Overcoming the Security Challenge of BYOD Policies

Protect Your Enterprise With Personal VPNs

A White Paper by Golden Frog

Summary

Today, there are approximately *one billion* mobile devices (laptops, netbooks, tablets and smartphones) in use worldwide. By 2020, that number could reach ten billion.[1]

For professionals, the business use distinction between personally-owned mobile devices and company-issued devices has blurred. Employees look at their personal devices as indispensible tools that they carry at all times, and increasingly use them to perform work both on- and off-site. Many companies have responded by instituting BYOD (Bring Your Own Device) policies that attempt to regulate how employees should use their devices for work purposes.

While BYOD policies have benefits for both employers and employees, they also present a security risk for companies. Nonetheless, BYOD is here to stay; employees will use their own devices for work purposes whether or not a BYOD policy is in place. As an IT professional, your only options are to deny the inevitable or to determine a way to manage security risk effectively. This paper presents a low-cost, easy to implement solution using personal VPNs.

The BYOD Revolution

The BYOD revolution is just beginning. Gartner Research forecasts that **by 2014, 80% of professionals will use *at least two* personal devices to access corporate systems and data**. Three studies suggest that Gartner may have been conservative in its estimate:

- According to a study published in *CIO Magazine* in September 2011, **87% of executives say their employees are already using personal devices for work-related purposes**.[2]
- In addition, a study conducted in January 2012 of IT executives in the US, UK and Germany found that **78% of companies allow employees to use their personal devices for work-related activities**.[3]
- Finally, a study conducted in 2011 by Yankee Group found that 23% of companies will remove or block employee-owned devices from their work environments—which implies that **77% of companies either specifically or passively allow employee-owned devices**.[4]

Interestingly, companies might not even be aware of the extent to which personal devices are used in their organization. A 2011 study by IDC found that IT groups typically underestimate the proportion of employees using their own devices for work purposes: **40% of IT executives say they allow employees to access corporate information using their own device, but 70% of employees report that they do**.[5]

The bottom line is that the BYOD phenomenon—whether viewed as a formal policy or simply as common employee behavior—is prominent today, will continue to expand, and cannot be stopped. It's helpful to understand what's driving this trend.

BYOD: A Win-Win for Employees and Employers

BYOD offers compelling benefits for both employees and employers. Employees enjoy BYOD for several reasons. Foremost, employees don't want to carry multiple devices. If they're only going to carry one device, they'll choose the smaller, lighter or more modern one, such as a tablet instead of a bulky corporate laptop that's a generation behind the times.

Furthermore, employees prefer to use the device they know how to use most efficiently, which usually means the device they have at home. This can be a benefit for employers, too, because employees are immediately more productive with familiar devices.

Finally, employees welcome the ability to work on the go when traveling, telecommuting, or running errands. This is also great for employers, because it means employees can—and will—work from anywhere, often during extended hours.

The key benefit for employers is a reduced IT burden. Employees generally won't require support for a device they know well, and won't expect a corporate help desk to support their personal devices. In addition, in a BYOD environment IT doesn't need to worry about inventory tracking, configuring or updating employee-owned devices, or about stocking accessories or replacement units. Moreover, the employee already has the device—there's no productivity lag because a company-issued device needs to be ordered or provisioned.

Security Challenges of BYOD

Despite all the benefits of BYOD, the proliferation in use of personally-owned mobile devices for work purposes presents a formidable security challenge for employers. Regardless of how robust a company's BYOD policy is—and how rigorously it is enforced—companies inevitably lose some degree of control in a BYOD environment.

One area where this is particularly troublesome is data security. The flip-side to the benefit of mobility is that IT cannot control where and how employees will access their work email or sensitive corporate data; in many cases, it will be at a coffee shop, hotel, or at home over an unsecured Wi-Fi or cellular network, with data transmitted unencrypted.

A recent survey by Harris Interactive of 1,300 employed adults highlights some of the security risks of BYOD.[6] The survey revealed that:

- 81% of employees use a personal device for work-related functions.
- 31% who use a laptop for work will connect to the company's network via a free or public Wi-Fi connection.
- 33% who use their personal device for work admit that their organization's data and/or files are not encrypted.
- 66% have been a victim of malware or hacking on a personal device.

