ZIMPERIUM®

Management Is Not Security

Why Mobile Threat Defense Has Become Essential to Cybersecurity Strategy

Several years ago, checking your company email from a personal device might have been frowned upon by your employer. However, the use of personal devices at work has now become standard in an enterprise organization. **According to Zimperium's 2022 Global Mobile Threat Report, 66% of mobile phones used at work are employee-owned.**

The COVID-19 pandemic and remote work are partly responsible for this shift. For example, employees use productivity apps like Office 365, G Suite, JIRA, Okta, and Salesforce from their personal devices, even if they're in the office and not just working from home. And both personal and corporate-owned devices are routinely used for multi-factor authentication (MFA), exposing even non-mobile access to corporate data.

The use of personal devices at work boosts employees' productivity. However, it also blurs the lines between devices and data, presenting cyber criminals with a treasure trove of enterprise information ripe for stealing. As a result, adversaries are evolving their tactics and leveraging multiple channels to carry out phishing attacks, with mobile being the new backdoor.

Mobile devices are directly connected to an individual's identity. These devices are used to verify an individual's identity to gain access to work data outside of the traditional office perimeter. Adversaries target mobile device users because they provide more access to an enterprise's data than ever and are much less protected than traditional endpoints. **Legacy security and management controls, such as Mobile Device Management (MDM), fall short whenever it comes to effectively detecting and resolving advanced threats. As the name implies, MDMs only manage a device.** More proactive mobile security tools, like Mobile Threat Defense (MTD), are necessary to protect your enterprise from both adversaries and your employees themselves.

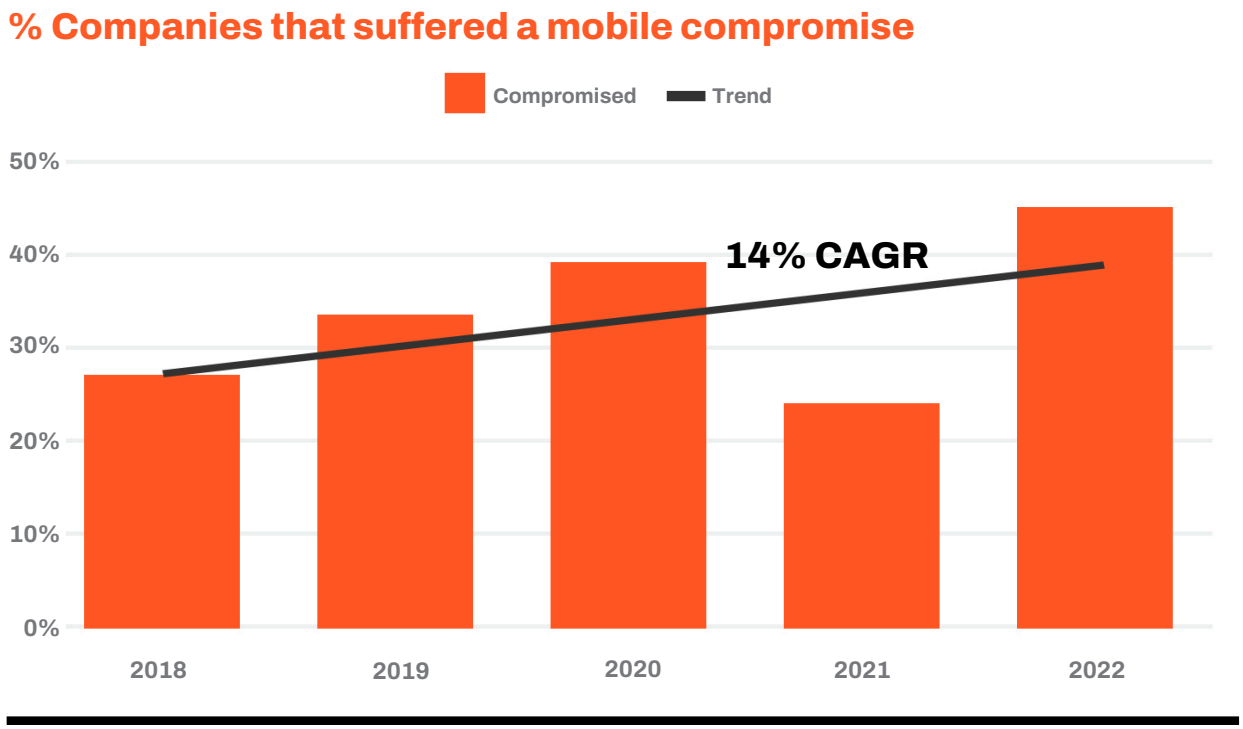


Figure 1. Percentage of respondents that admitted their company suffered a compromise that involved a mobile device and led to the loss of data or downtime. [n=601, 671, 876, 856, 632]

