SOLUTION BRIEF

proofpoint.

SECURING YOUR MOBILE WORKFORCE:

WHY MDM/EMM SYSTEMS ALONE CAN'T STOP TODAY'S THREATS

Mobile devices are an essential tool for modern business, giving people access to email, files, and other key business data anytime, anywhere—on any device imaginable.

Embracing mobile devices in the enterprise, especially those owned by employees themselves, can save money and keep workers happy. But they also pose huge security risks to your enterprise.

A compromised phone can give attackers access to the same networks and data that make the device so valuable as a business tool. That opening, in turn, can lead to data loss, data theft, malware-infected networks, password compromises and more. And attackers can leverage stolen corporate data such as address books, calendars, credentials and network profiles to mount sophisticated attacks through other channels such as email.

MDM/EMM ISN'T ENOUGH

Many organizations have deployed mobile device management (MDM) and enterprise mobility management (EMM) systems. While an important first step, MDM/EMM tools are only the underpinnings for enforcing policy, taking defensive actions when alerted of a threat, and helping remediate compromised devices, users and networks.

MDM tools are designed to configure and manage mobile devices to protect corporate data if the device is lost or stolen. To this end, MDM solutions are effective. EMM tools help protect the broader mobile ecosystem by enforcing security policies and simplifying how enterprises manage devices, apps and content.

But on their own, neither detects new threats. For that, you need a mobile threat defense (MTD) solution that works with your MDM/EMM deployment. MDT provides the underlying intelligence to detect threats in real time and alert your MDM/EMM system to act on them.

FIVE THREATS MDM/EMM SOLUTIONS MISS

No matter what MDM/EMM system you've deployed, your MTD capabilities are crucial.

Most enterprises know better than relying on consumer app stores to vet mobile apps; malicious and counterfeit apps regularly slip through major app stores.[1] They may not be aware of other threats that are invisible to MDM/EMM tools on their own.

That's why Gartner says MTD systems are "increasingly important" for securing mobile devices in the enterprise in 2017 and beyond.[2]

[1] Vindu Goel (The New York Times). "Beware iPhone Users: Fake Retail Apps Are Surging Before The Holidays." November 2016.

[2] Gartner. "Market Guide for Mobile Threat Defense Solutions." July 2016.

Malware, crimeware, and side-loaded apps

MDM solutions do not scan and analyze unknown mobile apps. That paves the way for malicious apps to load malware onto corporate networks.

Data-leaking apps

Many apps published on major app stores leak or steal corporate data—with users' unwitting permission. Many users blindly click to accept apps' terms of service when it first runs, unaware of the security implications.

Wi-Fi hotspot compromises

MDM solutions allow users to access Wi-Fi hotspots in the clear. That leaves data and network activity vulnerable to anyone monitoring the network, including potential attackers. Even legitimate networks can pose a risk when misconfigured.

Zero-day threats

Preventing zero-day attacks requires real-time threat intelligence deployed across all devices and networks. MDM tools don't have this level of intel built in.

Phishing and spear-phishing

MDM solutions have no way to determine whether a link is malicious or to stop users from clicking on it. Attackers can use these links to download malware or trick users into handing over their account credentials.

PROOFPOINT MOBILE THREAT DEFENSE

Proofpoint Mobile Defense works with your MDM/EMM tools to identify and block malicious and risky apps, neutralize malicious URLs, and keep users from harmful Wi-Fi networks.

It gives you the power of a global network of threat intelligence that spans apps, email, social media, and the web to secure mobile devices that have access to your corporate data. And it integrates directly with the top MDM/EMM platforms to automate the way you protect your enterprise from mobile threats—and remediate them before they can cause lasting harm.

We have analyzed more than 50 million apps on Android and iOS. We combine this data with the unique intelligence derived from real-time sensor data and our analysis of more than 1 billion messages per day in enterprise environments. This far-reaching insight allows us to dynamically alert your MDM/EMM system as threats are discovered. These include malware, crimeware, zero-day threats, URLs used in phishing attacks, and Wi-Fi networks that are malicious or compromised.

We also analyze apps that are not overtly malicious to determine whether they pose a threat to corporate data. You can use the insight to allow or prevent apps from transmitting or accessing corporate data automatically based on your security policy.

To learn more about how Mobile Threat Defense can ensure that BYOD doesn't stand for "bring your own disaster," visit our website: proofpoint.com/us/products/mobile-defense.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.