White Paper

DLP for Tablets

An Intelligent Security Decision

By Jon Oltsik, Senior Principal Analyst

November, 2011

This ESG White Paper was commissioned by Symantec and is distributed under license from ESG.

Contents

Executive Summary 3

iPads are Everywhere 3

Tablet Security Remains Challenging..5

Which Data Security Controls Are Best?..5

DLP for Tablets..6

Symantec DLP Provides an Elegant Tablet Solution..7

The Bigger Truth 7

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.

Executive Summary

Given its ubiquity, it's hard to believe that the Apple iPad has only been on the market for 18 months. Consumers love these devices, but they are also sprouting like weeds in the commercial sector as they enable new types of business processes and applications.

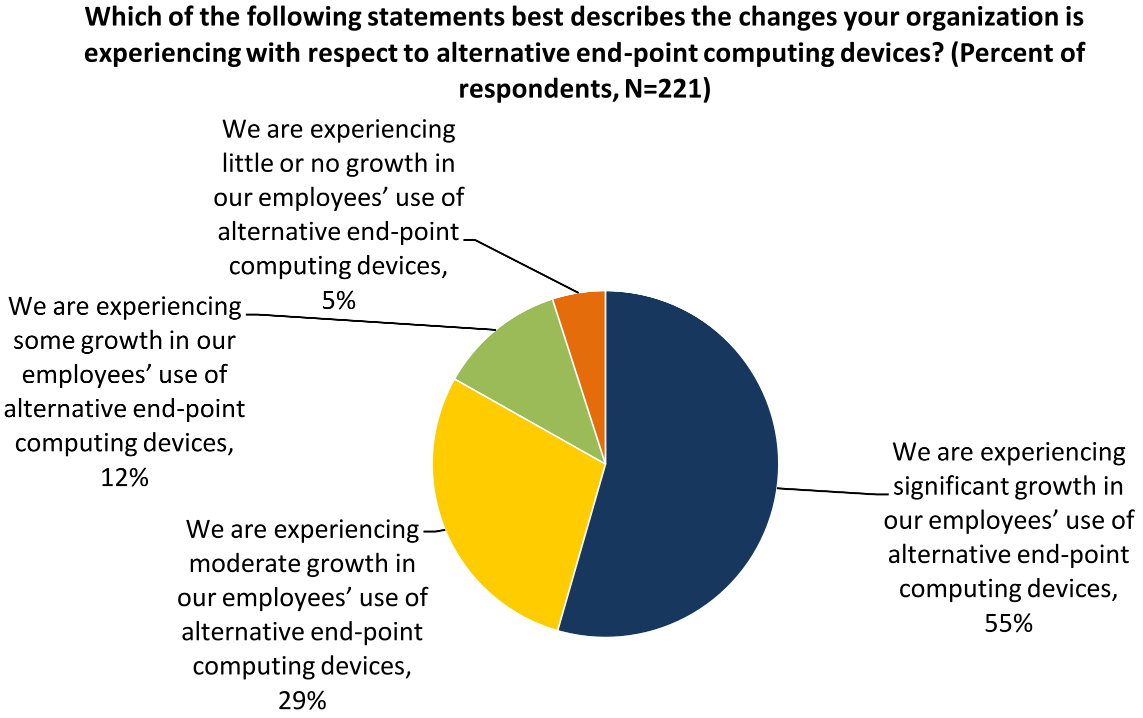
As tablet computers become more and more pervasive, will their presence increase IT risk? In other words, where does tablet security fit into CIO's implementation plans? This report concludes:

- **Employees access sensitive data with tablets and other mobile devices.** ESG research indicates that many users access company confidential data, customer data, and regulated data via an army of mobile devices. A lack of security controls will inevitably lead to some highly publicized disclosed data breaches or routine regulatory compliance violations.
- **CISOs are leaning toward data security controls for tablets.** Large corporations may install endpoint security software controls on tablets over time, but in the near-term, security executives have issued a clear directive around data security.
- **DLP for tablets is the best initial fit.** DLP tools have oversight over users, devices, and data. By tracking all three parameters, these tools can execute granular security policy enforcement decisions, making them extremely flexible and effective. The best DLP for tablet suites will give users the freedom to access corporate and personal data and applications, align device-centric and enterprise policy management and enforcement, and provide central command-and-control and reporting.

