WatchGuard

Bring Your Own Device

BYOD: Bring Your Own Device – or Bring Your Own Danger?

White Paper

Published: January 2013

What is BYOD?

BYOD stands for Bring Your Own Device, and is used to describe the phenomenon of employees or guests connecting their personal mobile devices and computers to the corporate IT network. It happens in organizations of all sizes and carries with it a unique set of challenges.

BYOD is also referred to as the "consumerization of IT," highlighting the problems IT admins face when confronted with consumer-grade devices accessing their networks rather than the managed, controlled and secured corporate assets of the past.

This white paper describes the market drivers behind the BYOD phenomenon, the challenges presented to an organization, a strategic outline to manage BYOD, and how WatchGuard helps to create a secure BYOD ecosystem.

So what is the danger?

In order to appreciate the challenges and risks that BYOD presents, it is important to recognize the trends and drivers of the BYOD movement.

Up until recently, a typical IT department provided employees with all necessary (and approved) tools and programs to enable productivity, ensuring manageability and security were maintained. This consisted of supplying workers with a computer (desktop/laptop) and installing all required applications (e.g. an "Office" suite) that met company-specific IT standards.

With the mass adoption of mobile technology and the widespread use of social media, the BYOD trend emerged.

Businesses suddenly faced a work environment where employees were bringing in personal mobile phones that could take notes and record sound as well as take photos of sensitive data or internal documents and then easily share this data outside of the bounds and controls of the corporate network. Other devices, such as MP3 players, could also function as removable hard drives, allowing workers to take information with them anywhere without any record of the data leaving the office.

In addition, employees began to participate in the new wave of social media applications. Early on, most IT administrators viewed social media as a waste of time and a drain on employee productivity. However, the success of early adopters proved that social media also enabled worker efficiency by allowing them to share, collaborate, and communicate in a much more flexible and user-friendly manner than strictly-controlled corporate applications.

This trend accelerated as the lines blurred between work and personal activities. Work was no longer a place to go, but more of a thing to do. Employees can now work anytime, anywhere. We work and play with multiple devices (phones, laptops, handhelds, etc.) without sacrificing productivity or work/life balance and personal satisfaction.

In less than 10 years, the consumerization of IT has taken hold, leaving IT administrators to face new challenges of information security and control versus employee productivity and freedom.

Make no mistake about it – BYOD is here to stay. A 2011 analyst survey stated that 40 percent of devices used to access business applications are consumer-owned, up 30 percent from 2010[1]; while another analyst published a report that by 2014, 80 percent of professionals will use at least two personal devices to access corporate systems and data.[2]

Although BYOD could also stand for "Bring Your Own Danger," there are benefits to an organization and its employees in adopting BYOD as part of an IT strategy. By comparison to traditional IT assets, consumer mobile computing devices are inexpensive. And, as more employees utilize personal devices, employers can scale down on provisioning and managing devices, which in turn lowers IT costs. Conversely, a recent study in the UK showed that IT actually increases costs when trying to restrict employees bringing in their own devices.

As for increased employee productivity, a published survey of 1,100 mobile workers showed that "employees who use mobile devices for both work and personal issues put in 240 more hours per year than those who do not."[3]

Additional benefits of adopting BYOD in the workplace include companies reporting that employees are more satisfied with their work and are having better results with collaboration and working remotely.

BYOD is the new workplace reality. In the end, there are multiple reasons – from cost reductions to increased employee efficiencies – that support corporate adoption. IT must, however, take into account the risks and challenges associated with BYOD.

Challenges for IT

"You can't protect what you don't know." This statement is sometimes used as justification for not adopting BYOD. But, with every rule, there are exceptions, and often the exception for BYOD resided in the corner office of a C-level executive.

In many ways, BYOD started at the top. Senior executives who wanted to work from home and abroad were among the first to demand that IT enable access to corporate resources from their personal devices. Because these C-level exceptions were relatively infrequent, IT could manage risks associated with the requests.

The trickle down from this exception quickly escalated, and many organizations have been caught off guard without a BYOD policy in place. And, because consumer devices are so diverse in capability, form factor and function, IT departments can be frustrated with efforts to develop a scalable and manageable plan on how to allow or deny specific consumer devices into the organization.

Unquestionably, BYOD challenges long-standing IT controls to minimize and mitigate risk. And, as businesses explore how to adopt BYOD, the risks associated with it must be examined.

[1] IDC (sponsored by Unisys). "IDC 2011 Consumerization of IT Study: Closing the "Consumerization Gap." July, 2011.
[2] Gartner
[3] iPass. "The iPass 2011 Mobile Workforce Report." November, 2011.

