Consumerization of IT

Trend Micro Technical Brief

There are **three important areas** to consider when planning your security and management strategy for the widespread business use of consumer devices

1. How can I protect corporate data?
2. How can I ensure the device is secure and safe to access my networks, applications and data?
3. How can I minimise the cost and effort associated with managing these devices?

In this paper, we explore the principles behind each of these three areas and discuss how you can apply these principles to your organisation.

"By 2014, 90% of organisations will support corporate applications on personal devices."[1]

You would be hard-pushed to find an organisation that is not aware of one of the most significant trends to impact IT over the last few years, and the potential opportunities such as business growth and agility, increased productivity and customer satisfaction are now well-understood. But this trend introduces risks and challenges that can be a barrier to an organisation's ability to embrace consumerization and fully unlock this opportunity.

The following three challenges are important areas to consider when planning your strategy for the widespread business use of consumer devices. This paper will address each area and outline specific guidance and examples of different approaches.

1 **How can I protect corporate data?**
We explore the policies and tools you can implement for limiting data loss incidents

2 **How can I ensure the device is secure and safe to access my networks, applications and data?**
We look at the device configurations and protection you can deploy to prevent malware and reduce the risk of compromised devices

3 **How can I minimise the cost and effort associated with managing these devices?**
We consider how you can centralise visibility and control of device management and security to relieve the cost and resource burden.

"My advice for organisations facing an increasingly consumerized IT world is to realise that Consumerization is happening and they can't stop it - and in fact they shouldn't. I strongly recommend our customers to embrace Consumerization to unlock its business potential."

Cesare Garlati, Sr. Director, Consumerization, Trend Micro

OLD SCHOOL VERSUS NEW WAVE

For the purpose of this paper, we will draw on comparisons between the traditional company-owned laptop and the new breed of mobile devices infiltrating the organisation – employee-owned smart phones, ultrabooks and tablets, to name but a few. This is a useful comparison to make since increasingly, employees want to use this new class of device to perform many of the same tasks that were previously carried out on the humble company laptop. And for the same reason, IT departments increasingly want to find ways to perform centralised security management with the same degree of control that they had with laptops.

PROTECTING THE DATA

"Who knows what could happen when our corporate data is on all of these personal devices?"

Aerospace company, US Fortune 500[2]

What measures do you take to protect data on company-owned laptops? It sounds obvious, but this goes some way to explaining why all of the different methods of protection are necessary for mobile devices, too. Crucially, this area considers what policies and tools should be implemented in order to limit data loss incidents.

Company-owned laptops typically have domain-based users

Amongst other functions, the attributes of a user's account controls the password policy in order for the user to access the machine, and then enforce the level of access that user has once authenticated onto their machine. In the majority of cases, a machine build is locked down so that the end user doesn't have the required administrative rights to install or remove software.

In addition, Fine Grained Group Policy can be applied to control what the user can or cannot do on their machine; Password quality rules can also be applied. However, the majority of popular employee-owned mobile devices were never developed with the corporate infrastructure in mind. For this reason, the vast majority of those fine grained controls that can be carried out on a laptop don't translate for usage on a mobile device, but must still be considered an essential security policy.

Company-owned laptops increasingly have full disk encryption

Many organisations now deploy full disk encryption to all company-owned laptops to prevent unauthorised access and data breaches, especially with ever-tightening compliance mandates such as the Data Protection Act.

1 Gartner 2011

2 Trend Micro Consumerization research, June 2011. Survey of 200 IT decision-makers for organizations of 1000+ users.

However, this approach can be difficult to apply to the range of mobile devices currently being bought into the workplace. For instance, not only does the level of encryption available vary from device to device, but for some, it's not even possible to install a dedicated encryption agent (as is currently the case with Apple and Blackberry devices). Compound this with the fact that some mobile device will be employee-owned, and you end up with a more complex challenge when it comes to device encryption.

Company-owned laptops can be remotely wiped or locked
A typical feature of a laptop's encryption agent is the ability to perform a remote wipe of the machine, or to remotely lock it in the event that it is lost or stolen.