(Source: The Verizon Mobile Security Index 2022)

The Impact of BYOD

BYOD has changed dramatically just in the last couple of years alone. Before the COVID-19 pandemic, 60% of businesses reported that they did not have a BYOD policy in place. While that has changed, there are still a significant number of organizations that do not have a BYOD policy; almost 30%, according to our 2022 Global Mobile Threat Report.

In reviewing the mobile device population in an enterprise environment, it was surprising that many of these devices that access corporate information either on email, apps, or other communication channels are not protected with a comprehensive mobile security solution. Devices managed by an MDM have an agent that controls a mobile device and has the ability to erase a mobile device if it is out of compliance, which leaves many employees unwilling to comply with managed device policies. **Zimperium learned that, on average, 66% of smartphones connected to the enterprise are unmanaged, and 5% of respondents aren't sure if their devices are managed at all.**

A fair amount of space on the average phone is dedicated to working: 10% of the applications installed on the mobile device are work-related. **Given that the average phone has between 100 and 120 apps installed, this means about 10 to 12 work applications are living on your employees' phones.**

Suppose those devices aren't being monitored and protected in some way. In that case, sensitive corporate data or credentials can be intercepted by mobile trojans, man-in-the-middle (MiTM) network attacks, or worse: ransomware, phishing tactics, and even malicious apps. In fact, most users probably won't know they have these threats on their mobile devices until it's too late. The stakes are high: the average cost of a data breach was $4.24 million in 2021. The breaches that occurred due to remote work were even more expensive—about $1.07 million higher.

How Threat Actors Exploit the Expanded Attack Surface

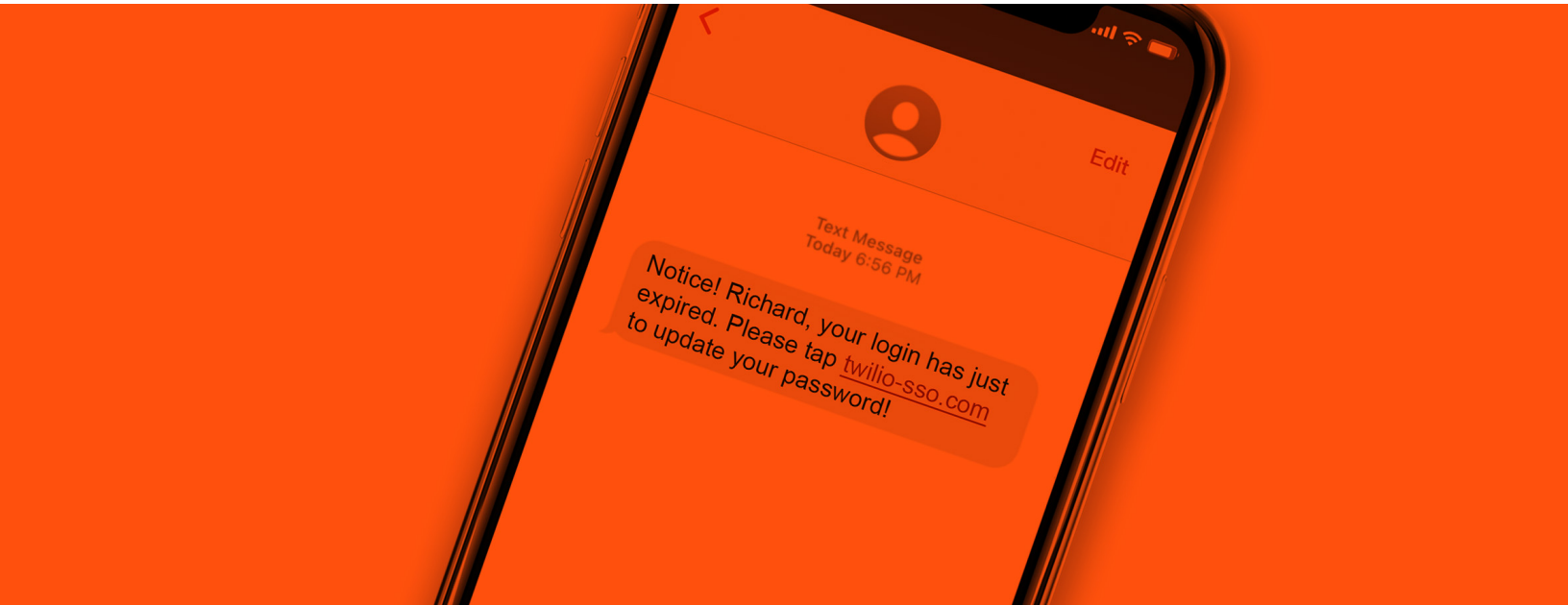
Even a decade ago, IT departments had considerably less to worry about when it came to protecting their organization against attacks. Security has evolved beyond "protecting the perimeter." Traditional endpoints, like desktops, are no longer located on-site and are owned by the company. In the past, these assets were protected on-premises by layers of security.

