WHITE PAPER

Embracing Consumerization with Confidence

Sponsored by: Trend Micro

Stacy K. Crook

December 2011

EXECUTIVE SUMMARY

Organizations need to start thinking about the consumerization of IT in a more strategic way. Specifically:

- **Consumerization is a powerfully disruptive trend.** Major technology movements such as cloud-based services, virtualization, and social networking have all contributed to the powerful paradigm shift that is now impacting organizations of all sizes. These technologies, in tandem with mobile device proliferation, afford end users the freedom to collaborate and be productive anytime and anywhere. Along with these benefits, however, consumerization has a highly disruptive impact on IT, shifting the balance of power from centralized IT decision making to a decentralized end-user base. This change usually results in an uneasy loss of visibility and control for IT.

- **Companies need to think about consumerization holistically.** While many enterprises today have developed a formal "bring your own device" (BYOD) policy, most have not taken the time to evaluate how user behavior with these devices impacts their infrastructure needs. Although the first sign of consumerization may be the need to support new device types, this is just the beginning. As an end user yourself, think of all the ways you interact with your personal device and realize that your employees are all doing the same things with theirs, but without the knowledge of the potential security risks they may be creating. For instance, many will not think twice about storing and syncing corporate data in consumer apps and clouds. Companies must consider not only how they will provide secure access to corporate data and apps but also how they will protect that information once it's on an employee-owned device.

- **Trend Micro's approach.** With respect to consumerization, Trend Micro's goal is to help organizations build a holistic, balanced mobile security and management framework that meets the needs of each company's unique environment. Trend Micro has organized its solutions for consumerization across a spectrum that ranges from high end-user freedom to high company control while striking the balance in between. These products support three main pillars: helping IT regain visibility and control, allowing IT to share corporate content with confidence, and helping IT ensure that data is protected anywhere.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

IN THIS WHITE PAPER

In this white paper, we explore the key converging market dynamics driving the consumerization of IT. We then examine some of the significant opportunities and challenges that this rapidly evolving trend represents. Next, we introduce Trend Micro, a company looking to help organizations build a holistic mobile security and management framework that allows them to embrace the consumerization of IT. Finally, we offer recommendations for companies to consider when developing their own strategies for embracing consumerization.

SITUATION OVERVIEW

Consumerization: Powerful Disruption

Few current IT trends have been as swiftly disruptive as consumerization. Major technology movements such as cloud-based services, virtualization, and social networking have all contributed to this powerful paradigm shift that is now impacting organizations of all sizes. When the speed at which mobile device proliferation has taken place over the past couple of years is included, a perfect storm has developed that offers end users the freedom to collaborate and be productive from anywhere and at any time. Thus, consumerization represents a unique opportunity for progressive companies to harness this collective power to their advantage. Along with these benefits, however, this trend also gives rise to new challenges related to visibility, data access, and data protection that require organizations to reassess their existing security and management strategy.

The consumerization of IT is such a powerful trend not only because of the speed at which it is moving but also because of the disruptive impact it has on the IT organization. In the past, decisions were made within IT and end users had to abide by them; today, consumerization represents a shift in the core power balance between these two parties. And as that balance tips more toward end-user freedom, the result is typically a severe loss of visibility and control for IT. Although end users would ideally like to be able to use whatever devices and applications they want to conduct business, the fact remains that IT needs a way to ensure that corporate data and networks are secure. No matter what computing shifts take place, security must remain at the core of enablement.

Key Issues to Consider for a BYOD Strategy

At first, consumer mobile devices made their way into the enterprise via the "back door," but today we are at an inflection point where many enterprises have developed a formal BYOD policy. By 2015, in fact, IDC expects that the majority of business use smartphones worldwide will be employee liable (55%) versus corporate liable (45%) (see *IDC Worldwide Business Use Smartphone 2011–2015 Forecast and Analysis*, IDC #230311, September 2011). Despite this trend, many companies have not taken the time to holistically evaluate how user behavior with these devices impacts their infrastructure needs. Today, organizations may believe the primary issue with consumerization is that they need a way to support and manage new device types, such as iOS or Android smartphones and tablets. However, thinking about

consumerization from a device-only perspective does not properly prepare organizations for all the other potential security risks this model represents.

To take an integrated approach to the problem, companies must consider all the different activities end users engage in with their devices. The typical consumer downloads many types of applications from public app stores, which may or may not be infected with malware. Users are downloading content/file access applications such as Dropbox or Evernote where they can easily house corporate content if they so choose. In addition, iOS 5 users can now sync and store all of their devices' data in Apple's iCloud. In both instances, your corporate data is now sitting in another company's cloud. In addition, many end users do not bother to password enable their devices. As a result, your corporate data is potentially sitting both in an app on an unsecured device and in a cloud somewhere where you have no control. Your more technically savvy end users are even "jailbreaking" their devices just for fun — and the list goes on.