First and foremost is the risk of data loss. Data loss can vary, and the consequences can be extreme. For example, a recent study estimated that a data breach could cost a company about $200 per compromised record, based upon a variety of factors including the cost of lost business because of an incident; legal fees; disclosure expenses related to customer contact and public response; consulting help; and remediation expenses, such as new security technology and training.[4]

Additionally, regulatory laws and compliance rules can further impact an organization's bottom line in the event of data loss. For example, a retailer that experiences a breach may have to pay for credit monitoring services for affected customers, payment of legal settlements, and PCI DSS information control audits for up to five years.

Second to data loss are the risks associated with viruses entering the corporate network via consumer devices. Many off-the-shelf, consumer mobile devices lack antivirus and/or antimalware protection. For example, Android devices are often the subject of media headlines that tout the virus risks, such as keyloggers, trojans and other forms of malware.

Similar to viruses entering the workplace via a consumer device, so too are the risks associated with intrusion attacks. Granted, the industry is at a nascent stage of targeted intrusion attacks via mobile devices, but the expectation is that hackers will be able to break out of device browser "sandboxes" and get access to other device functions. This could easily lead to directory harvest attacks or new types of BYOD-driven botnets.

And, relating to the web browser that operates in these consumer devices, WatchGuard predicts that Man-in-the-Browser (MitB) attacks will escalate. Traditional malware tends to infect the OS – typically, as an executable program that modifies various boot parameters so it runs every time a computing device is turned on. In contrast, MitB or browser zombies, arrive as malicious browser extensions, plugins, helper objects, or pieces of JavaScript. They do not infect the whole system; instead they take complete control of a device browser and run whenever the user surfs the web.

In addition to outright attacks, IT is challenged with policy enforcement. With so many devices available to the consumer, IT departments are simply ill equipped to create device-by-device policies. Due to the wide range of devices, it is critical for IT to be able to identify each device connecting to the corporate network, and be able to authenticate both the device and person using it.

Lastly, IT is challenged with having sufficient insight as to what is happening in their network. Without being able to see what is going on in the corporate network, IT is hindered in its ability to protect business and information assets. That lack of insight (both in terms of logging and reporting) supports the adage that "you can't protect what you don't know."

Risk challenges aside, there are related productivity challenges to BYOD. Knowing that work is a thing employees do, not necessarily a place that they go, IT must afford secure access solutions, such as virtual private networks (VPNs), in order to empower employees to work anywhere.

[4] Ponemon Institute (sponsored by Symantec). "2011 Cost of a Data Breach." March, 2012.

IT must also prepare for more employees who expect to collaborate via the web, use remote access solutions, and have the freedom to use their personal mobile devices in the workplace environment.

In conclusion, there are a myriad of challenges that IT faces in order to deal with BYOD. Some of these are risk-management challenges; others are empowerment and usage challenges. Nonetheless, IT must expect to adopt and enforce a BYOD strategy as part of its services to the organization.

Ten Strategies for Embracing BYOD

The following are strategic points that an IT department or administrator should consider as part of their BYOD planning process.

1. **Get Insights**: WatchGuard identifies common mistakes in creating a BYOD strategy. The first of which is the failure to know what employees are doing on the network. By taking a benchmark snapshot via firewall logs and reports, IT gains invaluable insight as to what devices are actually connected to the network, and just as important, what applications are being used.

2. **Support social media**: Do not immediately assume that use of Facebook or other social media applications means that employees are wasting their time. Instead, it is much better to review and examine the nature of the applications traversing the network before making any draconian moves that could grind productivity to a halt.

3. **Manage passwords**: Another mistake to avoid involves password management. All too often businesses resort to user-generated passwords as part of their access controls. This can lead to very weak passwords, which can compromise IT systems. Password policies for BYOD devices should be no different than strong password requirements for traditional IT assets, such as laptops or desktop computers.

4. **Establish policy**: IT should focus on policy to “keep BYOD simple.” IT should consider making a broad list (a meta-table) of acceptable devices that can access the corporate network. Additionally, IT should also state which devices/operating systems that it will and will not support. This way, tech-savvy employees can utilize what they like, knowing that they are responsible for the management and well-being of their device if IT does not support it.

5. **Separate work from fun**: IT should also include in their policy that work information should be kept separate from personal information wherever possible. Consider making it a standard operating procedure that when employees access the corporate network on their own device that they also agree to adherence of company acceptable use policies, as well as IT monitoring and risk management tools.