Smartphones and tablets are mobile devices that have transformed the way we stay connected with family, friends, and colleagues. However, new risks have been introduced into the workplace as employees access communication channels like email, SMS messaging, apps and messaging apps.

Employee-owned devices are challenging to manage and lack the visibility needed to block advanced threats, even if they are enrolled under company management. IT teams find it challenging to remediate threats or identify risky devices because they do not have adequate control over them because they lack the same level of controls and permissions granted to the device owner. However, corporate-owned devices face the same challenges. In fact, **42% of enterprise organizations reported that their mobile devices and web applications led to a security incident in 2020.** The same percentage indicated that unauthorized apps in the workplace got access to enterprise data, and 10% of IT and security leaders reported unsecured apps due to a lack of encryption or authentication.

Mobile threats are not the only risks enterprises should be concerned about; even the apps you might expect to be rigorously protected regularly fall victim to various types of malware. The apps you get from an official app store are typically safe, but there are some that pass inspection and still contain malware. As just one example, according to Zimperium's research, 121 financial apps in the U.S. — including mobile wallets and banking apps — are targeted by Trojan Horses that use various methods to access sensitive data, steal credentials and share stolen information. This malware is disguised and hidden in a normal-looking app and, for the most part, is downloaded onto devices from the major app stores.

Threat actors count on the fact that many apps are not hardened, and the users pay little attention to the permissions and settings that contribute to making their devices vulnerable. As a result, mobile devices are seen as the new golden ticket to corporate data. Bad applications, rogue networks, or compromising the device itself are only a few ways adversaries try to gain access to corporate assets. For example, the cloud communications company Twilio recently disclosed a data breach after their employees were targeted through an SMS spear phishing attack. "The SMS phishing messages baited Twilio's employees into clicking the embedded links by warning them that their passwords had expired or were scheduled to be changed."



An Introduction to Mobile Threat Defense

As technology evolves to address new business challenges and needs, the modern mobile era has ushered in a new category of security to help combat current threats. Mobile Threat Defense (MTD) is a comprehensive mobile security solution that prevents and detects mobile threats across devices, networks, and applications. MTD leverages various techniques such as machine learning (ML) and behavior analytics to detect threats, app vetting, and device vulnerability management.

Although MTD and MDM share a broad goal — protecting your business from mobile threats — MTD is an advanced addition to the mobile security tech stack. MTD tools appeared on the market in the last decade, but most of them do not offer comprehensive on-device protection and need to be updated or connected to an active network.

The first published mention of the solution category appeared as Mobile Advanced Threat Defense (MATD) in Gartner's 2014 Hype Cycle for Enterprise Mobile Security. At that time, MATD was seen as a subset of the Advanced Threat Defense (ATD) market. However, MTD soon became its own solution market, appearing as MTD in a presentation at the Gartner EMEA IT Infrastructure and Operations Management Summit that year.

Mobile Threat Defense is a proactive way of protecting mobile endpoints against attacks and threats. MTD functions as a comprehensive alarm system, continuously scanning a device to protect against threats. If a device isn't secure — if there is an attack or a vulnerability, like unpatched software — both the user and the enterprise will be notified.

Are You Securing Mobile Devices or Just Managing Them?

MDM is, as its name suggests, a management tool. An MDM controls the device itself, allowing organizations to securely distribute apps, set minimum operating system (OS) requirements, and block apps.

