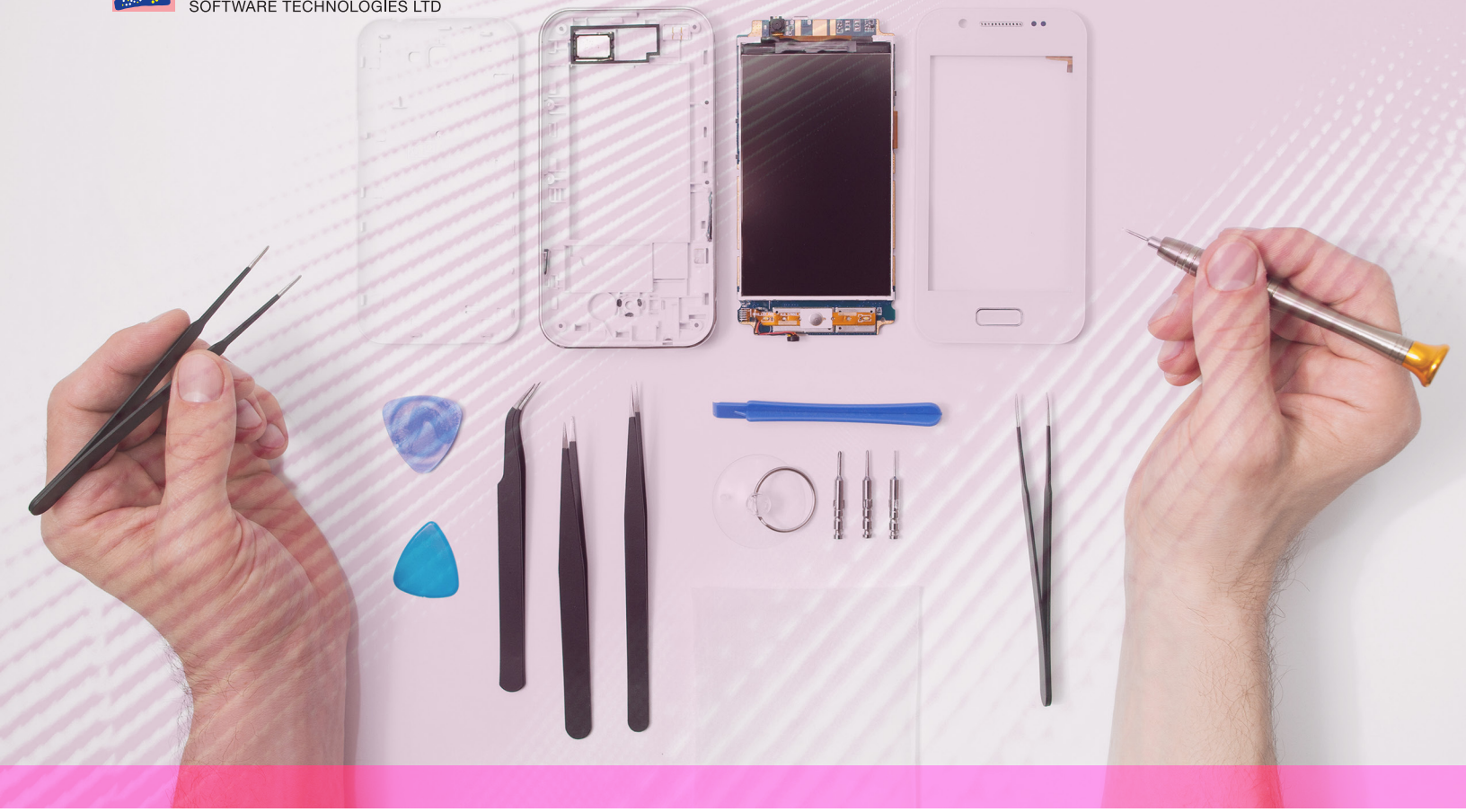
Check Point
SOFTWARE TECHNOLOGIES LTD



# MOBILE MANAGEMENT SOLUTIONS ARE NOT SECURITY

## Use The Best Tool to Secure Mobile Devices

# Introduction

Mobile management solutions were never designed to protect devices against sophisticated cyberattacks. The operative word with these solutions has always been the word 'management'. Security was never their focus, however many businesses mistakenly bought these expensive solutions with the belief that they were locking down the devices.

For more than a decade enterprises have deployed mobile management solutions to accommodate and offer basic protections for mobile programs, both in bring-your-own-device (BYOD) ownership models as well as in corporate owned scenarios. But the security provided by these solutions was always quite limited. Threat actors quickly identified mobile devices as easy targets for exploits and malware, even with mobile management solutions in place.

In this paper we will review the use cases addressed by mobile management solutions, and why they are not built to protect fleets of mobile devices from threats that put enterprise data at risk. We will also elaborate on how to effectively address the need for mobile security and implement a Zero Trust, comprehensive mobile security strategy to remain protected from the ever-evolving mobile threat landscape.

