Today’s users are accustomed to a consumer-like experience that is simple and convenient, and they expect to be able to work from anywhere, anytime, and on any device. With more than 2 billion active endpoints worldwide, Android offers a wide range of devices fit for many enterprise price points and use-case scenarios. To enable device management, Google unveiled device administrator APIs in 2010. However, enterprise needs have evolved, sparking the development of Android Enterprise.

With the proliferation of various endpoints in the enterprise, organizations have begun to demand a single management tool and process. A unified endpoint management (UEM) approach is a holistic management framework that enables organizations to manage any endpoint to create a fully connected and secure IT environment.

The modern management approach for enterprises using Android offers flexible integration options to suit a wide variety of use cases while maintaining a consistent native experience for end users, regardless of the device manufacturer.

**DEVICE ADMINISTRATOR “DEPRECATION”**

In order to support today’s more demanding requirements, Google has introduced Android Enterprise, a modern management approach with three management modes:

- **Work Profile Mode**: Designed for personal or bring-your-own (BYO) devices. Enables IT to manage a work profile on a personal device. Corporate policies restricted to the work profile keeping company info secure and separate from personal data.
- **Fully Managed Device Mode**: Designed for corporate-owned and dedicated device use cases. Enables IT to manage the entire device enforcing an extended range of policy controls. Can be further locked down to restrict settings and the apps that can be installed.
- **Corporate-Owned Personally Enabled (COPE) Mode**: Designed for corporate-owned devices that are used both for work and personal purposes. Allows a work profile to be set up to separate work from personal apps and data. Enables IT to secure or wipe the entire device in cases of loss or theft.

**THE ROLE OF VMWARE WORKSPACE ONE UEM**

VMware Workspace ONE provides a single yet robust solution for managing and supporting any device—from smartphones and laptops to rugged devices and wearables—from one central console. Workspace ONE combines UEM with apps and identity management to enable a complete digital workspace.

VMware Workspace ONE offers a fully integrated solution, providing scalable, extendable management flexibility. It includes device management features and pre-integration with leading identity and app services. The result is a single cockpit that is ideal for organizations that want to support a wide range of devices and applications.

To learn more, visit [www.vmware.com/products/workspace-one.html](http://www.vmware.com/products/workspace-one.html).