MDMs provide basic threat protection by notifying security teams when someone tries to jailbreak the device. However, if you want to protect your organization from as many of the threats covered by the MITRE ATT&CK framework as possible, using MDM alone, you'd have to restrict usage of the device to a nearly impossible extent. In addition, your users would likely resent the control and worry about the privacy of their personal devices, apps, and data. Plus, you would not have the ability to detect or resolve threats from networks, phishing, or apps.

MTD scans for several kinds of attacks, such as SSL-stripping, man in the middle (MiTM), phishing, rogue networks, malware, and other attacks. A comprehensive solution will be deployed on-device and machine learning to detect and prevent mobile threats across devices, networks, phishing, and malicious app attacks. Using an MTD solution, your security team will have more control over the security policies required to meet stringent security and compliance mandates. In addition, MTD providers should include privacy policies to make it easier for employees to understand how data is handled without compromising their privacy while their devices are being protected.

Leveraging MTD and MDM tools in concert comes with some benefits. For example, once an MDM has enrolled in a mobile device, applied policies, and is granted access to company resources, employees have limited restrictions that interfere with their daily productivity. Security teams can monitor devices in real-time and securely push the MTD app down to the device without little to no steps necessary to install, significantly increasing an organization's adoption rate while preserving an employee's privacy.

Mobile Data Security and Privacy Concerns

Over half (60%) of enterprises allow their workforce to access email on their mobile devices, with another 31% in consideration. Securing BYOD can be more difficult than securing a company-owned device for several reasons. For starters, an employee-owned device is just that - owned by the employee. As an employee, it feels intrusive to be told what you can and cannot download by your employer.

Installing an on-device agent to scan the mobile ecosystem on an employee's property may also be regarded as intrusive, especially to their privacy. Depending on the security requirements, enterprises using an MDM can set up email accounts, download and restrict apps from an app store, and secretly gather personal data and payment details to ensure the employee's device is in compliance. Naturally, employees will have concerns over how their data and location are handled by the security team.

For these reasons, security teams have a slow adoption rate when it comes to securing BYOD. Employees want to know their privacy is respected and that only the appropriate quantity and quality of data is being gathered from their device for security reasons.

In preserving the privacy of the workforce, it is critical that the confidentiality of a user's personal data is protected. Complying with applicable data privacy laws and regulations is a great place to start to ensure data meets compliance standards. Security teams deploying mobile security should consult with in-house counsel to determine what data privacy laws and regulations they must adhere to, depending on the location and industry. Baking these requirements into your mobile security architecture with privacy policies, privacy recommendations, and prominent privacy notifications on an employee's device will help educate them on why securing their device is important to protect their personal data.

Common Mobile Threats

Criminals always go where the money is. In the old days, they robbed stagecoaches and banks. Now your enterprise's data is worth money, and with more and more workers using their personal mobile devices at work, criminals are targeting those mobile endpoints. Here are a few of the most common mobile threats that our team sees in the wild:

Phishing

Phishing is an ever-present cyber threat, probably because cybercriminals find that it works. Despite the fact that users are often trained to spot and avoid phishing scams, Zimperium's research found that 1 in 10 mobile users clicked on a malicious link in 2021. In fact, 90% of attacks start with a phishing attack, and your users are likely to check their work email on their phones.

