Tackling 'Consumerization of IT'

How the explosive growth of employee-owned mobile devices on corporate networks challenges IT

the Fact Point group

By Tim Clark
Partner and Senior Analyst
February 2012

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Introduction

Given the ever-growing number of mobile devices sold to consumers, managing workers who want to utilize their own mobile devices for business use has become a daunting task. According to analyst firm IDC, smartphone vendors were expected to ship 472 million smartphones in 2011 compared to roughly 305 million units shipped in 2010. IDC expects that figure will nearly double to 982 million by the end of 2015.

But smartphones are not the only category that is causing trouble on corporate networks —Apple® reported selling 15.43 million iPads globally during its first quarter, a 111% increase over a year earlier,[1] dwarfing other tablet-makers, who combined for more than 1.2 million units sold in the U.S. from January through October 2011.[2]

This trend toward business use of personal devices is a result of a broader shift called "Consumerization of IT." First coined in discussions of enterprise social media and Web 2.0, consumerization of IT describes the trend for new information technologies to emerge first in the consumer market and then spread into businesses. This consumerization has forced IT professionals to adapt to new technologies they do not control. No longer do technology innovations come first to corporations, where IT was firmly in charge.

The consumerization trend has most recently been driven by the preference of employees to work on their own personal devices such as smartphones and tablets. That has birthed the Bring Your Own Device (BYOD) movement, increasingly supported by businesses. More broadly, however, the consumerization of IT shows up in consumerish interfaces for serious business applications, a trend that goes farther than the UI. Powerful, easy-to-use software with Enterprise 2 interfaces can be seen in offerings on collaboration software in many forms including Workday (HR), Box (online storage and collaboration) and Zendesk (help desk).

The inconvenience of carrying separate devices for work and for personal use has given way as employers increasingly acknowledge and even support the Bring Your Own Device (BYOD) policy. If anything, consumerization of IT creates growing pressure that will continue to push IT departments to establish BYOD policies in the future:

- By 2012, annual worldwide sales of mobile devices will increase to 650 million units.[3]
- By 2013, smartphones will overtake PCs as the most common web access devices worldwide.[4]
- By 2014, smartphones that users purchase outside company policy for work or attach to corporate networks will sell faster than any other smartphone segment.[5]
- By 2015, cumulative smartphone sales of 2.5 billion units with annual tablet sales will reach 326 million units.[6]

[1] "Apple Reports First Quarter Results," Jan. 24, 2012, press release, Apple Computer http://www.apple.com/pr/library/2012/01/24Apple-Reports-First-Quarter-Results.html

[2] "U.S. Tablet Sales (Excluding Apple) Exceed 1.2 Units in First 10 Months of 2011," press release, Nov. 22, 2011, NPD Group. http://www.npdgroup.com/wps/portal/npd/us/news/pressreleases/pr_111122b.

[3] Ro. erta Cozza, "Forecast Mobile Communications Devices by Open Operating System, Worldwide, 2008-2015." Gartner, Inc., April 5, 2011.

[4] "Gartner: Mobile To Outpace Desktop Web By 2013," Media Post Communications, January 13, 2010.

[5] IDC report: "Worldwide Business Use Smartphone 2010–2014 Forecast and Analysis", September 2010

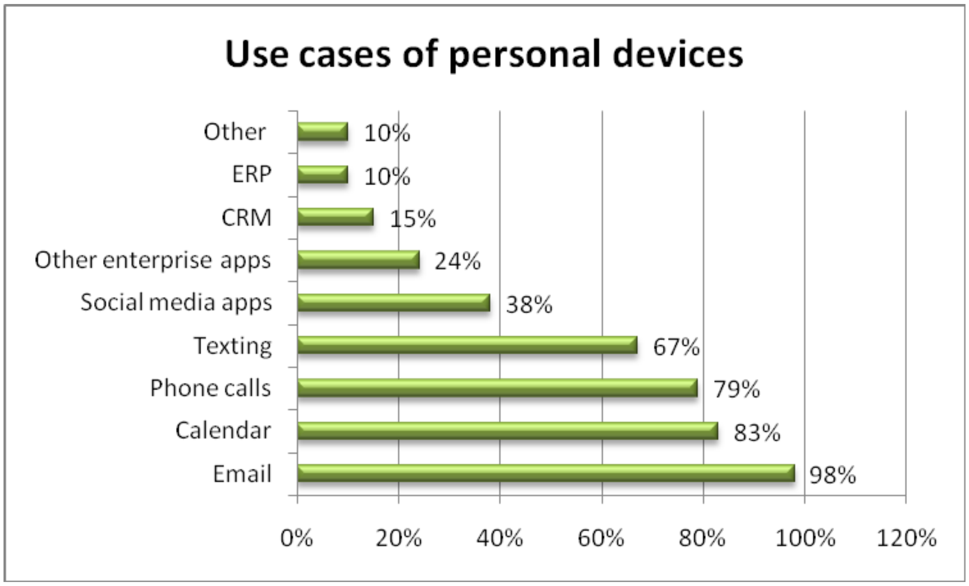
- By 2013, 80% of organizations will support a workforce using tablets; by 2014, 90% will support corporate applications on personal devices.[7]