These findings illustrate that all sorts of lucrative corporate data commonly stored on mobile devices—passwords, email content and attachments, corporate financial information, sales leads, marketing plans, product designs and much more—are vulnerable to interception by hackers using inexpensive (or free) packet sniffing tools. In fact, once a hacker has obtained login credentials to a Web-based corporate application such as Salesforce.com, he can from that point on access those applications directly and logout before anyone knows how much data he has viewed or downloaded—if anyone even notices that the incursion happened at all.

Are Company-Provided Devices Safer?

In a 2011 corporate study, 70% of respondents felt employee-provided smartphones were a security threat, but only 23% felt company-provided smartphones were a security threat. For tablets, the figures were 74% and 28%, respectively.[1] The bottom line: all mobile devices are susceptible to data theft.

Certain popular consumer devices inadvertently exacerbate the security threat. For instance, according to security consultant Mark Wuergler, the Apple iPhone and iPad transmit over Wi-Fi the last three wireless access points their owner has logged into.[7] These are easy to intercept and can provide hackers with valuable clues about where someone works; if that's a lucrative target, the determined hacker will focus on that device.

There are additional risks for companies in specific sectors. For example, in health care, companies need to ensure devices used by employees comply with the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Failure to secure devices to comply with these Acts can have significant financial and legal consequences.

VPNs: An Old Solution to a New Problem?

The classic solution to data theft by hackers is a virtual private network (VPN), which encrypts all transmitted data and masks a device's IP address. This prevents hackers from accessing an employee's emails, documents, chat streams, passwords and other sensitive information. It also prevents, for instance, a competitor from knowing that an employee of your company was perusing their website if they access it through your infrastructure. The proven effectiveness of VPNs means that they will remain the de facto standard for accessing corporate resources from outside the office.

Unfortunately, most employees narrowly think of a VPN as a means to access their corporate network, not more broadly as a way to protect work-related data that they might access even *without* connecting to the network. As a result, most employees fail to use a VPN all the time.

Consider this common scenario: An employee emails a spreadsheet from his corporate account to his personal account so he can work on it at a coffee shop using his personal laptop. When that file is downloaded at the coffee shop unencrypted over a Wi-Fi network, the file is vulnerable to data theft. But because the employee felt he was merely accessing his personal email, he didn't see a need to use a VPN.

There are several other reasons why employees transfer sensitive corporate information (through email, FTP or other means) to or from their personal devices while unprotected by a VPN. It may be because:

- They lack VPN capabilities on their device.
- They don't want to take the extra time to establish a VPN connection.
- They don't want to risk a slower or less stable connection.
- They simply don't know about the inherent risks.

Is Mobile Device Management (MDM) the Answer?

MDM suites offer some compelling functionality, such as the ability to remote-wipe devices, force screen locks, or require more elaborate passwords. These address other issues of BYOD security risks, namely lost or stolen devices. But employees may resist companies placing this functionality on their personal devices since it can result in a poor user experience. And MDM doesn't address data theft by hackers.

Some companies insist that employees *always* establish a VPN connection when using a device that holds *any* corporate data. This would indeed protect *corporate* data, but this solution is a double-edged sword. Employees often shift between personal and work tasks when using their devices in remote locations, and companies do not want employees' *personal* data routed through their VPNs for various legal and technical reasons. For instance, companies don't want employees' banking or health information flowing through their infrastructure, and don't want the added network congestion and tie-up of limited VPN IP addresses while employees, say, stream movies to their device.

The Ideal Solution

From a technical standpoint, VPNs are the right answer to the security risks of BYOD. The ideal solution would complement the traditional corporate VPN—not replace it—with a *personal* VPN. The corporate VPN would protect business-related assets during working hours, while the personal VPN would protect personal data and the occasional transfer of corporate information when the employee is "off the clock." A personal VPN solution should be:

- ✓ *Effective*, with the most widely-used 256-bit encryption protocols such as OpenVPN, L2TP/IPsec and PPTP.

- ✓ *Multi-platform.* The solution should work with all popular mobile device operating systems. A superior solution would be that the VPN runs independently of the device's hardware and operating system (e.g., in a Web browser), so platform compatibility is not an issue.

- ✓ *Easy for a user to install and configure* on their own, with little or no help from your company. Or, better yet, there would be *nothing* to install—the VPN would be delivered as a service, not as an application. Employees will resist any attempts by IT to install anything on or otherwise

manage *their* devices.