Malware

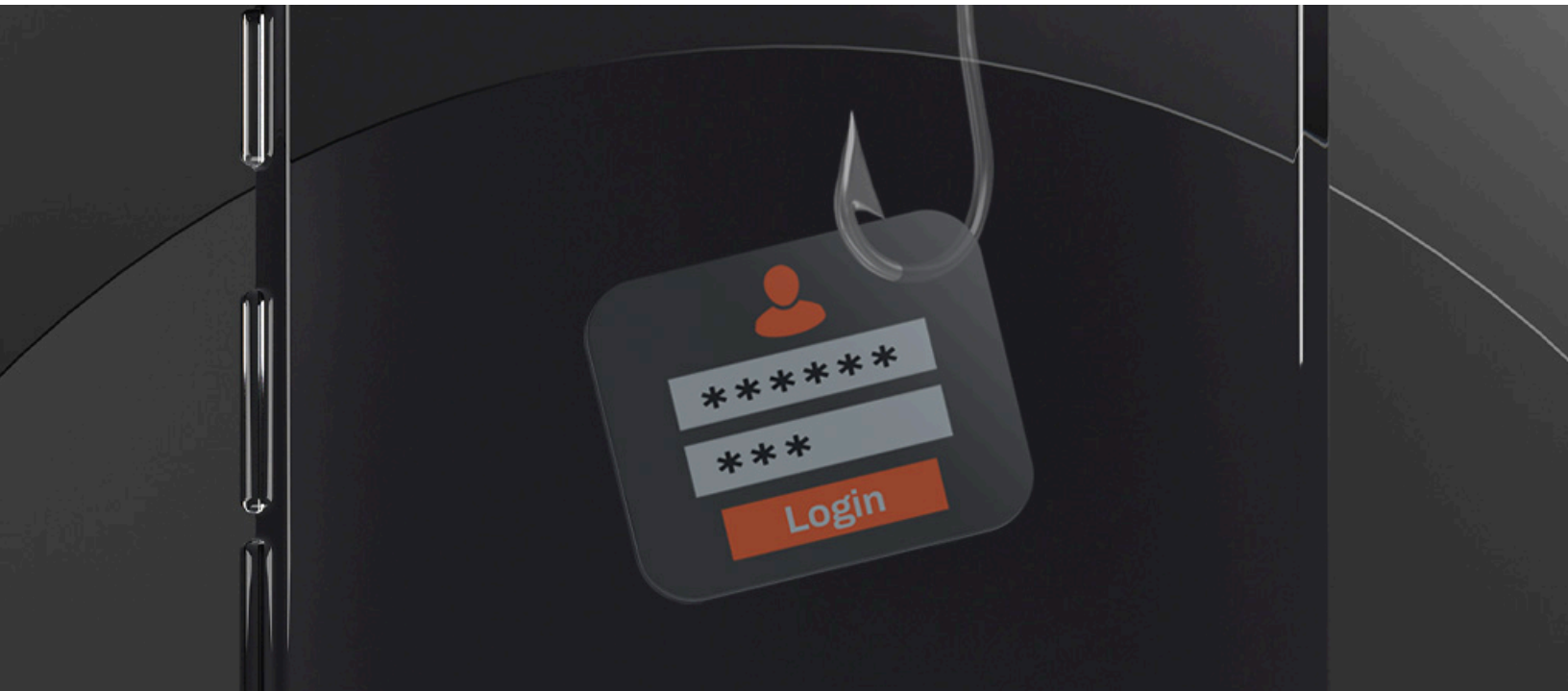
Malware is a common threat affecting mobile devices to a sobering degree. One in four mobile endpoints encountered malware in 2021, and according to a recent survey of IT and security leaders, 52% of organizations experienced malware attacks, including viruses and ransomware. Trojans are an example of mobile malware found in mobile apps that users unknowingly download.

Zero Click Attacks

Zero click attacks are attacks in which the user doesn't trigger the attack by clicking on a malicious link. In a zero-click attack, the attacker is able to exploit previously unknown vulnerabilities to create their own entry point into the device. The exploitation of zero-day vulnerabilities in mobile devices is on the rise; in 2021, such attacks rose by 466% in both Android and iOS devices.

Rogue Wi-Fi Networks

Mobile devices will connect to any Wi-Fi network when cellular service is weak, making them easy targets for adversaries. Wi-FI networks are an easy exploit in the wild by a bad actor. Rogue wi-fi networks are one of the best ways criminals can compromise a device. An Adversary can use a fake wi-fi network with a common name such as Coffee Shop Guest, immediately gaining your trust. However, this rogue network acts as a gateway for a man-in-the-middle attack to spy on your activities, steal information, or launch malware to steal credentials.



Mobile-Specific Security Considerations

It's important to understand that mobile security requires different measures than traditional cybersecurity. A mobile device's technology functions differently than your traditional endpoint, and they, therefore, have different security considerations. Here are two of the more commonly cited mobile-specific considerations:

Device State

Device state is an indicator of whether software can be freely flashed to a device and whether verification is enforced. For Androids, there are two states: Locked and Unlocked. iOS devices, on the other hand, are supposed to be locked only, although they can be jailbroken to give a user root access and bypass Apple's restrictions.

An unlocked Android comes with security risks, however. If an Android is unlocked, a bad actor who gets physical control of the device can reboot the device and access its data, bypassing security measures meant to keep them out. Likewise, a jailbroken iPhone is more susceptible to malware and other threats.