iPads are Everywhere

It seems like a lifetime ago that large organizations standardized on Blackberry devices for mobile computing. This all changed in early 2007 with the introduction of the iPhone and then again in April 2010 when the iPad made its debut. By the March 2011 release of the iPad 2, Apple had already sold more than 15 million iPad devices. This was not just a consumer phenomenon: according to Datamation, the iPad penetrated 50% of the Fortune 100 companies. And while iPad use is growing, many organizations are also adopting Android tablets and other mobile devices as well. ESG research data also points to tremendous growth here: 55% of IT professionals are experiencing "significant growth" in their use of alternative endpoint devices, primarily iPads and other types of tablet computers (see Figure 1).

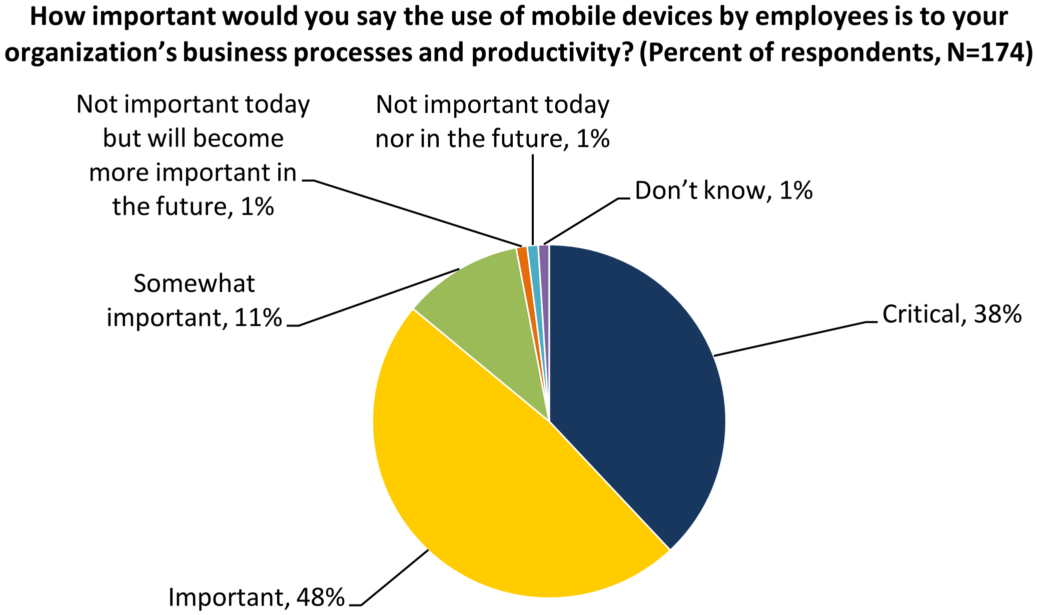
Figure 1. Alternative Endpoint Device Growth



Source: Enterprise Strategy Group, 2011.

At first, tablets were brought in by executives and marketing managers, but their popularity has been driven an avalanche of new applications and use cases. Health care facilities are embracing tablets for pharmacy applications and emergency services. Financial services firms are rolling out tablet applications for account management and high-value customer services. Retailers are looking at tablets for point-of-sales promotions and rapid check-out, and many universities are considering tablets as an alternative to physical books. Little wonder, then, that 86% of large organizations now consider mobile devices like tablets as either "important" or "critical" to business processes and productivity (see Figure 2).

Figure 2. Mobile Devices Are Business-critical



Source: Enterprise Strategy Group, 2011.