6. **Acceptable use**: In accordance to standard security practices, companies should always enforce minimal access controls. In other words, even with BYOD, a strong security policy would be to deny all, except for approved devices, applications and users. Every business will be different. Therefore, it is critical to know in advance what your security policy is with regards to access controls.

7. **Limit access via VPN technologies**: For businesses that require higher degrees of protection, IT administrators may want to limit access controls to devices that support some level of VPN connectivity. This way, regardless of where a consumer device is used, a secure connection is required to access corporate data.

8. **Look beyond the device**: Application control strategies play an important role in making a BYOD policy secure and efficient. Make sure your BYOD policy also includes specific applications that are acceptable as well as others that are not. With application controls in place, the network becomes agnostic to the device, and instead can enforce policies based on specific, acceptable applications.

9. **Apply policy to a segmented network**: Sensitive data should always reside on a different network than that which is open to guests, contractors or other non-employees. With a segmented network, IT can apply one set of policies for employees and another set for guests.

10. **Understand compliance**: Examine what else is at risk. Is your organization subject to regulatory controls, such as HIPAA or PCI DSS? Are damage controls in place so that if an employee loses a smartphone or tablet, it can be wiped to avoid loss of data?

Lastly, notification is critical for avoiding legal liabilities. Make sure your BYOD policy is regularly communicated to all employees. Have a written policy that states what rights an employee gives up in order to gain access to corporate resources with an employee-owned device.

In the end, the best BYOD strategy is going to build upon a solid foundation of security best practices and end user policy enforcement.

Creating a Secure Ecosystem with WatchGuard Technologies

Knowing that BYOD is here to stay, WatchGuard provides IT administrators with easy to use security services that businesses need in order to manage BYOD.

Policy made easy: First of all, WatchGuard designs all of its Next-Generation Firewalls and UTMs (XTM products), Secure Email Gateways (XCS products) and SSL VPN products with powerful, yet easy-to-use policy tools. This way, administrators can enforce the policies that best meet their environment, whether it is a small retail shop or a multinational, distributed enterprise.

Network segmentation: WatchGuard solutions allow an administrator to easily and quickly set up various network segments. And, with WatchGuard's virtual product lines (XTMv and XCSv), even virtual assets can be protected and segmented in order to maintain compliance and high security.

Application Control: No other security vendor provides as rich and easy-to-implement application control capability. With WatchGuard Application Control, administrators can monitor over 1,800 types of applications traversing their network. Administrators can set a variety of policies in place, ranging from monitoring to complete application blocking. Even applications within web apps can be controlled. For example, a business may want marketing employees to have access to Facebook, but not have the ability to play Farmville. With this level of application control, IT can rest assured knowing that regardless of what device an employee brings in, IT will have the power to control the applications moving through their networks.

Gateway antivirus: With WatchGuard, the perimeter of the network can also be the first line of defense against mobile malware. WatchGuard utilizes a "best-in-class" approach, which ensures that all connected devices on the network are shielded with an antivirus umbrella. Adding cloud-based Reputation Enabled Defense to this further provides advanced protection to all networked devices from both dangerous IP and URL destinations worldwide.

WebBlocker: In addition to Application Control, WatchGuard's WebBlocker service also makes it easy for IT to setup and administer policies around acceptable and unacceptable web surfing activities. Because this service resides at the gateway, it is agnostic to the type of device that an employee brings in. Therefore, safe web surfing practices can always be enforced.

VPN functionality: With WatchGuard's VPN capabilities, administrators can enforce acceptable use policies for mobile, remote and road warriors who need to access corporate data anytime, anywhere. These controls even protect users in the most hostile environments, such as hotels and public Wi-Fi hotspots.

Logging and Reporting: This may be one of the most valuable resources that IT can leverage for their BYOD strategy. With WatchGuard, administrators gain deep insight into what is connected to their network, as well as the applications being used. This type of insight not only helps to protect resources, but also illuminates trouble spots and potential weaknesses, and helps to remediate areas of concern.

Summary

BYOD is a force that is here to stay, and by all expectations, is expected to grow in size and scope. With it, come new sets of challenges and opportunities for businesses as well as their IT departments. This means that a BYOD strategy is critical for success and data security. As part of a strong BYOD strategy, having well-designed policies and end user agreements in place will be key. WatchGuard provides the tools and solutions to make a BYOD environment a safe and productive ecosystem for today's IT administrators.

For More Information

For more information, visit the WatchGuard website, contact a WatchGuard reseller, or call 1 (800) 734-9905 in the United States and Canada.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. Part.No. WGCE66791_011113