SearchEnterpriseDesktop.com
E-Guide

Best practices for introducing tablets in your enterprise

Everyone is buzzing about tablets right now, but how can you tell if this technology makes sense for your organization? This expert e-guide from SearchEnterpriseDesktop.com provides insight into the top reasons why tablets make business sense, including its video and Web conferencing abilities. Learn best practices for securing tablets after adoption. And find out if you can use the same strategy for smartphones and tablets to simplify management and ease security concerns.

Sponsored By:

SearchEnterpriseDesktop.com
E-Guide

Best practices for introducing tablets in your enterprise

Table of Contents

Making a case for tablets in the enterprise: Where they make sense

By Jonathan Hassell, Contributor

The world is buzzing about tablets. These keyboardless handheld devices are large enough to work on for an extended time, but they're also small and light enough to be portable. As the Apple iPad and the Samsung Galaxy start appearing in more consumer hands, you might be wondering what these tablets mean for the enterprise -- and how you should respond when users start clamoring for them.

Where do tablets make sense? At this point in time, you will get the best bang for your organization's buck in three areas: video and Web conferencing, sales applications, and data entry.

Video and Web conferencing

Since tablets provide stunning visuals and a rich media experience in a portable platform, they're ideal for conferencing users. The tiny screens on mobile phones haven't been a big boon for video and Web conferencing, but a 9.7-in. full-color iPad display, for example, makes it much easier to put a face with a name. Combine this display with the ability to share documents and Web sessions, and you have a compelling solution via a simple wireless connection, rather than a bunch of cables, video ports, RGB cords and a nonmobile footprint. Tablets let you conference in your office, in a briefing room, in a coffee shop or almost anywhere else with Wi-Fi.

Sales

Your sales team is already full of mobile veterans. They are always on the road, and they need a conferencing and presentation tool as well as a device that can assist with simple data entry like putting proposals and orders into a customer relationship management (CRM) system. In addition, tablets are attractive to people who spend large swaths of time on planes, and combining a sales tool with a productivity device is a winning mix for sales

and client-service teams. For even more productivity, consider tablets with the 3G chip -- especially useful for road warriors.

Data entry

Users who work with inventory and other specialized applications probably already have specific devices. However, the clerical staffers and workers who deal with back-office data entry, CRM or accounting systems, blogs, profiles or wikis can take advantage of tablets' portability. Obviously, tablets aren't great for dictation, detailed spreadsheet work, or letter or other content creation, but they provide a unique way to manage bits and bytes of information and keep systems updated.

Despite the popularity and potential usefulness of tablets, they're not wholesale desktop replacements. The lack of a physical keyboard prevents many users from getting real work done. Furthermore, current tablets don't run Windows and therefore can't participate in managed network policies such as Group Policy. This makes them difficult to administer and secure.

Regardless, senior staffers in your organization will probably ask you about tablets soon -- if they haven't already. It makes sense for these members of your team to be a "pilot" group so you can have a sense of how tablets will interact with your business' systems and processes.

Over the next year, prepare yourself to answer an onslaught of access and procurement questions from legions of users who see tablets in use in many scenarios in their daily lives. Since the Microsoft tablet seems a long way away, look for tablets that have the best chance of integrating with your existing back-end systems and for tablet operating systems with strong management and security features.

Tablet security: Best practices for the tablet computer onslaught

By Lisa Phifer

Adoption of tablet devices by business users has been astonishingly quick, taking some IT departments by surprise and wondering what to do about tablet security and support. To some extent, tablets can be treated like smartphones with the same mobile operating systems. But tablets are not just big flat smartphones -- they tend to be used differently and thus pose some unique challenges of their own. In the companion to this article, we explored the influx of tablet devices and related mobile security risks in the IT environment. Here we'll discuss how to mitigate those risks.

Leverage smartphone mobile security practices

Companies that rely on corporate-standard phones to ensure security will have more trouble embracing tablets. Employers may procure tablets for specific use cases, but this alone will not address all tablet demands. Instead, IT must facilitate safe business use of many different employee-owned tablets. Companies that are already securing employee-liable smartphones can start by applying smartphone mobile device security policies and practices to tablet security. The most important of these include:

1. **Device lock:** If a tablet is lost or stolen, enabling native device authentication (PIN, password, pattern) can reduce risk of application, data, or connection misuse. All contemporary tablets support this practice, although strength and enforcement vary.
2. **Anti-theft measures:** Many tablets support remote lock or data wipe to stop missing tablets from being misused -- including those owned by former employees. While such measures are readily available for tablets, policies must be defined. For example, workers may be asked to consent to remote wipe and back up their own personal data. Employer use of tablet "find me" services can also raise privacy concerns.
3. **Over-the-air encryption:** All contemporary tablets can secure Web and email with SSL/TLS, Wi-Fi with WPA2, and corporate data with mobile VPN clients. The primary

challenge here for employers is proper configuration and enforcement, as well as protecting credentials and configs to prevent reuse on unauthorized devices.

