Protect your company data from mobile threats

Increasingly, hackers are targeting mobile devices as the vehicles in which to carry out their attacks. Why? Mobile devices are everywhere and access practically everything. And because most users have sub-par, if any mobile security measures in place, hackers are having a heyday.

Organizations are challenged with visibility into malicious threats, meeting compliance and regulatory security guidelines, and lack complete control over employee-owned devices. Users want instant access to corporate data on a device of their choice anytime, anywhere.

MobileIron Threat Defense allows you to fully secure both corporate and employee-owned devices so users can be more productive while securing mobile endpoints against advanced threats. MobileIron's non-intrusive approach to securing Android and iOS devices provides comprehensive protection around the clock without impacting the user experience or violating their privacy.

MobileIron Threat Defense delivers unparalleled mobile security that enables enterprises to monitor, manage, and secure devices against attacks that occur at the device, network and application-level, as well as prevent mobile phishing attacks. With one application, known and zero-day threats can be stopped on-device, even without network connectivity, before they cause damage. Users are not required to take any action to deploy or activate the application, and they cannot uninstall the protection. There is no disruption to their productivity, and mobile devices are prevented from impacting the corporate network and risking data loss.

Key Benefits

Built for mobile devices, MobileIron Threat Defense uses machine-learning algorithms optimized to run continuously on-device, detecting threats even when the device is offline.

Easy

One app makes it easy for you with the protection built into your MobileIron client. And it is easy for your users who are not required to take any action to activate the client.

Insightful

Gain immediate and ongoing visibility into malicious threats across all mobile devices, and detailed analyses of risky apps.

On-device

Receive unmatched detection and remediation of known and zero-day threats with machine learning algorithms on-device without internet connectivity required.

About MobileIron

MobileIron is redefining enterprise security with the industry's first mobile-centric, zero trust platform. MobileIron Threat Defense is available on-premises and in the cloud.

For additional information, visit www.mobileiron.com/threatdefense, or contact your MobileIron sales representative.

MKT-0819 EN US V3

Capabilities

For timely detection and remediation of device, network, app and phishing attacks on mobile devices, enterprises can protect their company data with the MobileIron Threat Defense solution.

Proactive Detection of Threats and Attacks

Protect your corporate network and data against known and zero-day malicious threats with sophisticated machine learning and behavior-based detection on-device.

Timely Remediation

Limit time of exposure for possible exploitation and stop zero-day attacks with policy-based compliance actions that provide alerts of risky behaviors, proactively shut down attacks on-device without network connectivity required, isolate compromised devices from your network, and remove malicious applications and their content.

Greater Visibility

Gain visibility and awareness into device, OS, network, and application risks, and receive actionable information to respond more quickly and effectively to threat vectors.

Easy Management

From one application, provide granular policy and compliance actions to easily manage corporate and employee-owned devices with automatic deployment and activation, no user action required.

Our Unique Approach

MobileIron Threat Defense pushes a local compliance action that detects and remediates the next generation of mobile threats on-device, even if the device is not connected to either the Wi-Fi or cellular network, which is uniquely different from other solutions.

Real World Examples

Device Exploitation

After MMS messages were sent to targeted users, an exploit was executed, privilege was escalated and the device was compromised in a way that remained persistent for targeted attacks.

Network Attacks

At a coffee shop near their office, a Wi-Fi man-in-the-middle (MITM) attack against a company redirected users to a spear phishing page where corporate data was stolen.

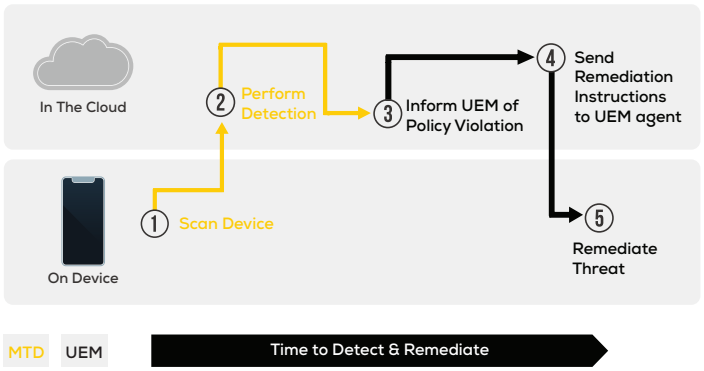
Malicious Apps

Unsuspecting users installed an app from a third-party app store. The app abused permissions, executed a device exploit, leaked data and was used as weapon to penetrate internal networks.

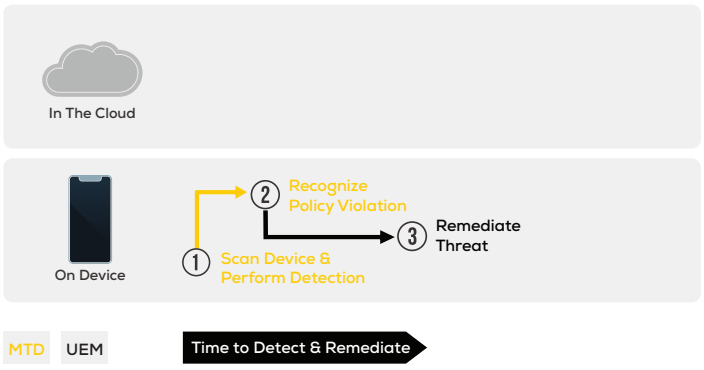
Phishing Attacks

Leveraging social engineering, a bad actor tricked an unsuspecting user into clicking on a link and providing their corporate login credentials. The attacker was then able to login as the user and access corporate resources.

Other threat defense solutions



MobileIron Threat Defense solution



mobileiron

490 East Middlefield Road, Mountain View, CA 94043
info@mobileiron.com www.mobileiron.com
Tel: +1.877.819.3451 Fax :+1.650.919.8006