# Mobile Management ≠ Mobile Security

Unified Endpoint Management (UEM) solutions, or their predecessors Mobile Device Management (MDM) solutions, were designed to help mobilize businesses by streamlining processes, managing device lifecycles, and creating a managed workspace on smartphones and tablets. Today UEM solutions have evolved into consolidated solutions that work with other endpoints beyond mobile devices, including PCs.

UEMs enforce some device-level policies to maintain a basic hygiene, such as device encryption, remote wipe, and in some cases, have a basic jailbreak/root detection function too. But these basic features don't provide the protection needed to withstand even the most basic mobile malware attack. UEMs do not scan for mobile-related threats like malicious apps, vulnerable operating systems, network-based attacks, or protect users against phishing and other social engineering attacks. As a result, users and organizations remain exposed to credential theft, data leakage, or device takeover.

UEMs do not scan for mobile-related threats like malicious apps, vulnerable operating systems, network-based attacks, or protect users against phishing and other social engineering attacks. As a result, users and organizations remain exposed to credential theft, data leakage, or device takeover.

## MAN-IN-THE-MIDDLE-ATTACKS

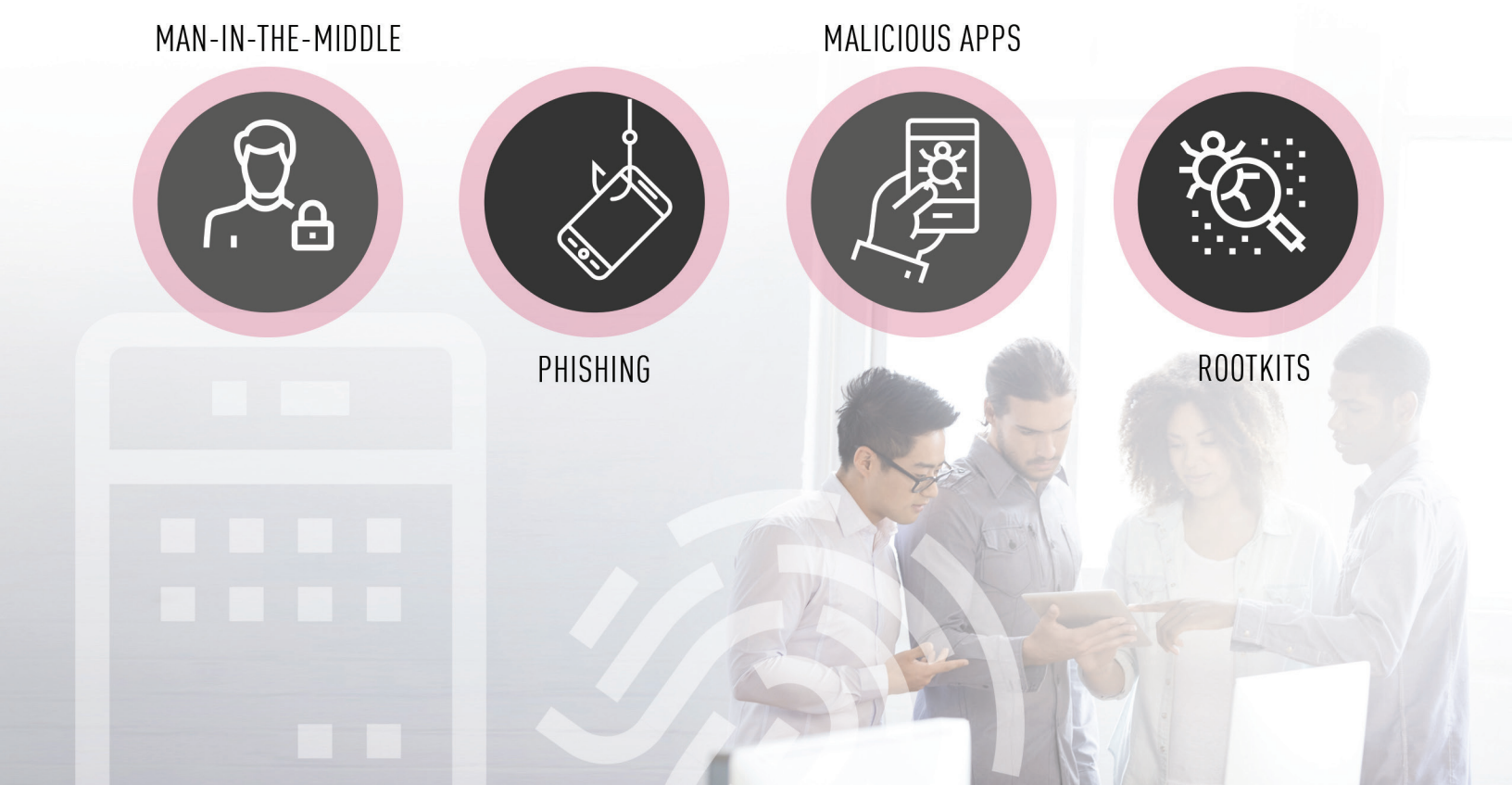
One of the most common network-based attacks on mobile devices are Man-in-the-Middle (MitM) attacks, where malicious actors fool unsuspecting users to connect to a rogue WiFi network. Two kinds of MitM attacks are SSL stripping and SSL bumping. SSL stripping removes the SSL certificate without the user's knowledge and decrypts the traffic, hence making it readable to anyone. SSL bumping uses fake SSL certificates to fool apps and browsers into believing they are using secure connections. Cybercriminals can then intercept communications, allowing them to steal data in transit.

