EXCLUSIVE ESG GUIDE

Enabling Business Success with Enterprise Mobility

Today, business is being transacted anywhere, any place, at any time, so it's essential to offer your mobile workforce a secure way to access data and information, while protecting your organization's business-critical data.

With the burgeoning trend of bring your own device (BYOD), workers are using a variety of personal and corporate devices (laptops, tablets, and android, iOS, and Windows phones) to access and share files.

IT is charged with ensuring the right people have the right access to the right information at the right time, maintaining application performance, and meeting compliance and government regulations—while simultaneously making sure that nothing will negatively impact a seamless user experience. With this list of real challenges, it's no wonder that your IT organization is looking for a cost-effective solution that provides full control over the corporate environment.

So, as an IT professional, are you prepared to meet your organization's growing workforce mobility demands? Consider:

1. Implementing a solution that enables you to build secure mobile workspaces—one that combines delivery models, centralizes management and security, and supports various devices.

2. Addressing current mobility challenges that center around improved IT control, security, and an enhanced end-user experience.

3. Aligning your organization's go-to-market initiatives with both short-term business goals for simplifying application, desktop, and data deployment, *and* long-term business mobility strategies.

Evolving from a Device-centric Approach to a User-centric One

Let's face it, we're moving from a personal computing (PC) model to a new model that ESG calls the productivity, communication, and security (PCS) model—in the PCS model, a user is associated with a workspace that can be securely accessed from assorted devices and locations.

The ESG PCS model includes:

- **Productivity applications**: Native mobile applications, SaaS, projected legacy applications, and file and data access.

- **Communications and collaboration**: Voice, video, and text options to maintain existing lines of communications, and create new communication and collaboration surfaces for a productive environment.

- **Security controls**: Identity and access management (IAM), enterprise mobility management (EMM), single sign-on (SSO), digital rights management, and machine learning capabilities to recognize threats before *and* as they're happening.

And with this new model, you'll need to rethink how you're going to develop and architect applications for easy, secure user access—on any device—to evolve the endpoint computing strategy from device-centric to user-centric.