

# Securing **BYOD** in a Mobile-First Threat Landscape



As cybercriminals move to a “mobile first” attack strategy, attackers do not discriminate between corporate provided mobile devices and those owned by employees themselves. Given this risk, organizations must define and implement clear BYO Mobile security policies to ensure proper protection. BYO Mobile, a subset of BYOD policies, introduces unique security challenges that organizations must address because everyone is a target. Employee-owned devices pose additional risks due to the lack of standardized security controls.

Regardless of whether mobile devices are BYOD or corporate provided, 50% of devices are running out of date operating systems,<sup>1</sup> so they face the same threats and require the same risk posture visibility. If an organization is implementing a zero trust approach to cybersecurity, the scope must extend beyond traditional desktops and laptops to encompass mobile devices, which often have the same access to enterprise data and networks.

With mobile device adoption increasing in the workspace to 82% of organizations,<sup>2</sup> existing security infrastructure often falls short in providing adequate mobile protection. Over time, misinformation and a false sense of security have compounded these challenges. As a result, security breaches across many industries continue to expose the weaknesses in current mobile security practices, underscoring the need for robust and proactive defenses.

As organizations embrace mobile access, IT policymakers must carefully evaluate their strategy for enabling secure mobile access to business apps and networks. They must consider several critical questions:

- **How many mobile devices do I have accessing my corporate data?**
- **What are the tradeoffs between a corporate owned, BYO and hybrid mobile device strategy?**
- **What visibility do I have into the data and network risks posed by these devices?**
- **How will I protect against attacks like mishing (mobile-targeted phishing) & malware on our user’s mobile devices?**
- **How can I assess the security and privacy risks posed by the personal apps my employees have downloaded on their mobile devices?**
- **How can I incorporate device trust signals into my zero trust strategy implementation?**
- **How can I detect and respond to devices that have been compromised?**
- **How am I integrating mobile threat data into our security reporting systems and processes to ensure compliance and security?**
- **Do I have a zero trust strategy in place? If so, how will I meet zero trust requirements when enabling mobile access?**

## Use Cases for Mobile Access

Organizations have to decide on their mobile strategy based on business needs. The following questions need to be answered:

- What are the applications that employees need to access from mobile devices?
  - Email (Outlook, GMail, etc.)?
  - Business communications and meeting apps (Teams, Webex, Zoom, Google Meet, Slack, etc.)?
  - MFA apps to support Zero Trust strategy to access applications on their corporate desktop/laptop devices?
  - Commercial cloud based business applications (CRM (Salesforce, etc.), Financial (Netsuite, etc.)?)
  - Corporate apps that we developed for our business?

Overlay the answer to these questions with the answer to the following question:

- Do we wish to allow employees to access their personal email and personal apps (social media, banking, news, etc.) on the same device used to access business apps?

If the answer to this question is “no”, then providing employees who need the business application access with a corporate owned and provided device is your only choice, since employees are highly unlikely to let you shut down use of their personal device for purely business use.

If the answer is “yes” then BYOD may be an option. There are benefits and risks to permitting BYO mobile use.








### In this paper, you'll learn:

- **To determine the use cases for mobile access to corporate data** and how those use cases can threaten your business if not addressed.
- **The tradeoffs between corporate owned and BYOD device use**
- **The costs** for both approaches
- **Impact of BYOD on a zero trust strategy**



## Benefits of enabling BYOD

-  **Cost savings**  
Companies don't need to purchase expensive devices for employees.
-  **Increased productivity**  
Employees are more productive because they're using devices they're familiar with. Employees have increased access to data and apps from anywhere and any device. Users don't have to juggle two devices (work and personal).
-  **Increased employee satisfaction**  
Employees are happier with their choices and have more flexibility. They see their employer as progressive in embracing technology. Employees can use their preferred mobile platform.
-  **Increased workforce mobility**  
Employees have more mobility, which can improve their satisfaction and productivity.
-  **Reduced IT burden**  
There's less need to manage company-owned devices.
-  **Reduced training**  
Employees use tools they already know, so they require less training.

## Risks from unsecured BYOD Access

- Mobile devices, including BYOD, significantly expand the attack surface, making mobile a primary target for hackers, especially since they are often unsecured
- Data breach: unauthorized access to apps and data due to lack of device policy control
- Sensitive data loss by insider (intentional or unintentional)
- Expands attack surface to techniques used in Mishing - Vishing (voice call), Smishing (sms/text), Quishing (camera/QR codes)
- Exposes organization to risks from risky Wi-Fi usage
- Risk from insufficient access controls
- Risk of mixing of personal and corporate data
- Lack of device visibility, access control and security
- Challenges in maintaining regulatory compliance and reporting
- Determining whether a device is running out of date OS, which may include vulnerabilities
- Apps on the device containing malware or are compromised, or violate policy on data communications, permissions, etc.

