Intel® Device Protection Technology

Hardened Security for Android* OS

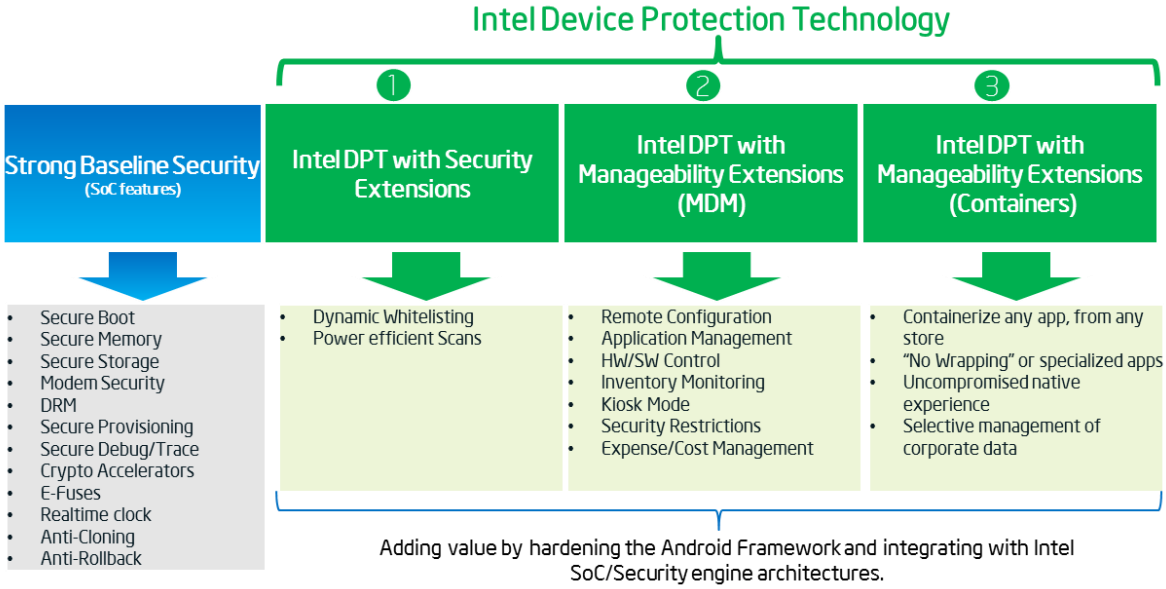
Recent industry reports indicate Android* is the OS in more than 59 percent of laptops, tablets and smartphones worldwide[i]. While its growth has been explosive and continues, vulnerabilities exist because Android is an open platform. Additionally, corporate IT departments are looking for security and manageability functionalities for Android-based devices that meet the needs of their organizations.

Intel recently announced its Intel® Device Protection Technology (IDPT) that includes enhanced security capabilities for Intel-based devices running Android OS. Coupled with the strong security baseline features on existing Intel SoCs, IDPT further strengthens Intel's security offering.

Security Features

Security Extensions for Android OS proactively blocks and helps secure devices from malware that is delivered through malicious applications and websites. These devices need to be paired with an enabled security service, such as McAfee Mobile Security v3.2.

In addition, the security extensions optimize routine scans to minimize the impact on performance or power. It allows the enabled security service to monitor new and changed files and scan only those files, thus streamlining the scan so it takes seconds, rather than minutes, as it is able to ignore unchanged and previously scanned files.



Manageability Features

For managed devices in the enterprise, mobile devices with Intel's Manageability Extensions for Android OS benefit from hardware and software-enhanced security capabilities that provide IT increased levels of control.

Intel added approximately 400 new APIs to cover the following areas of managing devices:

- Application Management
  These policies allow for granular control of applications that may or may not be installed and run on the device. In addition, IT managers can specify which applications are protected so they cannot be blocked or uninstalled.
- Device Configuration, Inventory and Remote Management
  These policies are focused on allowing the IT manager to provision the device and manage settings (such as passwords, Wi-Fi, Bluetooth, etc.).
- Kiosk (single-use) Mode
  Kiosk mode replaces the standard home screen with a single application that is displayed when the device boots. Once in Kiosk mode, the device is locked to that one application and the user cannot exit or uninstall the kiosk mode application. This is often used for single-use devices (e.g. self-guided tour app for a museum) or to provide information on lost or stolen devices to assist in recovery (e.g. return information and ability to call specified number).
- Communications/Network Configuration
  These policies are focused on allowing the IT manager to provision the device and manage settings (such as passwords, Wi-Fi, Bluetooth, etc.).
- Expense/Usage Management
  These controls enable IT administrators to set limits on device usage (e.g., data cap or voice calls) to manage usage of the device and control expenses.
- Container Management
  IT administrators can also create secure containers where corporate data may be stored, effectively separating it from a user's personal applications and data. The container may contain any application from any app store the administrator specifies to protect against data leakage while using native apps to maintain the common Android user experience.

Consumers get all of the convenience and productivity of their mobile devices with no impact to their user experience. IT managers are empowered with more robust manageability controls and know the corporate data is more secured.

Intel Device Protection Technology will ship with supported IA devices and are enabled on the solutions by AirWatch*, Citrix* and McAfee*, among others. Check with your software provider for a list of all supported features.

[i] Canalys, http://www.canalys.com/newsroom/smart-mobile-device-shipments-exceed-300-million-q1-2013