ZIMPERIUM®

How to Implement Mobile BYOD in a Zero Trust Environment

The perimeter-based network security model that defined users inside a corporate network perimeter as "trusted" no longer provides the same level of security as it did in the past. Today, cloud computing, mobility, and remote work change how people connect to digital resources. As part of these new models, employees increasingly want to use their own devices, making Bring Your Own Device (BYOD) policies even more critical to security. Implementing a zero trust architecture in a BYOD environment should incorporate mobile threat defense to augment the security technology stack.

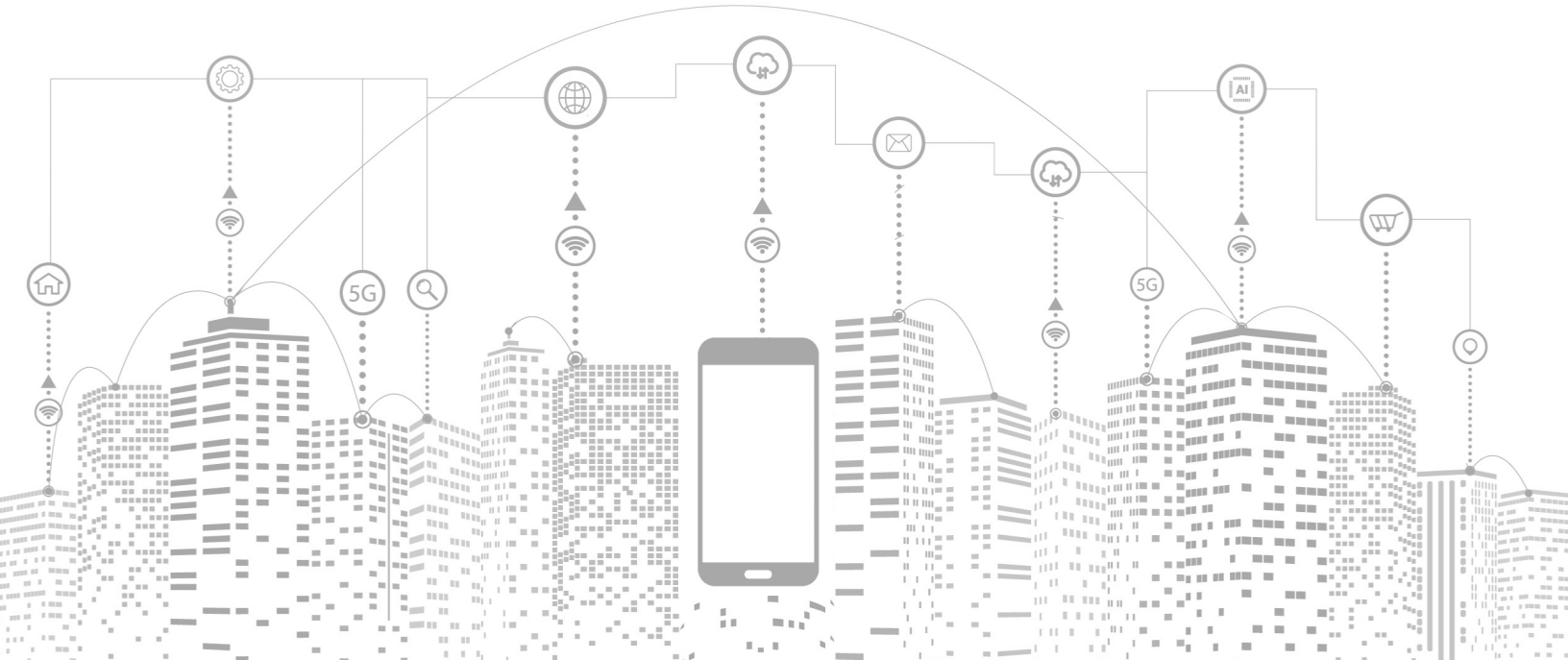
Why Zero Trust?

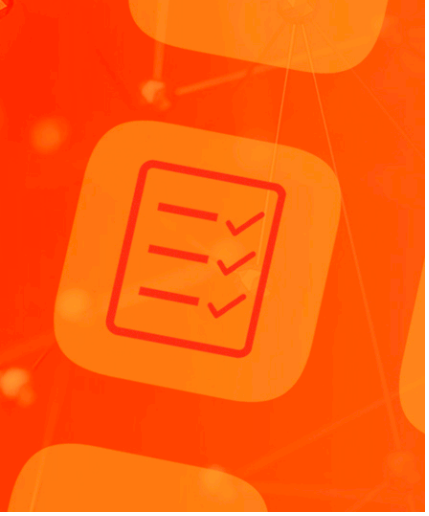
New technologies and workforce models change the way that organizations need to approach security. For example, an inherent trust exists when all users and devices connect to protected networks.