- ✓ *Fast and reliable*, with a stable connection and no degradation in data transfer rates up or down.
- ✓ *Non-intrusive*. The VPN shouldn't interfere with employees' devices, applications or workflow.
- ✓ *Supported.* The solution should come from a reputable, stable vendor that will support it.

There is a personal VPN solution that meets all of these requirements.

Introducing VyprVPN, from Golden Frog

VyprVPN is a Cloud-based VPN solution that provides 256-bit data encryption on *any* mobile device, including iOS and Android devices, and all variants of Microsoft Windows. Delivering VPN capabilities as a service means there's nothing to install on users' mobile devices—which will increase user adoption and reduce technical support headaches. VyprVPN stands out from competitive offerings in four areas:

1. Optimized for Internet Scale

Most corporate VPNs were not designed to support thousands of connections, significant bandwidth, and connections over thousands of miles. In contrast, VyprVPN was engineered to support modern uses, such as streaming video at broadband speeds over vast distances. And unlike other VPN providers, VyprVPN has no throttling limits, usage restrictions or download caps.

2. Cutting-Edge Infrastructure

Unlike virtually every other VPN provider, VyprVPN is not an outsourced or hosted solution that relies on third parties to deliver its VPN service. We built our network from the ground up to ensure that we offer the fastest, most reliable VPN connections. Golden Frog:

- Owns its VPN routers and servers, which are housed in dedicated clusters in data centers around the world.
- Maintains direct contractual relationships with Tier 1 Network Providers and peers extensively with major consumer ISPs.
- Has fully redundant infrastructure; our server clusters do not have a single point of failure. The benefit: VyperVPN has never had an outage.

3. Scalability for Large-Scale Deployments

Golden Frog's VPN infrastructure is ready to scale with you. In concert with our sister companies, we have 17 years of experience building and managing infrastructure to service large-scale custom deployments for some of the largest service providers in the world, all while maintaining network reliability and speed.

And with VyprVPN, an insufficient number of IP addresses will never be a problem. Golden Frog has been a registered network provider since 1994. As such, we can request additional IP addresses from ARIN, RIPE and other regional registrars.

4. Best-in-Class Support
There's no burden on your IT group to install or support VyprVPN on users' devices. Golden Frog provides 24x7x365 Tier 1 and Tier 2 support with a human response in less than ten minutes via email or live chat.

Recommendations

Employees expect freedom. The "bring your own device" trend is happening—in fact, accelerating—and cannot be curtailed. The good news is that this can actually be a net positive for companies, as long as some straightforward measures are put in place to mitigate risk. A few recommendations:

1. *Establish or revise your BYOD policy*. Don't just passively "allow" BYOD—institute a formal policy. In particular, clarify corporate versus employee responsibilities. Who is responsible for ensuring data security, for support, and for equipment and usage costs? In addition, remember that a policy is useless if employees aren't familiar with it. Make sure that employees understand the risks—and the benefits—of using their own devices for work purposes.

2. *Offer a VPN solution to all employees*. A Cloud-based VPN solution such as VyprVPN significantly reduces data theft exposure for your company in a way that maximizes employee adoption and satisfaction with the solution. VyprVPN can be positioned to your employees as a *personal* VPN—good for protecting anything, anywhere, anytime.

3. *Educate employees*. To further increase user acceptance of a VPN solution, Golden Frog recommends companies institute a basic employee education program to familiarize users with data security risks, best practices for safeguarding their data (including personal data), and how to use a VPN to maximize data security.

To learn more about VyprVPN, visit https://www.goldenfrog.com/vyprvpn.

---

[1] "The CIO's Guide to Embracing the Consumerized Mobile Enterprise." Yankee Group Research, 2011.
[2] DELL/KACE, *CIO Magazine*, Sept. 15, 2011.
[3] "Mobile Consumerization Trends & Perceptions: IT Executive and CEO Survey." Decisive Analytics, February 2012.
[4] "2011 U.S. Enterprise Mobility: IT Decision Maker Survey, Wave I." Yankee Group Research.
5 "2011 Consumerization of IT Study: Closing the Consumerization Gap." July 2011.
[6] http://blog.eset.com/2012/04/04/byod-infographic-for-security-not-a-pretty-picture
[7] http://arstechnica.com/apple/news/2012/03/loose-lipped-iphones-top-the-list-of-smartphones-exploited-by-hacker.ars