotten. The Zimperium EULA documents how we handle data and privacy. See **www.zimperium.com/zimperium-eula** for more information, in particular in Sections 6 and 7 of the EULA.

In summary, implementing a privacy-first mobile security strategy in a BYOD environment is critical to ensure the security of corporate applications and data, but providing users with the confidence that their personal data, identity and device usage is kept absolutely private is an essential component for a successful implementation.

About Zimperium

Zimperium is the world leader in mobile security for iOS, Android, and ChromeOS. Zimperium solutions, including Mobile Threat Defense (MTD) and Mobile Application Protection Suite (MAPS), offer comprehensive mobile security for enterprises. MTD is a privacy-first application that provides mobile risk assessments, insights into application vulnerabilities, and robust threat protection. It is used to secure both corporate-owned and bring-your-own devices (BYOD) against advanced mobile threats across device, network, phishing, app risks, and malware vectors. MAPS delivers automated security testing and in-app protection to safeguard applications from attacks and ensure data integrity. Together, these solutions empower security teams to effectively manage and mitigate mobile threats.

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