Today, people use the public internet - even within protected networks - to access web-based applications to do their jobs. Additionally, third-party business partners, like contractors, use the public internet to meet their obligations.

A Zero Trust approach to security focuses on creating secure resource access that incorporates:

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





Why Zero Trust Compliance is Challenging

At a high level, Zero Trust focuses on six primary pillars:


Users


Device


Network


Application


Automation


Analytics

Meeting Zero Trust compliance can be quite challenging because, within each pillar, an organization needs to secure multiple things. Further, very few step-by-step processes exist for putting a zero trust architecture in place.

For example, within the 'Device' pillar, organizations must ensure continued security for workstations, mobile devices (including tablets and smartphones) and Internet of Things (IoT devices like printers and servers).

Under this pillar, organizations need to manage device security by establishing baseline protections. Additionally, they need visibility into the security going forward, which means enforcing those policies and engaging in continuous device risk attestation.

As part of the compliance monitoring function, it should look like this:

- **Traditional:** Visibility into whether a device complies with the established security policies
- **Advanced:** Ability to enforce compliance for most devices
- **Optimal:** Monitor and validate device security posture in real time

In BYOD environments, many organizations will struggle to get visibility into whether a device complies with established security policies. They may be unable to control what device someone uses or struggle to meet privacy requirements when leveraging a technology to help gain visibility.

Every Organization Should Provide Protection Against These Mobile Device Threats

Continuous device attestation is fundamental to an effective BYOD strategy for meeting Zero Trust security requirements. When building these strategies and initiatives, organizations must consider various threats that can undermine their goals. Employees constantly use their mobile devices, and as they traverse the landscape, they encounter real threats.

Mishing

The increased focus on mishing (mobile phishing) attacks by threat actors is nothing new. According to the APWG, the number of phishing attacks has grown by 150% per year between 2019 and 2022.

According to our 2024 Global Mobile Threat Report, 82% of phishing attacks target mobile devices. Attackers now have a "mobile-first" attack strategy because mobile devices are largely unsecured and attackers know this. Mobile is a large and undefended attack surface.

While most end users never really mean to cause harm, the increased sophistication and barrage of activities make it difficult to sort out the digital wheat from the chaff. Traditional signature-based antivirus or phishing solutions offer a starting point. Still, many of them are reactive in nature and don't adequately address the challenge of the volume of new phishing sites being stood up every second.

In 2023, the Anti-Phishing Working Group reported nearly five million phishing attacks, making it the worst year on record and surpassing the 4.7 million attacks seen in 2022. Zimperium's zLABS threat data aligns with this trend, underlining the increasing sophistication of phishing sites. Notably, there was a 7% increase in phishing content specifically targeting mobile devices. Furthermore 25% of mobile users tapped on at least one phishing link every quarter in 2019.

For example, attackers targeted mobile devices with the following two techniques:

- **Adaptive websites:** Depending on the device used, adaptive websites can load different content and redirect to alternate sites. By adapting content based on the user agent of a mobile endpoint, attackers can exclusively target mobile devices.
- **Responsive websites:** Since these adapt the size and placement of objects based on endpoint screen size, attackers can use these legitimate features to target mobile devices.

Mobile devices offer an additional layer of complexity that makes traditional antivirus and phishing approaches not adequate for mobile. First, connectivity of a device to a cloud, in addition to privacy considerations and latency concerns, makes any cloud-first approach not feasible both from a technical security perspective and operationally as well. Additionally, mobile devices cannot download or support large signature files, so any reliance on known databases, or threat feeds, is inadequate and infeasible.

This means that the only viable options to protect mobile devices must be able to do so on-device without any reliance on the cloud and must be able to detect known and unknown threats without having to have seen them before. Zimperium's detection engine uses AI classifiers to detect known and unknown threats across mishing, device, network and applications, all without reliance on the cloud.

Downloaded Apps

Many organizations already know the risks that shadow IT can cause on traditional devices. However, the inability to add these applications to asset inventories leads to a lack of visibility.

Downloaded apps on mobile devices become even riskier. Workforce members use mobile devices personally and professionally, causing organizations the inability to control the security of the applications they use to manage their personal use.

The convergence of mobile apps/desktop apps into the modern OS is a trend that makes it easier for threat actors to use mobile devices as a backdoor into systems and networks. According to Zimperium's Threat Report data, 42% of companies reported unauthorized apps and resources accessing enterprise data.

Zimperium Mobile Threat Defense (MTD) is dedicated explicitly to threat prevention, detection, and response for devices running iOS, Android, and Chrome OS. While a mobile device management (MDM) solution can help with policy administration and enforcement, Zimperium's MTD shields the organization by compartmentalizing sensitive information and processes, reducing the attack surface.