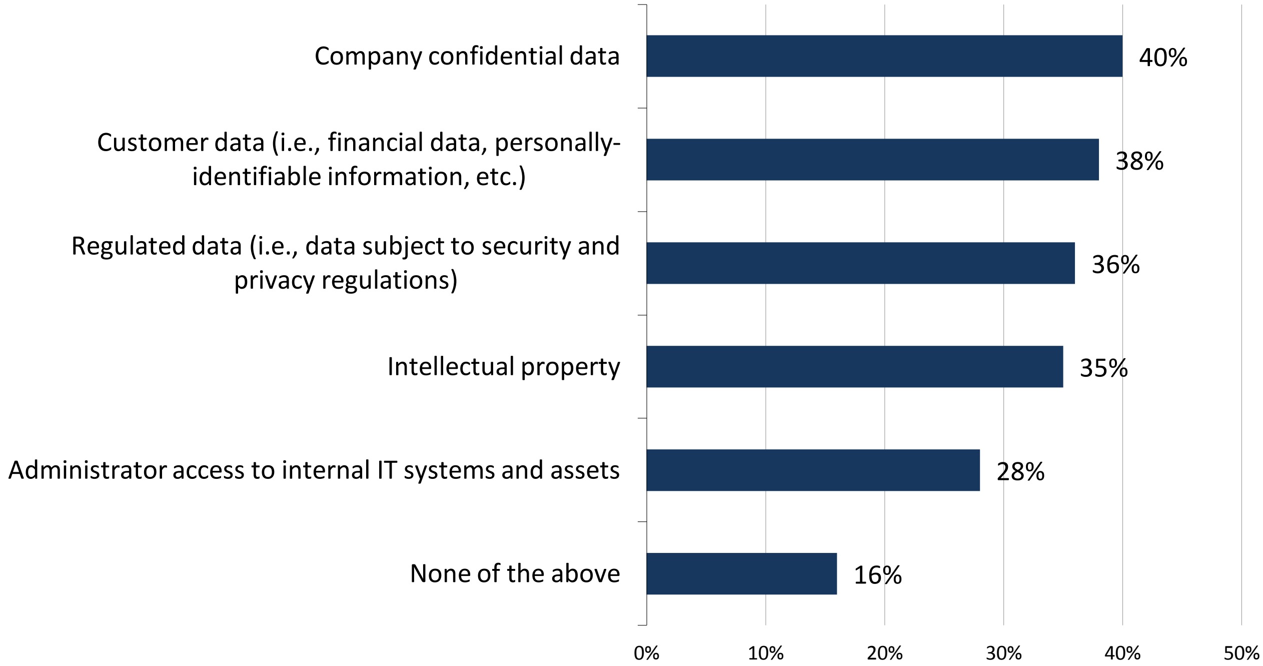
Tablet Security Remains Challenging

In spite of overwhelming popularity and demonstrable value, CISOs continue to look at tablets with trepidation and for obvious reasons. Tablets and mobile devices are hyper-connected devices able to receive and send information with a finger swipe. Users can send and receive email from corporate and personal accounts, upload information to cloud services, and send files to social networking sites. When the device is populated with sensitive corporate data, it only takes one careless action to leak valuable information via any of these channels. According to industry statistics, the majority of data loss is generated by well-meaning insiders using standard information sharing tools (email, web upload, etc.).

Security managers are also concerned about tablets accessing sensitive data. According to ESG research, employees regularly access, retrieve, or store many types of sensitive data including company confidential data, customer data, and regulated data on mobile devices like tablets (see Figure 3).

Figure 3. Employees Access Sensitive Data from Mobile Devices like Tablets

In your organization, can an employee access, receive, or store any of the following on their mobile device? (Percent of respondents, N=174, multiple responses accepted)



Source: Enterprise Strategy Group, 2011.

Tablet users with access to sensitive data represent a security vulnerability. They could easily violate security policies by leaking sensitive data from their tablets via corporate/personal email, Twitter, Facebook, Dropbox, or a host of other Internet applications. CISOs recognize that a data breach is a data breach regardless of the device that caused it, so tablet-based security risks must be addressed as soon as possible.

Which Data Security Controls Are Best?

Given the rapid growth of tablets in the commercial market, many security technology vendors are pitching a multitude of data security products. Unfortunately, most of these are incomplete solutions offering only partial protection (see Table 1).

