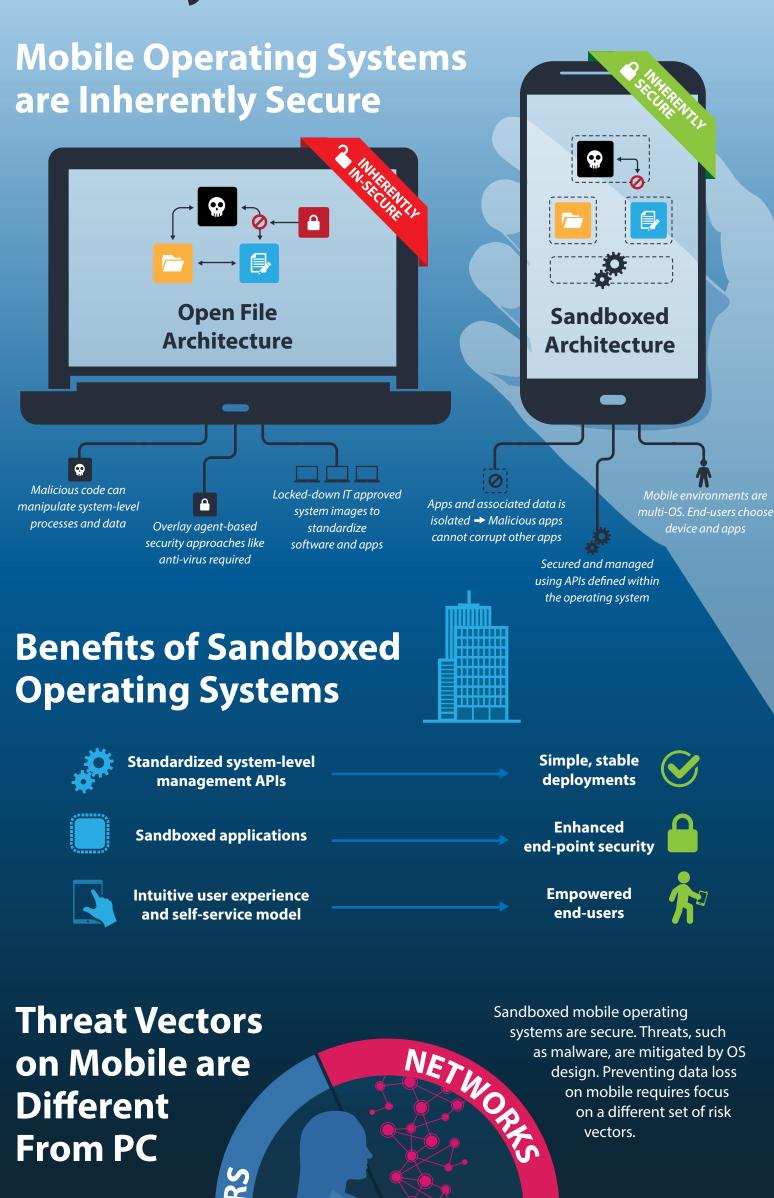
Security for the Mobile First Era



Countermeasures to Enforce Data Loss Prevention (DLP) on Mobile

Data Loss

functions

Device Tampering

Exploit OS vulnerabilities to

jailbreak or root devices, bypass

security, and install malicious apps from un-authorized app stores

Data loss to cloud services and

productivity apps via open-in,

copy, paste and forwarding

Agent-based security solutions such as anti-virus software rely on controlling all processes on a system. This approach breaks in sandboxed environments as one process cannot control other aspects of the system. To secure mobile, IT has to replace traditional PC management tools with purpose-built **enterprise mobility management (EMM) Platforms**, designed to enable end-user productivity while securing apps, content and devices.

Form Factor

Portable form-factors make mobile

devices susceptible to loss or theft

DEVICES

Malicious or Risky Apps

Collect and share data such as

personally identifiable information (PII) and device location with third party advertising and analytics systems **Always-On Connectivity**

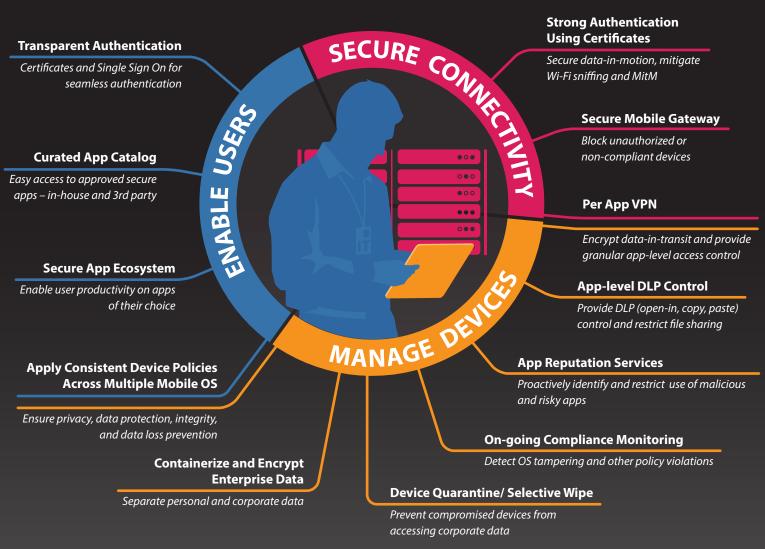
Mobile devices are hyper-connected

and often access sensitive data over

untrusted networks, increasing the

sniffing, rouge access points and Man-in-the-Middle (MitM) attacks

risk of data loss through Wi-Fi



Regulatory Compliance









Industry Data Portability and Information
Security Standard Accountability Act Services

MobileIron is a purpose-built mobile IT platform for enterprises to secure and manage mobile applications, content, and devices while providing their employees with device choice, privacy, and a native user experience.

www.mobileiron.com