## Tradeoffs for Corporate owned and BYO Mobile Strategies

Tradeoffs exist between both strategies. These tradeoffs include costs, threat exposure, employee privacy concerns and compatibility with implementing a zero trust strategy.

### Cost

Organizations often are attracted to a BYOD strategy on the assumption that it will be much cheaper than purchasing and deploying corporate owned devices. The cost savings are not always as much as one might expect.

Costs for Corporate owned devices typically consist of <sup>3</sup>

- Average Monthly line service: \$65
- Damage insurance \$15
- Device cost: \$20 (\$720 device over 36 months)

This totals \$100 per month. But implementing BYOD does not necessarily result in a per employee savings of this monthly sum. Industry, geographic location, employee status and competitive pressures can cause these savings to shrink. For example:

- In what industry and what parts of the world do my employees operate?
  - Regulations in financial services in the U.S. UK, EU, and Japan, to name a few, severely restrict BYO mobile device use.<sup>4</sup>
- Which employees need to have access to corporate applications and data from a mobile device and are they exempt or non exempt workers? If non-exempt, can I legally ask them to spend their own money or use their own devices for work use?
- Will I need to reimburse the employee for use of their personal mobile device? The choice to reimburse is influenced by factors such as what your competitors' policy is, and whether the organization wants BYOD to be seen as a benefit which may be taxable to the employee. Typical reimbursements cover:
  - Monthly cell service or some portion of it
  - Partial stipend, reimbursement or allowance (SRA) for the device purchase and insurance

Depending on the answers to these questions, savings from BYOD policies can shrink substantially.





## Threat Exposure

Mobile devices are exposed to threats regardless of whether BYOD or corporate owned. Threats exist from multiple vectors, including the devices themselves, from networks, as well as mishing and the apps loaded onto the device.



### Device Threats

Unpatched device operating systems with CVEs present vulnerabilities that can be exploited by hackers. The Zimperium Global Mobile Threat Report<sup>5</sup> found that 14% of Android devices cannot receive an OS upgrade, leaving critical vulnerabilities open to exploitation. In addition, 80% of iOS versions were actively exploited in 2023. Hence, organizations permitting BYOD need to know if user owned devices are still operating on OS versions with known vulnerabilities.



### Network Threats

It is quite common for users to connect to public wifi hotspots and they do so with unwarranted trust that the network connection is safe. Zimperium researchers found that the number of devices connecting to unsecured networks increased by 45% in 2023,<sup>6</sup> potentially exposing them to man-in-the-middle attacks, which can steal confidential data, including login credentials.



### Mishing Threats

Cybercriminals have adopted a mobile-first attack strategy, as they have found mobile to be a much easier vector (compared to laptops/desktops) for executing social engineering upon users. This ease is the result of one or more of the following: lack of security vigilance by users, most devices lacking threat detection, and the unique features of a mobile device that provide additional methods of attack (text, QR codes, etc.). Zimperium research has identified multiple sophisticated email phishing campaigns that only execute when activated from a mobile device. In fact, 83% of phishing attacks are targeted at mobile devices.



### App Threats

Unless a device is corporate owned and limited solely to corporate provided apps needed to support the business, users of BYOD expect to download and use personal apps in categories like social media, finance, entertainment and more. But most personal apps (as well as many business apps) are not designed with security in mind. 85% of apps on a phone are personal apps that can increase enterprise security risk exposure.<sup>7</sup>

## Employee Privacy

Employee owned devices naturally contain personal and confidential information: geo location info, photos, documents, browsing history, personal email and messaging, social media app data, network connection information, etc. Employees are naturally very concerned about this information being shared with their employer. Hence employers who chose to permit BYOD must communicate and implement policies and technology to not only secure corporate data and the devices used to access them but do so in a way that prioritizes employee privacy regulations and expectations.

## Zero Trust

Lastly, BYO mobile devices are impacted if the organization is pursuing a zero trust security strategy.

Zero trust requires secure resource (ie. data and apps) access that leverages:

- Device health attestation
- Data level protections
- Identity and access management
- Network segmentation

Hence, permitting BYO mobile device access as part of an enterprise zero trust initiative requires that the organization address the device, network and application challenges outlined here. Furthermore, a zero trust strategy often leverages identity and access management by utilizing two factor authentication.