Why does BYOD gain momentum in companies?

Think of BYOD as the second wave of the consumerization of IT. The first wave came when businesses began to embrace social media and created corporate pages on Facebook®, marketing tweets on Twitter® and recruiting on LinkedIn®. Other factors driving the Bring Your Own Device policy trend are the vast attraction of consumers to mobile devices, younger workers who want to work with familiar devices, and claims that BYOD may boost productivity. Anyone who hopes BYOD is just a fad will likely be disappointed. Organizations may encourage employees to use personal devices for work because it reduces the number of devices they must purchase.

"Consumerization of IT is not simply a passing trend — it is the way business will be conducted on an ongoing basis," said Diane Hagglund, senior research analyst at Dimensional Research, which conducted a survey on BYOD for Dell KACE. "It is critical that companies put policies and standards into place to support these devices and ensure the security of corporate data and intellectual property."[8]

How employees use personal devices for business



Source: Dimensional Research, September 2011

As the table above demonstrates, personal devices are used for work primarily to communicate—via email, text message or a voice call. Use of social media apps is relatively high, but so far, the use of personal devices to interact with enterprise application is not as common, perhaps because not all apps support smartphone or tablets.

[6] "iPad to dominate tablet sales until 2015 as growth explodes, says Gartner," Charles Arthur, The Guardian, Sept. 22, 2011.

[7] "Delivering mobility solutions to the workforce," by Monica Basso, Research VP at Gartner, Oct. 5, 2011, ARN, http://www.arnnet.com.au/article/403094/mobility_trends_delivering_mobility_solutions_workforce.

[8] "Consumerization of IT Taking Its Toll on IT Managers," by Shane O'Neill, CIO magazine, Sept. 15, 2011, [(http://www.cio.com/article/print/689944.

In the early days of the iPad, Forrester Research, classified use cases as "Displace" when iPads replace laptops, "Replace" for tablets replacing clipboards, and "New Place" when a tablet is used in places where nothing was used before—as when Lloyd's of London piloted iPads with brokers so they could write business directly from the field.[9]

IT Concerns about BYOD

Dimensional Research found that 82% of IT managers have concerns about use of personal devices for work purposes.[10] Their concerns ranged from 62% concerned about network security breaches, 50% about loss of customer data, 48% about theft of intellectual property, 43% about additional overhead to support devices and 43% about difficulty to meet compliance requirements. Only 13% had no concerns.

Although security issues dominate the list of IT concerns, operationally the issue of how the corporate help desk supports employee-provisioned devices may be more pressing. If the employee-owned device adds to existing devices that the help desk already supports, the issue becomes how to support more devices per user with limited IT resources. Adding more devices on additional platforms also makes the IT environment more complex.

Because of the sheer number of additional devices, some employers require their workers to purchase a support plan (and sometimes insurance) from their device vendor, a bid to reduce support demands. Or IT may outsource support for smartphones to an outside support entity.

Gartner found that the cost of BYOD support varies widely. Some organizations report reduced costs after implementing BYOD, whereas others report an increase in costs due to the wider range of hardware and applications that must be supported. Some believe support costs will initially be higher until staff members adjust to the new models, after which costs may fall, especially if strong peer and community support arrangements are in place.[11]

Another challenge arises as application development executives decide how to prioritize which mobile devices to support in internal applications. Do they devote their limited resources first to Android or to iOS? How do they weigh application support for iPads vs. desktop PCs? More device platforms mean more integration issues as well—IT executives must rank needs to decide where to put their efforts.