The baseline measures to ensure that corporate data on employee and company-owned devices is protected from theft and loss should include enforcing the use of passwords, remotely locking and wiping devices. These measures are vital within the context of a basic mobile security policy and there are several reasons behind this. First, smartphones and tablets are more likely to be lost or stolen than a laptop. Secondly, it doesn't matter if the mobile device in question is an employee-owned or company-owned device – the fact is that the device is capable of storing potentially valuable or sensitive organisational data and ensuring that this data does not fall into the wrong hands is vital. Thirdly, device encryption capabilities vary between platforms. And finally, the connected nature of mobile devices make the enforcing of a remote device lock or wipe a simple and quick task for an administrator to perform.

The Trend Micro solution to protecting corporate data
Trend Micro provides a solution that bridges the security shortfalls outlined above.

Trend Micro Mobile Security enforces policies for data access and protection by enforcing the use of passwords and encrypting data. This solution also offers "Feature Lock" – the ability to disable certain security relevant features on mobile devices such as cameras, Bluetooth and SD card reader. Combined with location awareness, these features can even be disabled according to device location, for instance, disabling a camera in a production site.

Finally, the vital ability to remotely lock and remove data from lost or stolen devices can also be performed by Trend Micro Mobile Security.

SECURING THE DEVICE

Protecting the data through policy enforcement is undoubtedly the cornerstone of a good security policy, but this only mitigates a proportion of the risks associated with mobile devices. Mobile devices are increasingly being targeted through various methods, such as tricking users into downloading and installing malicious applications.

The security posture of the major platforms differs greatly, with Android being seen as the most open platform, and as a result, the least regulated and most at risk of infection. We're seeing more and more scams on the Android Market, especially from developers that use popular app names to trick users into downloading fake ones. In one week alone, 37 of these types of "fan apps" – malware posing as real games – were identified.

Company-owned laptops can be controlled through Group Policy
Although it is unusual for an organisation to prescribe an exact list of software applications that can or cannot be installed on every company-owned laptop, Group Policy can provide protection through the ability to deny users the right to install software on their own machine.

By contrast, application control is performed in a different way with smart phones, and typically requires functionality that maintains applications blacklists. If a user installs an app that is on the blacklist, this will generate an administrator notification.

Company-owned laptops have virus and web threat protection
A company-owned laptop will undoubtedly have some kind of AV installed to provide protection against viruses, spyware, spam, phishing attacks and other web threats.

The same approach is essential on employee-owned mobile devices. They too need to be able to detect and block malicious data files, and with the widespread use of smart phones for accessing email and social networks, it is critical that they have web protection in order to block access to malicious web content and data-stealing sites. They are also more susceptible to infection from malicious applications for the platform security challenges highlighted above.

Company-owned laptops don't take calls
An increasingly common threat on mobile devices is that of phone call or SMS based spam. This can result in a deluge of "nuisance" calls or text messages, which can not only be annoying, but also dangerous as this can be used as a mechanism to deliver malicious URLs.

Tools that allow the end user to manage their own blocked caller and SMS lists can be an important control against these kinds of risks.

The final control necessary to provide the device with security controls on a par with a company-owned laptop is the ability to control or lock out certain applications and device functions. A simple example is an SD card in a phone; it is removable storage that can be used to take company data offsite in much the same way as with a USB key. Some operating systems will only allow you to use on-phone storage, even though they have an SD slot, and if you have the ability to enforce that, then it is one more way to reduce the risk of data loss.

The Trend Micro solution to securing the device

Trend Micro Mobile Security ensures the correct device configurations and protection to prevent malware and reduce the risk of compromised devices.

Leveraging industry-leading, cloud-based threat intelligence from the Trend Micro Smart Protection Network™, the solution detects and blocks malicious applications and data files, safeguards against accessing malicious web content and sites, detects attacks on the device via network applications, ports and services and enforces passwords when powering on devices. Underpinning this approach is the ability for Trend Micro to block threats at the earliest opportunity, so the solution also includes Web Threat Detection, which leverages Trend Micro's global threat research network to provide Web Reputation data with regards to currently malicious URLs. This means that mobile device users can be blocked from accessing potentially unsafe URLs that harbour malicious code.