Malware Inside Downloaded Apps

Since the mobile attack surface differs from the traditional attack surface, mobile malware is also unique. Sometimes, the app is the malware, while other times, attackers use apps to deliver the malware via a vulnerability.

Malicious Apps

In 2024, Zimperium mobile security analysts reported a 13% increase in mobile malware over the previous year and one in four protected devices encountered malware with 80% increase in spyware detections on enterprise owned mobile devices.

While some mobile malware variants act like traditional endpoint attacks, others look and act differently. For example, some may:

- Steal two-factor authentication (2FA) credentials through SMS or app notifications.
- Perform overlay attacks where a user enters credentials into a secondary app that they believe is legitimate.
- Monitor other installed apps through Accessibility Service permissions.
- Use location tracking through GPS services.
- Activate cameras or microphones to record audio and video.
- Access sensitive content like photos, contacts, or personal data.
- Capture and track sensor data.

Risky Apps

As a newer technology, mobile apps may not have the same level of security built into their software development cycle, especially as companies try to push out new experiences quickly.

Our 2024 Global Mobile Threat Report reported that almost 36% of iOS work apps use the keychain in a way that might leak data. In addition, roughly the same percentage of iOS apps (36%) do not check the reason for initiated traffic from the app, therefore risking leakage. On Android, our analysis of the top 50 apps across work categories yielded that a little over 50% of them might store information insecurely on the device.

In other words, even when end users download legitimate apps, they can create risks that impact the organization. With mobile app development security still in its nascent state, companies need to consider how they protect themselves from these risks.

Network Attacks

Work-from-anywhere means that employees are connecting to insecure Wi-Fi networks. While this is not new, man-in-the-middle (MITM) attacks remain effective, with Zimperium's research finding that 13% of devices encountered MITM attacks.

Equally problematic, previously "protected" Wi-Fi networks can be undermined through evil twin attacks where malicious actors spoof a free Wi-Fi network that uses a portal for entry, like at a hotel or airport. Based on Zimperium's research, around 16% of mobile devices encountered either a known malicious network, traffic manipulation, or a rogue access point. That being said, end users who previously connected to the real Wi-Fi network are more likely to trust that it's secure. However, when the user logs into the company's portal via this fake Wi-Fi network, the malicious actors can steal their credentials.

With Zimperium, organizations can enforce conditional access requirements when people change their location because the device's "condition" is continuously monitored. With Zimperium's MTD solution, the company has visibility into device security and can more appropriately deny access from a rogue WiFi connection.

Charging Stations

When organizations consider mobile risks, they often worry about phishing the most. However, focusing solely on phishing fails to consider other malware delivery methods.

Recently, the FCC warned consumers that public USB charging stations, like those in malls and airports, were being exploited by cybercriminals. This attack type, known as "juice jacking," can be executed through the USB port or a cable left by the cybercriminals. When users plug their phones in, the malware can lock a device or export credentials.

Traditionally MTD is an on-device security implementation to understand a user's device's risk. The threat posture then provides the attestation needed to determine whether a company should trust that device. Even as cybercriminals evolve their methodologies, an MTD solution offers the device attestation necessary for implementing Zero Trust strategies for BYOD.

Preventing Mobile Device Compromise is Fundamental to Zero Trust Architectures

If mobile devices fail to meet an organization's security requirements, they undermine its Zero Trust policies. According to Zimperium's research, 7 out of 10 organizations consider mobile devices to be critical to their operations. However, employees use personal mobile devices to access everything from customer lists and account strategies to financial models. As these access and store sensitive information, a compromised mobile device can lead to a data breach.

Further, these devices are often the organization's primary means of implementing multi-factor authentication via SMS or a 2FA app. As a result, a compromised mobile device may be used as part of a larger attack against the organization, leveraging the user's credentials, intercepting the 2FA, and gaining access that enables lateral movement.

In short, a compromised mobile device can undermine Zero Trust's device and identity pillars.

Improving BYOD Mobile Device Security for Implementing Zero Trust Architecture

Incorporating BYOD into a Zero Trust architecture poses many challenges. While BYOD provides employees with greater flexibility, it also creates new security risks. Organizations need to include MTD as part of their Zero Trust strategies to improve BYOD security.

Zimperium's MTD is an advanced mobile threat defense solution for enterprises, providing persistent, on-device protection to both corporate-owned and BYOD devices. Zimperium MTD's on-device security gives organizations the mobile device integrity attestation necessary for a complete approach to Zero Trust. Additionally, by design, Zimperium MTD protects end-user privacy, ensuring that organizations comply with Zero Trust Architecture (ZTA) and privacy mandates.

To see a demo and learn more about protecting your organization from mobile threats, visit www.zimperium.com/contact-us/.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244