Editorial Brief

How Can You Prepare for the Consumerization of IT?

by Candace Worley, Senior Vice President and General Manager, Endpoint Security, McAfee, Inc.

The consumerization of IT is all about productivity. That's the finding from a recent survey of organizations that currently allow or plan to allow employees to use personal IT devices and consumer-driven software on the enterprise network. But the increased productivity is not without cost. More than half of the survey respondents also agreed that consumerization of IT increases security concerns, and nearly half (45 percent) feel that managing consumer-owned devices and related technologies within the enterprise network is "critical."

Level of Criticality in Managing Consumer Devices

	Overall (Mean=3.24)	McAfee	Non McAfee
Base	*196*	*76*	*120*
Extremely Critical	8%	8%	8%
Somewhat Critical	37%	41%	34%
Indifferent	32%	28%	35%
Not Very Critical	17%	18%	17%
Not Critical at All	6%	5%	6%

In a recent survey of 233 IT decision-makers, 45 percent of the respondents said that managing consumer-owned devices and related technologies within the enterprise network is "critical."

According to this survey[1] of IT decision-makers, administrators, consultants, and security analysts, the key drivers of consumerization of IT are increased employee productivity (58 percent) and greater flexibility and turnaround time (52 percent). Like the companies they work for, employees are striving to become as productive as possible. To achieve that goal, they've turned to the world of consumer electronics, smartphones, personal laptops, and newly minted mobile devices like the Apple iPad. If employees feel they can do work faster and easier using their own technology, they won't hesitate.

But giving employees unfettered access to valuable company data on whatever device they happen to prefer is a risky proposition. The fact that these devices are mobile means that they're also easily lost or stolen. Which means that the data they contain is more vulnerable to theft or accidental loss. Access to company data on an employee's laptop, mobile phone, or other personal device can also create compliance issues by making it difficult or impossible to verify that data is secure at all times. Finally, because consumer devices are not adequately protected against malware, enabling access through these unsecured devices can open a gaping hole in the company's otherwise secure firewall. These risks have led many organizations to firmly resist consumerization by restricting the introduction of personal devices or consumer electronics into the workplace and attempting to lock down data.

But it doesn't have to be an all-or-nothing proposition. It is possible to balance access with protection, to allow employees (under the right conditions) to use a variety of tools to gain the productivity they seek while maintaining security for the company's data and systems. Not only will you benefit from your employees' productivity, but you can actually save money in other ways that you may not have considered.

The first step is to recognize that this trend, the consumerization of IT, is here to stay. The number of mobile workers worldwide is expected to reach nearly 1.2 billion by 2011 (source: IDC). During the course of a day, today's employees use four consumer devices and multiple third-party consumer applications, such as Facebook, Twitter, and other social networking sites—and they use them interchangeably for business and personal activities.

The result is that the boundaries of a company's information network are not as clearly defined as in the past. It used to be that a company's information network ended at its firewall, and its valuable data remained relatively secure within that network. But today, data is no longer contained within the walls of your business and the network ends with the user and the user's device (mobile phone, laptop, and home computer). In this environment, security is far more complex than in the past.

[1] This survey was conducted during the first half of 2010 by an independent research firm with support from McAfee. McAfee was not disclosed as a sponsor of the research. For more information, please contact McAfee.

It's common for employees with mobile devices to mix multiple applications on the same device, such as Facebook, business applications, and personal finance and banking. This creates increased challenges for securing data on these devices.

So, how do you handle this situation? What steps can you take to prepare for the consumerization of IT? Here are some strategies we at McAfee recommend:

1. Deploy host and network anti-malware to reduce infections and protect company systems.
2. Deploy a firewall and network intrusion prevention system (IPS) to control traffic to and from key assets.
3. Require VPNs for secure connections to corporate networks.
4. Enforce remote encryption and wiping of information and applications for company-owned smartphones and other mobile devices to protect data in case the device is lost or stolen. Note that this approach is difficult to use with users' personal mobile phones and computers.
5. Use network access control (NAC) to ensure employee-owned devices have proper security tools installed and are otherwise compliant with IT standards prior to accessing the network. NAC can control guest devices and other unmanaged endpoints and ensure they have limited ability to access resources or infect your network.
6. Consider virtualized desktops (VDI). With VDI, employees can access company applications and data on personal devices, but the application infrastructure and data remain on corporate servers behind the firewall.
7. Implement encryption for information at rest and in motion. If a remote device falls into the wrong hands or a transmission is intercepted, encrypted information is unusable. Note that while this strategy is practical for company-owned laptops and employee-owned smartphones, it's difficult to enforce data encryption on employee-owned PCs and Macs.
8. Investigate a relatively new development called "PC on a stick," in which thumb drives (USB drives) or memory cards store a customized interface or launch pad, user-selected applications, and data. Users can carry this computer-on-a-stick to any public or shared machine, plug it in, and begin working with familiar tools and personalized settings. When the drive or card is removed, there is no trace of the user's work left on the PC.
9. Deploy integrated endpoint security with a centralized management console to ease the effort required by security administrators and enable them to easily manage all endpoints in the system. An integrated, centralized strategy is more efficient, more effective, and ultimately less expensive than deploying a series of point solutions.

If you follow these recommendations and deploy a comprehensive endpoint security solution, you'll find it's not only possible to support the consumerization of IT with adequate and effective security, but that doing so yields some nice benefits for the company. Increased productivity is the obvious one. A less apparent benefit is the ability to reduce IT costs by allowing employees to use devices they've purchased themselves. The greater mobility of the workforce and the ability of employees to work from home can also lighten other expenses, such as office costs. Over time these savings can be significant—and when combined with greater productivity, they can make your organization more nimble and competitive.

Candace Worley is Senior Vice President & General Manager, Endpoint Security at McAfee. She's responsible for defining and executing the strategic direction for the McAfee Endpoint Security business. Worley leads the engineering, marketing, and sales functions that drive worldwide growth for this area of the business, including McAfee anti-virus, anti-spyware, anti-spam, web security, desktop firewall, intrusion prevention, network access control, application control, and encryption products.

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.