Dimensional Research also found software tools to manage personal devices to be lacking (62%), thus obscuring what is really happening on corporate networks: 32% say employees use unauthorized devices and applications to connect to the corporate network, 36% admit it's possible but they just don't know and 64% are not confident that they know about all of the devices being used.[12]

[9] "How iPads Enter The Workforce," Ted Schadler, Forrester Research, Oct. 26, 2010, http://blogs.forrester.com/ted_schadler/10-10-26-how_ipads_enter_the_workforce

[10] "Consumerization of IT: a Survey of IT Professionals," September 2011, Dimensional Research, sponsored by Dell KACE, http://www.kace.com/redir/reg_success.php?doc=Consumerization-of-IT-Survey-2011. Dimensional Research

[11] "Best Practices for Supporting 'Bring Your Own' Mobile Devices," by Nick Jones and Leif-Olof Wallin, Gartner Inc., July 26, 2011 http://www.gartner.com/technology/reprints.do?id=1-17YXF39&ct=111110&st=sb.

[12] Dimensional Research.

To policy or not to policy?

Faced with the reality that employees work on personal devices, IT departments must decide how to manage those devices; avoiding a policy will not make the consumerization of IT trend go away. In an August 2011 survey by Dimensional Research, 88% of IT professionals surveyed said it was “important” or “very important” to have a policy in place on use of personal devices. In addition, 69% had a BYOD policy and 18% had plans to put one in place.[13]

Nonetheless, some organizations find it advantageous to keep their policy “under the radar” by supporting personal devices but not publicizing that support. Besides the obvious effort to keep support costs in check, some companies may hope to avoid contract issues with their PC suppliers.

Because of IT challenges and costs of supporting additional devices, some IT organizations keep an “approved list” of personal devices. SAP, for example, started by supporting the iPhone® and iPad® but later added Samsung Android™ tablets and smartphones. "The line between the consumer world and the corporate world is fading," SAP’s CIO Oliver Bussmann said. "We're watching consumer devices flood the office space — iPads, iPhones, Android devices. They're everywhere. And we need to empower our employees to have a mobile mind-set instead of trying to keep these devices out."[14]

BYOD policy requirements

IT organizations must consider four dimensions for employee use of personal devices: Where, what, who and when. The easiest answer to the “where” question is that use on the company’s wireless LAN is approved. But what should be the policy for connecting to the corporate network from an external Wi-Fi hot spot? “What” means which devices are allowed (whitelist of allowed devices or blacklist of banned devices). The “who” question is critical: It is not only about the devices but who is using the device—what data are users allowed to access and retrieve? For “when,” the policy may limit access to company databases or other resources to certain hours.

Do not set policy in a vacuum. The IT department at a healthcare provider standardized on Blackberry devices because of their security features, but its physicians used iPhones in their daily rounds. Lesson: Get input from users before setting policy. IT also should actively tell employees which devices are allowed on the network.

Increasingly, Gartner reports[15], organizations have written contracts to define employee responsibilities in a BYOD program. This covers issues such as who is responsible for backing up the device, what control the employer has over a personal device (e.g., wiping it, if necessary), the user’s responsibility if the device is required for e-discovery in a lawsuit, security and acceptable-use policies, insurance and support for lost/broken/faulty devices.

Promising practices

A number of promising practices has emerged as IT departments cope with managing employee-owned devices. Some companies give employees a stipend to buy the devices they want to work with. In

[13] Dimensional Research.

[14] “SAP CIO: It's Always Bring Your Smartphone To Work Day,” by Rob Wright, Computer Reseller News, Jan. 11, 2012, http://www.crn.com/news/client-devices/232400122/sap-cio-its-always-bring-your-smartphone-to-work-day.htm.

[15] Best Practices for Supporting 'Bring Your Own' Mobile Devices, Gartner, Inc.

addition to allowing employees to work with devices they prefer, anecdotal evidence suggests they may spend more on new devices than their stipend—meaning the employer gains from more sophisticated technology. In addition, employees tend to take better care of devices they buy themselves.

BYOD policies must be communicated to employees, monitored, and enforced, introducing a new source of friction between employer and employees, Gartner notes, advising support organizations to consult with legal and human resources departments about implementation. Blocking an employee's unauthorized device or, after a loss, wiping it clean of both personal and corporate data are sensitive steps.

