SOLUTIONS FOR A MOBILE WORKFORCE

How to Gain Visibility and Control of Your Mobile Users and their Personal Devices

INTRODUCTION

In the workplace, most employees prefer to use their own mobile device – one that they are familiar with and have selected as opposed to one that is provided to them by their employer. In fact, it was estimated that last year nearly 70% of all smartphones used for business were owned by workers rather than the company[1]. However, this usage of personal devices by people at work leaves organizations vulnerable to significant security risks.

The primary concerns are: 1) how to control and monitor just corporate data on an employee's device and 2) how to maintain the appropriate security controls, such as malware protection and data loss prevention (DLP), on the smartphone. To address these concerns, many organizations are establishing very specific bring-your-own-device (BYOD) policies that must be followed by employees using their personal devices.

This consumerization of the workplace is a two-way street. Many employees who use enterprise-owned devices act as if it's their own. For example, they will install favorite entertainment and game apps, which could be a serious threat to organizational data.

Policies on what applications can be installed on these devices must be spelled out. Reporting and enforcement is also required. One key element to strong mobile security that's often overlooked is the educating of the end user so he or she can be a dedicated team player in safeguarding the mobile device.

PRIVACY AND DATA LOSS PREVENTION

An individual's smartphone can have tremendous amount of information on it – both personal and business. One's calendar, contacts, browsing history, location history, email, and more can all be (and often is) stored within the memory of the device. Or the device can provide an easy online gateway to all of this information and more.

Organizations are struggling to determine what level of privacy is acceptable on mobile devices. Many are developing strict policies around likely scenarios where privacy could be invaded or data could be lost or stolen. Then whenever and wherever possible, they will enforce those policies via technology.

The preferred policy in many cases is to simply wipe all data off of a misplaced, lost, or stolen device. The theory is that it's better to lose everything on the device and have to re-populate if it's found, rather than risk facing compliance penalties or having the data accessed and misused by cyber criminals. Another possible tool is the use of enforceable encryption.

Mobile data and file management is also an issue for organizations, especially in that mobile devices are being readily used to access cloud data storage. Employees want to sync and share files and to have the ability to collaborate with others on them. They want an intuitive, holistic method for managing their content libraries.

Email is often the first priority, but the need goes well beyond that in terms of cloud data storage. Organizations are beginning to expand their data protection capabilities using encryption, data loss prevention, and secure access controls to data stores.

1 IDC

CORRUPTED APPLICATIONS COULD LEAD TO MOBILE MALWARE

Mobile malware is on the rise and poses a threat to the security posture of mobile devices. Mobile malware can be used to steal data directly from the phone or be used to infect other network components. Much of the malware is introduced from corrupted applications.

Currently, a large majority of mobile malware comes from the Android OS environment. It is made easy by the consumer conditioned behaviors of quickly and easily downloading apps and accepting permissions. As Android devices take on a bigger role in Enterprises[2], it is fairly clear that these "consumer bad habits" will have a direct and detrimental effect on enterprise assets. To battle this threat, many organizations only allow the downloading of applications from approved locations.

Many organizations are finding Trend Micro mobile solutions are what they need to make BYOD work for them.

Trend Micro mobile solutions are part of our Complete User Protection strategy, which is multi-layer security that provides the broadest range of interconnected threat and data protection across endpoints, email and collaboration, web, and mobile devices.

TREND MICRO MOBILE SOLUTIONS

Trend Micro mobile solutions allow IT managers to have visibility and control across all aspects of their end users' digital lives. A single console, directory, and policy can be applied to end users and processes and can be streamlined to make BYOD simple to embrace. You can deploy and manage mobile devices, mobile apps, corporate resources, and corporate data while respecting user privacy and not encumbering employees with proprietary software and processes.

Currently, Trend Mobile solutions consist of two industry-leading products: 1) **Mobile Security** and 2) **SafeSync for Enterprise**.

Trend Micro Mobile Security is a well-integrated mobility platform that provides Mobile Enterprise Management (MEM) functionality and the necessary tools for:

- BYOD device enrollment and user provisioning
  - Corporate Policy
  - VPN settings and enrollment
  - Secure corporate WiFi settings and enrollment
  - Data protection policies
- Mobile Device Management (MDM)
- Mobile Application Management
- Mobile Application Reputation Services
- Android Antivirus

SafeSync for Enterprise is a secure enterprise sync and share platform that provides a secure way for employees to access corporate data on mobile devices. It features:

- Secure sync and share for corporate information
- Mobile DLP to ensure compliance
- Persistent file encryption
- Numerous data protection controls to protect corporate information

2 IDC expects that in 2016, Android will make up 60% of all employee-liable smartphones and one-third of corporate smartphones.

Key Benefits

- Get a holistic view of user security
- Enroll mobile devices easily and provide access to corporate infrastructure, data, and applications using mobile device management
- Maintain and update user devices with visibility
- Deploy, allow, disallow user mobile apps
- Check the validity and risk of mobile apps
- Ensure that mobile devices remain healthy

ANSWERING EMPLOYEE COMPLAINTS ABOUT WHERE AND WHEN THEY CAN WORK

Supporting Features:

- Enabling employees to work securely from mobile apps and devices through a complete mobile suite of products
- Deploying mobile security alongside traditional endpoint solutions from Trend Micro is simple, low-cost, and fast

Trend Micro Mobile Security solutions simplify user security and management by combining mobility management and security features with all end user security management. This comprehensive mobile offering features mobile user management, application controls, data protection features and protection from mobile threats.

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide.

For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud

©2014 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.
[OV01_Mobile_Security_Sub_Solution_Overview_140414US]