Trend Micro Mobile Security has the ability to maintain App blacklists for iOS and Android, which generates an automated notification to a designated administrator in the event that a user installs a blacklisted application. The solution also Security provides the administrator with centralised control to lock out functions such as the camera, GPS or SD card storage, further helping to control the device usage and limit data egress.

The Trend Micro Mobile Security agent even provides granular functionality that allows the end user to manage their own blocked caller and blocked SMS id lists. This enables call and message filtering and logging, plus monitoring, blocking and logging calls, SMS and MMS messages sent to and from the device.

MANAGING THE DEVICE

Providing security controls at the device level is vital, but if there is no centralised provisioning, control and management, then it is difficult to maintain a defined security policy.

"My executives all showed up with iPads, what do I do now?"

Financial services firm, US Fortune 500

Company-owned laptops are easy to provision and manage

When a new starter joins or when an employee needs to replace an old laptop, the process to provision a new laptop is usually straightforward. A typical process involves a laptop being ordered from a pre-approved list and an image being installed with the required corporate programs such as Office and Adobe. The serial number, model of laptop and the assigned employee for the laptop is recorded and the user account created and configured. Finally, Group Policies are applied when the machine is added to the domain.

Whilst employee-owned tablets and smart phones can be identified relatively easily and can even be forced to use a different network to give internet access to pick up email, the problem is, of course, security... It is very difficult to impose IT policy on employee-owned laptops and devices and responsibility for keeping up-to-date with patches is shifted to the employee.

The Trend Micro solution to managing the device

Trend Micro provides a holistic, all-endpoints approach through a single, unified management console for PCs, Mac, Linux, Android, iOS, Blackberry, WinMobile and Symbian. This provides centralised visibility and control of device management and security, which increases management efficiency and reduces costs.

Trend Micro Mobile Security provides a centralised platform that allows administrators to find and enrol mobile devices and to provision them with Trend mobile device agent functionality where appropriate. Remote control in terms of making security policy changes on the fly is possible; this is particularly important to administrators in the event of a mobile device being reported as stolen or lost, and in the worst case scenario, the administrator can use Remote Control to lock or wipe the device.

Trend Micro Mobile Security also contains an asset tracking component; if the device has GPS capability, it can use this to report back its geographical position to the customer's Trend Micro central server. This allows the administrator to plot the physical position of the device on Google Maps.

TREND MICRO™

Securing Your Journey to the Cloud

In summary, a key step to unlocking the potential is to deploy appropriate IT tools that are specifically designed to secure and manage consumer technology in the enterprise. It is only this combination of mobile device management and security functionality that is capable of effectively enabling organisations to securely embrace the consumerization of IT.

Secondly, with the combined impact of the speed of growth of the mobile space and the rapidly evolving threat landscape, organisations should consider four aspects when prioritising security and management tools: solutions with a security framework based on context-aware security; solutions built on flexible architectures as opposed to point products; solutions that are flexible enough to accommodate diverse requirements; future-proof solutions that allow organisations to evolve their security.

Trend Micro believes that the answer to managing this situation is to stop thinking about individual devices and take a holistic, all-endpoints-approach that enables organisations to manage mobile devices and traditional PCs together. The Trend Micro solution to managing and securing both the device and its data is an integrated mobile device management and security solution within a security framework that spans physical and virtual endpoints, PC and non-PC devices. And because mobile management and security is integrated into our endpoint security offering, our solution can become your command centre for all endpoint related security and management tasks – regardless of the device or operating system.

"Rather than resist it, organisations should embrace Consumerization to unlock its business potential. This requires a strategic approach, flexible policies and appropriate security and management tools."

Cesare Garlati, Sr. Director, Consumerization, Trend Micro

Find out more about Trend Micro's approach to the consumerization of IT.

Call 01628 400552

Visit www.trendmicro.co.uk/consumerization

www.trendmicro.co.uk

©2012 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs 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.

Trend Micro (UK) Limited, a Limited Liability Company. Registered in England No. 3698292.
Registered Office: Pacific House, Third Avenue, Globe Business Park, Marlow, Bucks, SL7 1YL