HYPORI™
VIRTUAL MOBILITY

How Flaws in Mobile Device Management Solutions Expose Them as Major Cyberattack Targets

WHITEPAPER

Summary

At one point in time, Mobile Device Management (MDM) solutions were considered the ultimate development in mobile enterprise security. According to a 2012 Gartner report, 65% of enterprises would adopt an MDM solution for their corporate liable users by 2017.

But, are today's MDM solutions delivering? Or has the technology passed its prime, and is it time to look for something better? On the enterprise side, MDM systems allow companies to manage employee mobile devices. MDM gives end-users access to corporate data and apps on endpoint devices and proposes to separate these apps and data from mobile device personal apps and data. However, there are privacy concerns, security risks, and technology gaps inherent in the MDM model.

The Situation

When MDM came on the market, it was to control and secure mobile devices in the workplace and safeguard the systems these devices accessed. MDM relies on endpoint software—an MDM agent installed on the user device and an MDM server in a data center.

End-users access corporate data via this agent and download it to their mobile devices to perform work functions. However, once company data moves to the mobile device, it is challenging to protect and control, and it is no longer separated from the organization, presenting a significant security risk. Mobile devices are notoriously unsafe for many reasons and in higher workplace use today than ever. In Q1 2020 alone, mobile phishing attacks on corporate users increased by 66.3%.

Compromised end-user devices also mean risks for enterprise servers. Today, MDM servers are particularly vulnerable targets. There are accounts of multiple threats on Mobile Iron enterprise servers in recent news, including Distributed Denial of Service (DDoS) gang attacks and attacks by Chinese nation-state actors. In late 2020, the NSA listed the Mobile Iron CVE-2020-15505 remote code execution vulnerability in the "top 25 vulnerabilities currently being consistently scanned, targeted, and exploited by Chinese state-sponsored hacking groups."

With these kinds of attacks, it is clear that today's MDM software solutions are not effectively protecting mobile devices or enterprise data and servers. MDM vendors are engaged in a never-ending arms race with the hackers, and they are losing. Many organizations rely on and have implemented MDM to secure their corporate networks and mobile devices. However, as recent cyberattacks show, the enterprise and its mobile workforce are more at risk than ever. A better solution is needed.

The Problem

What is fundamental to MDM also presents its problem. MDM's objective is to deliver a central control for the entire fleet of mobile devices. However, a platform breach means a widespread mobile device breach. Because actual data transfers between the mobile device and the back-end enterprise system, that data is always vulnerable to attack. A breach on the device level, server level, or during transfer puts security at risk.

In the past, as reported by Cisco TALOS, malicious campaigns on MDM focused on controlling end-user devices. Bad actors now exploit broader vulnerabilities in MDM solutions and are attacking corporate-owned MDM servers.

In Q2 of 2020, Check Point researchers identified a new banking trojan targeting a multinational conglomerate distributed by its MDM server. When discovered, this malware had already infected over 75% of the company's devices. Using stolen access privileges, hackers could steal sensitive business and personal data, including Intellectual Property (IP), Personal Identifiable Information (PII), and Protected Health Information (PHI).