4. **Stored data protection:** Hardware and mobile OS support for stored data encryption varies. However, self-protecting apps are readily available for tablets, such as email apps that store messages, contacts, and calendars inside encrypted containers. Some employers find self-protecting apps preferable, because they insulate business data from personal data, making it easier to wipe the former without the latter.
5. **Mobile application controls:** Contemporary mobile operating systems employ code signing. data caging, and feature restrictions to deter malware. Nonetheless, many downloaded apps require access to sensitive data and features, and employers may have little or no control over app installation. Centrally-enforced restrictions and blacklists are still emerging for tablets; consider this more of a stretch goal than best practice today.
6. **Anti-malware:** Tablets are not shipped with on-board anti-virus, anti-spam, intrusion detection, or firewall apps. Although such apps are available, adoption has been slow. Instead, many users rely on corporate mail server or mobile operator SMS filters and a naïve hope that AppStore rules stop Trojans. The IT department has plenty of room for improvement here.
7. **Device management:** For visibility, policy configuration, app provisioning, and compliance reporting, employers can centrally manage tablets used for business, no matter who owns them. A minimum practice is Exchange ActiveSync policies -- for example, to deny corporate mail access by unencrypted devices. For more extensive and transparent control, use mobile device management (MDM) software from a vendor such as Afaria, AirWatch, BoxTone, MobileIron, Tangoe, or Zenprise. For example, all of these MDMs can enroll and secure iPads, without relying on iTunes or Exchange.

Adapt to tablet security needs

While these common practices are a good start, tablets do present a few new twists that may require policy customization or practice adaptation. These differences can be subtle. Let's consider a few examples.

- Unlike smartphones, which support cellular voice and SMS texting, many new tablets are available in Wi-Fi-only models. If your smartphone enrollment, remote lock/wipe, or AV update practices depend on SMS, they may not work on tablets running the same mobile OS. Look for measures that can be adapted to work on Wi-Fi-only devices, and realize those Wi-Fi tablets will not be continuously connected to the same degree.

- Smartphones have relatively little visual real estate, but tablets are appealing platforms for remote display and desktop app virtualization. In fact, new Chrome OS tablets won't even run locally-installed apps. If you use VPN clients to secure business communication on smartphones, this may not end up being your preferred approach on tablets.

- On the other hand, tablets are rich media devices, driving users to store presentations, PDF files, podcasts, and videos. Policies that block file attachments or file transfer apps on smartphones may not fly on tablets. Similarly, you are more likely to need to safeguard data beyond email, contacts, and calendars on tablets.

- In order to fully exploit tablet capabilities, mobile operating systems are being refined. For example, early tablets using Android 2.2 cannot run many Marketplace apps well. However, this year's tablets are expected to run Android 3.0 (a.k.a. Honeycomb), which will support for tablet-optimized apps. OS version and device type may therefore have a direct impact on a tablet's app support (including security apps).

- Finally, tablets are not always independent devices. For example, RIM's PlayBook will pair with BlackBerry smartphones for 3G and email. In fact, a PlayBook cannot reach a BlackBerry Enterprise Server (BES) on its own. The upcoming BES 5.0.3 will reportedly manage PlayBooks tethered to BlackBerry smartphones in this manner, but those tablets may end up being managed like a hardware extension of the associated BlackBerry.

These are just a few of the ways in which tablet differences may impact security policies and practices. The bottom line: Reuse what you can from the smartphone world, focusing on techniques that worked well for employee-liable devices. But don't fall into the trap of assuming all tablets can be secured just like their smartphone siblings. Take a hard look at how each tablet will be used, and adapt your tablet security best practices to fit.

About CTL

Founded in 1989, CTL™ designs and manufactures computer products including desktop and mobile workstations, LED Monitors, and high performance servers.

CTL's brands include the popular 2go™ PC and Nexus® Electronics. Headquartered in Portland, Oregon with offices in Asia, CTL and their OEM partners supply North American consumers, government agencies, and many of the most recognized corporate brands.