Support organizations will need new skills and more time understanding consumer technologies, Gartner advises.[16] Among the tricky areas likely to emerge:

- What happens when personal devices are lost, broken or faulty?
- Will proposed application upgrades operate on employee-owned devices?
- What happens when an employee owned device is more expensive to operate? What are the policies related to funding and reimbursement? Who will apply them?
- How must multinational organizations customize their BYOD support programs for each country, because of privacy, funding and taxation issues?
- Is a contingency plan needed to rapidly adapt the BYOD program and procedures in the event of unexpected legal or compliance demands?

Conclusion

The continuing popularity of mobile devices will accelerate Bring Your Own Device practices, drive the need for corporate policies governing BYOD uses and spur potential conflicts between IT and employees. Beyond technological and security matters, BYOD ultimately becomes a people issue that involves a balance between policies to control BYOD and BYOD-enabled worker productivity.

Why SonicWALL

SonicWALL Mobility solutions offer a powerful and simple-to-use security and policy compliance approach that enhances the security management of mobile devices on connected networks.

SonicWALL® Aventail® E-Class Secure Remote Access (SRA) Series, SRA Series for Small- to Medium-Sized Businesses (SMB), **and SonicWALL Next-Generation Firewalls** deliver easy, policy driven SSL VPN, offering secure and encrypted access to critical network resources for users outside of the corporate network for when they are traveling and using hotspots. The solution supports an extensive range of mobile device platforms, including Windows, Macintosh and Linux-based laptops, Windows Mobile, iOS, Google Android and Nokia Symbian smartphones.

SonicWALL Aventail Advanced End Point Control™ (EPC™) (available for Windows, Macintosh and Linux-based devices) integrates unmanaged endpoint protection, encrypted virtual **Secure Desktop,** and comprehensive cache control. EPC offers advanced endpoint detection and data protection for enterprises, by interrogating endpoint devices to confirm the presence of all supported anti-virus, personal firewall and anti-spyware solutions from leading vendors such as McAfee®, Symantec®,

[16] Ibid.

Computer Associates®, Sophos®, Kaspersky Lab® and many more before the device can access the corporate network.

The **SonicWALL Mobile Connect™,** a single unified client app for Apple® iOS and Google® Android™, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections to ensure confidentiality, data integrity and protection for users outside the network perimeter. When used with SonicWALL E-Class SRA, EPC can determine if an iOS device has been jailbroken or an Android device has been rooted so that connections from those systems may be rejected or quarantined.

In addition, **SonicWALL Aventail Connect Mobile™**, in combination with SonicWALL Aventail E-Class SRA appliances, provides a remote access solution for Windows Mobile smartphones and Google Android smartphones and tablets. Both Mobile Connect and Connect Mobile clients provide "in-office" access optimized for the device, combining a seamless network experience for users, along with a single, centrally managed gateway for mobile access control.

SonicWALL Clean VPN delivers the critical dual protection of SSL VPN and high-performance next-generation firewall necessary to secure both VPN access and traffic. The multi-layered protection of Clean VPN enables organizations to decrypt and scan for malware on all authorized SSL VPN traffic before it enters the network environment. Clean VPN protects the integrity of VPN access by establishing trust for remote users and their endpoint devices, using enforced authentication, data encryption, and granular access policy. Simultaneously, Clean VPN secures the integrity of VPN traffic by authorizing this traffic, cleaning inbound traffic for malware, and verifying all outbound VPN traffic in real time.

SonicWALL Clean Wireless delivers secure, simple and cost-effective distributed wireless networking by integrating universal 802.11 a/b/g/n wireless features with an enterprise class firewall/VPN gateway.

SonicWALL Application Intelligence and Control can maintain granular control over applications, prioritize or throttle bandwidth, and manage website access. Its comprehensive policy capabilities include restricting transfer of specific files and documents, blocking email attachments using user configurable criteria, customizing application control, and denying internal and external web access based on various user-configurable options.

About SonicWALL

Guided by its vision of Dynamic Security for the Global Network, SonicWALL develops advanced intelligent network security and data protection solutions that adapt as organizations evolve and as threats evolve. Trusted by small and large enterprises worldwide, SonicWALL solutions are designed to detect and control applications and protect networks from intrusions and malware attacks through award-winning hardware, software and virtual appliance-based solutions. For more information, visit www.sonicwall.com.

About The FactPoint Group

The FactPoint Group (www.factpoint.com) is a boutique market research, consulting and publishing company based in Silicon Valley. Since 1992, it has been helping technology companies understand and communicate with their customers through custom research, analysis and content.