Vulnerable Applications

Mobile applications are a source of entertainment on our mobile devices that enable productivity in the workplace to keep our finances in order with banking apps. Today, 120 apps are stored on a smartphone today. However, app vulnerabilities are more common than you may think. The code of mobile app developers can expose employee and customer data, putting privacy and security at risk. Mobile apps can be downloaded and reverse engineered by adversaries or rebuilt to mimic a common brand, with the intent of enabling sensitive permissions on a device handing every password and SMS message over to an adversary.

The Role of Machine Learning in Threat Detection

MTD's proactive approach is made possible by machine learning (ML), a type of artificial intelligence that uses algorithms to make increasingly accurate predictions as an ML model gathers more and more information.

A machine learning model is created through training and tuning; an algorithm is exposed to a set of training data. The training data teaches the model what it should look for in datasets (like threat data). Once the initial training has taken place, the model is exposed to data it's never seen before to see if it makes the correct inferences. Data scientists then tune the model, exposing it to more and more data and helping it learn.

How does this look in threat detection? ML models use various methods to detect attacks. For example, a classifier may be used to determine the probability that a link is part of a phishing scam or that an app is, in fact, malware.

To get the most immediate threat detection, machine learning must be deployed on the device itself, not in the cloud, to ensure the device is protected even if it is not connected to a network. A breach can happen quickly, in milliseconds. The machine learning algorithms must be local, so they can respond as fast as possible and not be at the mercy of weak wi-fi or mobile service.

Top Recommendations for Implementing MTD

Organizations have options when it comes to implementing a MTD solution. An MTD can stand on its own or be used along with other Unified Endpoint Management (UEM) solutions or MDM.

When used with an MDM solution, the MTD functions as an integrated part of the mobile endpoint security strategy protecting the actual device from mobile threats instead of managing the device. **The MDM's management policies enable automation, such as pushing the download of the MTD app and activation of MTD detections and make it easier for the admin to automate conditional access and security policies based on detections and policies from the MTD solution.**

For example, if a user is on a rogue wi-fi network, a MTD will alert the user and the enterprise to the threat, working in tandem with your MDM to shut down access to business-critical apps until the user is on a safe network.

In cases where the MTD is being used on its own on an unmanaged device, the MTD solution is still able to identify and prevent many attacks on mobile devices by using machine learning to proactively scan the device itself for harmful behavior, malware, or other threats. The MTD then notifies the user but is limited in the controlled remediations it can make on its own, such as locking access without the help of an integrated UEM solution.

In both cases, while the threat is handled locally, the MTD also reports back to the enterprise, so the security team can understand all threats that were encountered. However, it is highly recommended to complement a MTD solution with an MDM to reduce user friction greatly. Having both in place will allow you to preserve user privacy and protect critical business data.

Conclusion/Recommendations

According to Verizon, when asked how critical, on a ten-point scale, mobile devices were to the smooth running of their organization, 91% of respondents answered seven or above—and 78% answered eight or higher. The 2022 Mobile Security Index declared that "mobile devices are critical" to how organizations work.

In the context of mobile security, blocking and tackling means being proactive about finding and remediating threats to mobile devices. If you wait for notification of a breach, it's already too late. So it's important to sniff out the presence of a threat as soon as possible.

So, what steps can your enterprise take to proactively address mobile risk?

1. **Analyze Mobile Risks:** Rate and prioritize your risks based on your organization's specific security needs. For example, how great a risk is a stolen device? What about malware or a user's personal behavior with their device? By creating a risk register, you can quickly identify risks to your organization.

2. **Apply Zero Trust:** Gone are the days of trust but verify. Now that applications are in the cloud and mobile devices are increasingly important in the workplace, zero trust is critical to any security strategy. Apply the principle of least privilege to ensure your data and network remains safe.

3. **Invest in MTD:** MTD allows your organization to address risks as they arise without compromising your employees' user experience. According to Gartner, MTD can "stand on its own as a means to provide zero trust access, federate single sign-on across applications and continue generating telemetry" to help businesses make better, smarter, and faster access decisions.

Contact us today to learn more about how Zimperium's MTD solutions can help proactively protect your organization from the evolving threat landscape.

Recommended Reading

2022 Global Mobile Threat Report
Mobile Banking Heists: The Global Economic Threat
How to Implement BYOD in a Zero Trust Environment
Verizon's MSI Mobile Security Index 2022

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244