Unfortunately, these scenarios are only scratching the surface of possible security risks that arise from employee-owned devices. Thus, it is clear that companies must consider a number of issues and challenges when developing a BYOD strategy. Areas of consideration include the following:

- **Device management for visibility and control.** Do you know how many and which devices are accessing your network? Have you set up policies to prevent jailbroken/rooted or noncompliant devices from accessing your network? Can you ensure that the latest versions of software or OS patches are implemented across all the device types accessing your network?

- **Protection of sensitive data.** How will you ensure that employees are following secure practices such as password protecting and encrypting data on their devices? Do you have a way to remotely lock/wipe devices if they are lost or stolen? When your employees are downloading potentially infected consumer mobile applications on the same device as corporate applications, how will you ensure that all your sensitive data (in apps and unstructured content, media, etc.) is protected from malware? How can you ensure that end users are not synchronizing and storing your corporate data in non-IT-managed applications or clouds?

- **Security across application types.** Do you have security implemented for native applications, Web applications, and virtualized desktops/applications? With HTML5, Web applications will grow in relevance for the enterprise. Security for browsers on all devices is imperative. How do you avoid data loss from employees cutting and pasting corporate information into consumer apps such as personal email or Dropbox?

CHALLENGES/OPPORTUNITIES

The solution types available in the market today to address the aforementioned issues typically fall under the categories of mobile device management (MDM) and mobile security. While the two markets are closely intertwined, key features of MDM such as device provisioning and configuration, asset management, software

distribution, remote control, and reporting separate an MDM solution from a standalone mobile security solution. However, all MDM solutions also contain security features. These features range in sophistication from vendor to vendor, but at a base level, they will typically include mobile security and vulnerability management (MSVM) capabilities such as remote wipe/lock and policy management. From IDC's perspective, the mobile security market also includes several other subsegments, such as mobile threat management (antimalware, antispam, firewall, IDS), mobile IPC (encryption and data loss prevention), mobile VPN (VPN optimized for wireless), and mobile identity and access management (MIAM).

Because dealing with consumerization is a new, yet very real problem and creates myriad issues, organizations are faced with many vendors trying to sell them products to solve the problem from one perspective or another. The growing convergence between MDM and mobile security solutions tends to add to the confusion. Thus, one of the key challenges for end users today is dealing with the fragmentation in the market. In a sea of vendors claiming to have the solution to consumerization, it can be difficult for organizations to know what or which solutions are the best fit — or who can serve as a trusted partner to help them figure it out.

Despite this complexity in the market, consumerization is a tangible issue for most IT organizations today, and there is a genuine need for solutions that address their specific concerns. Companies that choose to embrace consumerization improve their risk posture because they have taken steps to address potential points of vulnerability instead of burying their heads in the sand. In addition, organizations that allow employees the freedom to work with the technology they are most comfortable with tend to have more satisfied employees while also enjoying the additional advantage of cost savings. Thus, there is a huge opportunity for companies that can offer real solutions to the pain points IT is experiencing today with regard to loss of visibility, data protection, and secure applications/file sharing.

INTRODUCING TREND MICRO

Founded in 1988 and headquartered in Tokyo, Japan, Trend Micro is one of the world's largest vendors of endpoint, messaging, and Web security technologies. The company provides a broad suite of solutions that secure desktops, servers, and mobile devices across physical, virtual, and cloud computing environments. With respect to consumerization, Trend Micro's goal is to help organizations build a holistic, balanced mobile security and management framework that meets the needs of each company's unique environment.

It is apparent that consumerization represents a shift in the power balance between IT and end users. However, how far that balance tips in either direction will ultimately have to be decided by each individual organization. While some companies may feel comfortable allowing end users a good deal of freedom, others are tied to compliance and privacy mandates that require IT to assume a greater degree of company control.

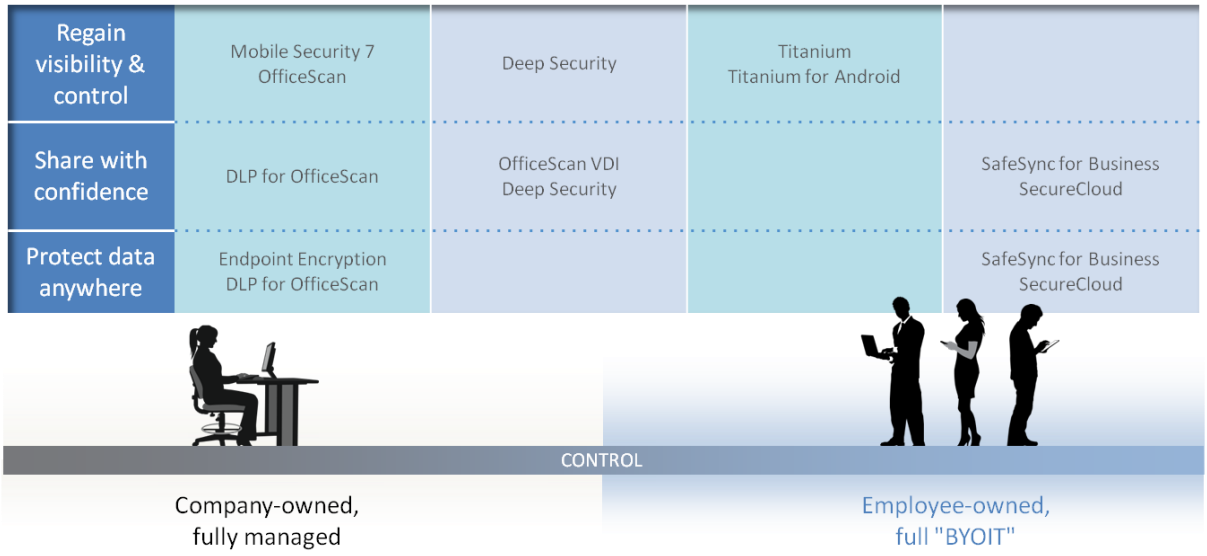
Trend Micro helps companies not only find the appropriate balance between end-user freedom and IT management but also develop an integrated approach to their consumerization strategy. Although IT may see the results of consumerization