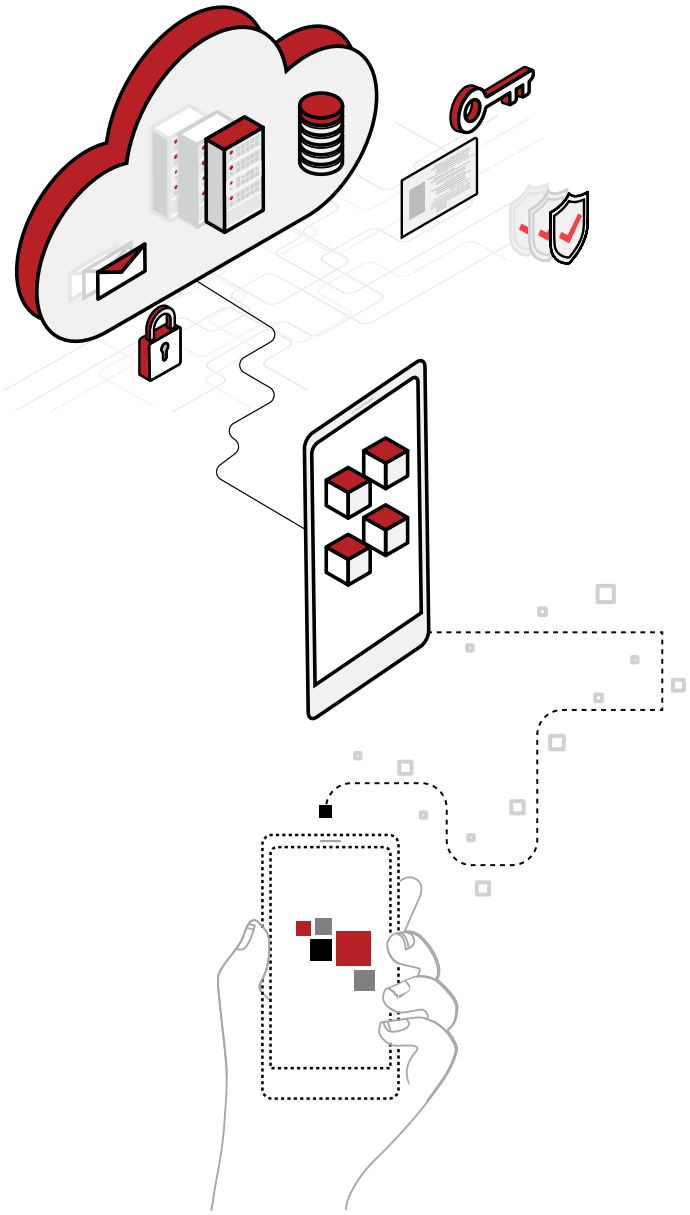
This attack was the first Check Point reported MDM server lateral movement attack inside a corporate network highlighting the difference between MDM's two objectives. One of managing mobile devices, the other of securing them.

MDM must enable IT to deploy apps, manage updates, and carry out other administrative tasks from a central server. Because MDM servers are always online to empower employees to do their jobs and stay up-to-date on corporate apps and data, they are accessible, opening them up to attack. Vulnerabilities exist at the server and end-user device level, and even with administratively managed access times, data delivery is in real-time, and the internet never turns off.

With MDM, every employee device must be maintained, updated, and managed. Because employees cede device rights and privileges to IT, they risk personal privacy. End-users resist this invasion of privacy. Often, rather than comply with MDM protocols, many employees circumvent or outright refuse to use company-installed MDM solutions, rendering them useless, wasting resources, and most significantly, compounding security risks. IT can also remote wipe compromised devices with MDM, creating more end-user concerns, and leading to greater user adoption issues. No employee wants their personal data's safety and preservation in the hands of corporate IT.

The Solution

There is a next-gen technology solution. Hypori Virtual Mobility™ delivers highly secure, regulatory-compliant enterprise mobility that protects employee mobile devices and secures sensitive customer and enterprise data.



Hypori's solution securely contains all organization data on a fully-featured virtual mobile device in the company-owned data center with 100% separation of personal and enterprise data. Hypori Virtual Mobility focuses on securing the data, not the device.

Hypori is also centrally managed, reducing administrative costs and labor. Organizations do not need to access end-user devices, ensuring employee privacy, and there's no company exposure should devices be compromised. With Hypori, cybersecurity management shifts from vulnerable personal devices to a secure data center. No data is ever at rest on mobile devices allowing the remote workforce secure enterprise data access in an intuitive, confidential environment.

Hypori delivers a military-grade secure, centrally managed, admin-friendly Virtual Mobility Solution for your financial institution that is regulatory compliant, cost-efficient, and user-intuitive.

To learn more about Hypori Virtual Mobility, contact us for a demonstration today.

Contact us

info@hypori.com

The National Security Agency Commercial Solutions for Classified (CSfC) provides DoD entities the ability to conduct secure classified communications using Commercial-off-the-Shelf (COTS) products. Under this program, the Mobile Access Capability Package v2.0 provides a framework for how to secure these communications from mobile end-user devices into government enterprise resources. Under the MACP v 2.0, communications must be established using an inner and outer tunnel to provide a secure communications path. Hypori Client v4.2 for iOS, Android, and Windows 10 is eligible to be used as a TLS Software Application Product component in a CSfC solution. This means that in combination with a CSfC eligible TLS Protected Server, Hypori is eligible to provide the inner tunnel for secure communications.

11 March 2019