A new threat known as SMS Stealer,<sup>8</sup> recently identified by Zimperium's zLabs, compromises the SMS text feature of mobile devices in order to execute account takeovers and credential theft. This threatens not only personal data but compromises the success of the zero trust initiative.

As NIST states,<sup>9</sup> Mobile Threat Defense (MTD) is core to permitting a BYOD platform. Without an advanced, on-device MTD, you cannot attest to having device integrity and declare a Zero-Trust environment.



## Enabling Secure BYOD

### *So how do you enable secure BYOD?*

The most common area of adoption for mobile device support has been around mobile device management (MDM) toolsets (also referred to as EMM – enterprise mobility management), enabling IT and security administrators to enforce base-level policies of access and control on both owned and BYOD assets. It is common to refer to what EMM does as “lock it, wipe it, track it”. EMMs can track that a device’s security access code is enabled, encryption is on, and that it is not jailbroken. If any of those are violated, it can be remotely locked or even wiped (for example if stolen).

From a security perspective, most MDM’s provide some rudimentary jailbreak/root detections based on known signatures at infrequently timed (6–12 hours) intervals. *But these checks are very basic and cannot detect or protect against the most common types of attacks such as phishing, malware protection, application or wifi analysis, much less zero-day exploits, that are deployed by the sophisticated attackers we are seeing today.*

And when it comes to supporting BYOD policies, MDM/EMM solutions are often viewed as invasive to the personal device, taking the control out of the owner’s hands and placing it with an administrator. With the ability to scan personal messages, view photos, and access other personal, non-essential information, as well as wipe the phone with no warning, these management solutions may represent overreach in consideration of some privacy regulations and can leave users feeling uneasy or worse.

**Simply put, MDM/EMM enforces and manages settings on the mobile device but provides little in the terms of detections or analysis for threats and risks, and all at the expense of user data privacy and control.**

## Securing the BYO Device with Zimperium MTD

Organizations have the choice to implement a BYOD strategy via either a managed (EMM/MDM) process or an unmanaged approach.



In both use cases, a mobile threat defense (MTD) solution that has been developed to be “privacy first” can provide needed security while addressing privacy concerns of the device owner. *Zimperium is a privacy first focused security solution that fully addresses device owner privacy concerns.*

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.

**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, 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.

## BYOD Privacy with Zimperium

### Administrative Privacy Settings

- Administrators set privacy policies based on corporate standards such as protecting BYOD user privacy.
- 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, yet the device and the user remain protected.

### User Privacy Settings

The end user and the administrators may each adjust policies of the MTD app that determines what data that they will permit to leave the device. Some personal data, however, is never collected from the device, regardless of policy including:

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

## 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.<sup>10</sup>

## Conclusion

Implementing a privacy-first mobile security strategy in a BYOD environment is achievable and critical to ensure the security of corporate applications and data. Zero trust frameworks play a key role in securing BYOD access by enforcing strict access controls and continuous verification of devices and users. A mobile security solution designed to respect user privacy while providing strong security protections is essential for a successful BYOD strategy.

---

## Sources

- 1 Zimperium 2024 Global Mobile Threat Report
- 2 Zimperium 2024 Global Mobile Threat Report
- 3 "When and How to Allow Mobile BYOD," 6 March 2024, ID G00796686, Gartner, Inc. <https://www.gartner.com/document-reader/document/5253063?ref=hp-wylo>
- 4 "When and How to Allow Mobile BYOD," 6 March 2024, ID G00796686, Gartner, Inc. <https://www.gartner.com/document-reader/document/5253063?ref=hp-wylo>
- 5 Zimperium 2024 Global Mobile Threat Report
- 6 *ibid*
- 7 *ibid*
- 8 <https://www.zimperium.com/blog/unmasking-the-sms-stealer-targeting-several-countries-with-deceptive-apps/>
- 9 NIST SP 1800-22, "Mobile Device Security: Bring Your Own Device (BYOD)"
- 10 [www.zimperium.com/zimperium-eula](http://www.zimperium.com/zimperium-eula), in particular in Sections 6 and 7 of the EULA.

## 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. Learn more at [www.zimperium.com](http://www.zimperium.com) and connect on LinkedIn and X (@Zimperium).

[www.zimperium.com](http://www.zimperium.com)



Learn more at: [zimperium.com](http://zimperium.com)  
Contact us at: 844.601.6760 | [info@zimperium.com](mailto:info@zimperium.com)  
Zimperium, Inc  
4055 Valley View, Dallas, TX 75244

© 2025 Zimperium, Inc. All rights reserved.