manifest itself in obvious ways here and there, those issues that they do actually have visibility into are just the tip of a much larger iceberg of problems that stand to arise at any moment. The only way to be prepared for these unforeseen concerns is to proactively implement an infrastructure that is built to address them.

Trend Micro has organized its solutions for consumerization across a spectrum that ranges from high end-user freedom to high company control — and every nuance in between. These products are organized along three broad "axes": helping IT regain visibility and control, allowing IT to share corporate content with confidence, and helping IT ensure that data is protected anywhere. Figure 1 illustrates how Trend Micro's current offerings for consumerization fit across the control spectrum.

FIGURE 1

Trend Micro's Solution: Balancing Management and Freedom



Source: Trend Micro, 2011

Evaluating solutions for consumerization on a spectrum helps companies across vertical industries and size segments realize that they can embrace this growing trend to the degree that they are comfortable. Organizations don't have to either say yes to everything or be in complete lockdown. All companies have the ability to mix and match these offerings to achieve the ultimate balance for their own organizations. By choosing solutions that are best suited to their culture and business needs from each of the three core areas, organizations can begin to build a comprehensive solution for mobility that addresses today's challenges as well as those that stand to wreak havoc tomorrow.

RECOMMENDATIONS

- **Think about consumerization strategically.** In today's environment, many companies take a reactive approach to consumerization, but employing a proactive, strategic approach has a number of benefits. The first step is realizing that this shift is probably already impacting your organization and that meeting it head-on is far better than choosing to ignore it. Important questions to take into consideration include the following: What mobile devices will you support? How will you decide who is eligible for the BYOD program — will it be determined by job function or by level in the organization, or will the program be all inclusive? What corporate resources will be accessible via smartphone or tablet? What are the security and compliance requirements that you need to respect, and how will you demonstrate your ability to meet them? Who will "own" security and compliance for consumer devices in your environment? Will you need additional resources in IT to support this initiative? What end-user education initiatives can you put in place for your organization? Companies that embrace consumerization have the opportunity to both improve their risk posture and increase employee satisfaction. So, if lowering vulnerability and improving the bottom line are goals of your organization, taking a strategic approach to consumerization can help get you there.

- **Think like a consumer to identify the potential risks of consumerization.** Although the first sign of consumerization may be the need to support new device types, realize that this is just the beginning. As an end user yourself, think of all the ways you interact with your personal device and realize that your employees are all doing the same things with theirs, but without the knowledge of the potential security risks they may be creating. Things that seem like common sense to IT personnel — such as not forwarding your company email to your personal email or storing company data in consumer apps — do not register as security risks with the average end user. Therefore, it is important to educate end users on why you have put certain policies in place — and if they want the privilege of connecting their devices to the corporate network, they must abide by them. At the same time, organizations should always aim to deploy solutions that take into consideration end-user experience.

- **Find the right approach to embracing consumerization for your organization.** There is no one-size-fits-all approach to most IT initiatives, and consumerization is no different. There are a number of points to take into consideration: Beyond making choices around device support and liability, organizations need to make decisions about the amount of freedom that they are comfortable affording end users and find solutions that match that comfort level. A question to take into consideration is, Which corporate resources will you make available on each device type? For instance, perhaps mobile applications housing your most sensitive data (such as a business intelligence app) are available for consumption only on corporate-owned devices. This may be dictated by anything from laws to organizational culture and can be automated by a policy management solution. Next, organizations should consider what their existing infrastructure looks like and how solutions for consumerization will integrate with it. Another important step is to put in place metrics for how you will track, measure, and define success for these projects. Finally, when choosing a

vendor, make sure it has both an understanding of what your organization needs today and a road map that helps you understand what you will need tomorrow. If your chosen partner in consumerization is one step ahead of the risk environment, your organization will be better equipped to stay ahead as well.