## PHISHING CAMPAIGNS

Mobile users are a prime target for a variety of phishing attacks. In fact, 91% of all cyberattacks begin with a phishing campaign[1], and mobile devices are the perfect channel to deliver them. Because of their small screens, phishing URLs become harder to identify on mobile devices. All it takes is for one employee to succumb to a phishing attack and reveal their corporate credentials, and a malicious actor can infiltrate the corporate network, even with a management solution in place.

## MALICIOUS APPS AND ROOTKITS

Management solutions provide visibility over the assets on the managed part of the device. However, when it comes to the personal profile, users can install applications from official app stores or third-party stores. Malicious apps can make their way to any app-delivery source, such as spyware, rootkits, Remote Access Trojans, and more. Without real-time threat intelligence and behavioral engines assessing an apps' behavior, users are exposed to mobile malware within infected applications.



# Use the Right Tool for the Job

Securing mobile devices is no longer optional in an era when data protection is central to any organization's security policy, and employees constantly use their smartphones to consume and share corporate data. Mobile Threat Defense (MTD) solutions should be a key component of all corporate mobile programs because only those solutions can protect against sophisticated attacks.

MTDs prevent enterprise threats on iOS and Android devices using a variety of techniques, including machine learning and behavioral analysis based on mobile threat intelligence[2]. In order to do so, their capabilities revolve around the three key pillars of mobile security:

- Protecting the device's operating system against vulnerable configurations, exploits, advanced rooting/ jailbreaking, etc.
- Protecting from application-based risks, such as malicious apps that can exfiltrate data, malware embedded on seemingly legitimate apps, abuse of privileges, etc.
- Protecting from network-based attacks, such as Man-in-the-Middle traps, data exfiltration to command & control servers, or phishing campaigns attempting to steal credentials.

MTDs are in most cases deployed as a non-intrusive app on the employees' devices, and centrally managed by a cloud-based dashboard.

There are several use cases where MTD solutions address enterprise mobility risk and compliance:

- First, as a comprehensive mobile security solution that prevents breaches originating from malicious apps, spoofed networks, Man-in-the-Middle attacks, and OS exploits.
- As a security component to be added on top of UEMs: Gartner has recommended adding MTD solutions to the incumbent UEM solution in the enterprise, serving as the security add-on to these management solutions.
- Mobile phishing protection, where MTDs can prevent credential theft by blocking phishing URLs, or by dynamically scanning for phishing indicators in unknown phishing sites.
- Regulation and policy compliance matters. Data regulation also applies to the data that is consumed on mobile, so having visibility of the risk posture of a device is critical to ensure that data does not leak outside the organization's network.
- Another frequent use case is app vetting, where the MTD analyzes apps and indicates which ones conflict with corporate policy, and report to the UEM for it to uninstall the app.

# Comparison of UEM (MDM) Capabilities vs. Market-Leading MTD Solution Capabilities

| Features | Mobile Management | Enterprise Grade Mobile Security |
|---|---|---|
| Device lifecycle management | V | |
| App management & containerization | V | |
| Remote Access | V | |
| Conditional Access | V | V |
| Jailbreak/root detection | Static only | Static and dynamic |
| Malicious app detection | | V |
| Download prevention | | V |
| Anti-Phishing (known and unknown sites) | | V |
| Anti-Bot (blocking C&C communications) | | V |
| Man-in-the-Middle attack prevention | | V |
| URL Filtering | | V |
| Real-time threat intelligence based on a global sensor network of mobile, endpoint, IoT, cloud, and network indicators | | V |

# A Comprehensive, Zero Trust Approach to Mobile Security

Mobile devices must be treated as any other endpoint on the corporate network when it comes to security, risk management, and threat visibility. A Zero Trust approach in the enterprise should include enforcing policies on the mobile endpoint that prevent threat actors or malicious insiders from infiltrating the organization and infecting the corporate network.

UEM solutions are used for managing mobile devices. On the other hand, MTDs provide mobile security by preventing, detecting, and remediating sophisticated cyberattacks, using a variety of techniques on the device, network and application level. MTDs feed critical information to the UEM to help them enforce Zero Trust policies. Together, they can provide an integrated management, security and enforcement solution.

Check Point SandBlast Mobile, part of Check Point Infinity, provides enterprise-grade mobile security within a consolidated architecture to secure network, endpoints, cloud and IoT.

[1] Enterprise Phishing Susceptibility and Resiliency Report

[2] Gartner 2019 Market Guide for Mobile Threat Defense

**Worldwide Headquarters**
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

**U.S. Headquarters**
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

**www.checkpoint.com**