Table 1. Mobile Data Security Technologies and Their Limitations

Data Security Technology for Tablets	Use Case	Limitation
Data encryption	Uses cryptographic algorithms to protect the confidentiality and integrity of data stored on tablets.	Does not prevent a violation of acceptable use policies by an authorized user.
Remote wiping	Used to delete data when a tablet is lost or stolen.	Does not prevent a violation of acceptable use policies by an authorized user.
Sandboxing/compartmentalization	Used to create a secure work partition within a tablet.	Can interfere with native tablet functionality. Can be defeated by user workarounds. Does not prevent a violation of acceptable use policies by an authorized user
Reverse proxy	Used to block sensitive data traffic flowing to and from tablets across networks.	Can disrupt business processes and impact user productivity.

Source: Enterprise Strategy Group, 2011.

DLP for Tablets

Few organizations have the time or money to layer multiple data security solutions on the growing army of employee tablets. This begs the question: Is there one data security solution available that delivers strong security, operations, and business benefits? Yes. DLP solutions designed specifically for tablets and other tablets may provide the best initial protection because:

- **DLP can enforce acceptable use policies.** Employees have different access privileges associated with sensitive data based upon their roles and responsibilities. DLP can help here by enforcing acceptable use policies for tablets granularly. In this way, DLP can be used to secure business processes, not just devices and data.
- **DLP can provide real-time protection across common corporate and web applications.** CISOs believe that sensitive data leakage from tablets is most likely to occur via corporate/personal email, web-based services, and Internet applications. DLP can be used to recognize sensitive content and approved applications, and then align these with corporate security policies.
- **Many DLP deployments are anchored to the network.** Devices like tablets are intrinsically network devices for access to web applications and services via HTTP/HTTPS as well as WiFi and 3G/4G. Leading DLP network gateways can be tuned to recognize tablet traffic, inspect network payloads, and then enforce policies. It may be permissible to use Dropbox to move sensitive data to corporate Windows PC with strong endpoint security safeguards, but large organizations may want to enforce security policies blocking tablets from using this type of service.

DLP solutions tend to act as a nexus of sensitive data, users, and devices. With oversight in these three areas, they offer lots of security and business flexibility—a perfect combination for iPads and other types of mobile devices.

Symantec DLP Provides an Elegant Tablet Solution

Symantec has been an enterprise DLP leader since its 2007 acquisition of Vontu, and the company recently extended its DLP footprint to include mobile devices. This makes an attractive combination for large organizations as it aligns enterprise and device-specific controls by:

- **Offering a single iPad/iPhone security agent as a security foundation.** To align strong security with iOS user requirements for minimal disruption, Symantec's DLP solution relies on routing traffic from the device to a network-based DLP server for inspection. To enforce this at all times, Symantec relies on native iOS capabilities and the Symantec Mobile Management agent that monitors the enforcement of VPN settings. In the future, Symantec will pivot off this agent, provide additional security options, and offer common iOS security suites.
- **Integrating with Symantec DLP.** Unlike standalone tablet security products, Symantec Data Loss Prevention for Mobile ties into existing Symantec DLP dashboards, command-and-control consoles, policy management, and reporting.
- **Strong roadmap.** Look for Symantec to enhance its tablet offerings with device management, data encryption, certificate management, and anti-malware capabilities. Symantec will also support alternative mobile platforms, like Google Android, in common tablet security and device management suites.

The Bigger Truth

The iPad has seen great success, but the tablet and mobile device revolution is just getting started. Since business managers see boundless potential, CISOs need to wrap their arms around risk management and security controls as soon as possible. Many security managers believe that DLP is the best logical first step as it not only offers data security, but also aligns with security policies and regulatory compliance requirements.

Symantec understands this alignment and recently introduced its initial tablet security product, Symantec Data Loss Prevention for Mobile. Smart move as Symantec Data Loss Prevention for Mobile provides device-specific controls and also integrates with Symantec Data Loss Prevention for protection of sensitive data across the enterprise. As such, smart CISOs should consider Symantec for all their DLP needs.

Enterprise Strategy Group | **Getting to the bigger truth.**