UBM

May 2015

Securing the Home Workforce

As workers move home for part or all of their work hours, protecting sensitive data becomes more critical—and more difficult. Emerging options for private connections go beyond VPN protection—without the performance hit.

INSIDE

1503123

Workers Move Back Home

As the service and information sectors grow into increasingly important parts of the world economy, remote work — particularly from home — has become more commonplace.

While there are many factors contributing to this movement (work/life balance, cost considerations and even concern over the environmental impact of commuting), one important driver has been the increasing availability of reliable broadband Internet connections to the home. At the end of 2013, 71.3 percent of U.S. households had broadband connections, according to a report from IHS.

The growth in the number of home workers has created a need for security solutions to secure the workers' data and the organization's resources. While the connection to the Internet at a workplace is — or should be — secured behind multiple layers of technology, such as firewalls and intrusion detection systems, home connections remain less secure.

Yet that situation is changing as organizations realize the need to ensure secure access for their home-office workers. Many are beginning to explore the security options available now and are keeping an eye on those being proposed.

Work Security for the Home Office

More frequently these days, the discussion around telecommuting includes concerns about and options for securing the home-work Internet connection.

Working from home has grown tremendously in popularity, increasing 80 percent between 2005 and 2012, according to Global Workplace Analytics. That organization also lists the percentage of workers who identify their home as their primary workplace — not counting the self-employed, mind you — as 3.6 percent of the total workforce. When you add in the number of self-employed who work from home, that percentage climbs to 5.6 percent of the overall workforce.

What's driving the acceptance of this phenomenon in the enterprise world? Essentially two things: increased productivity and reduced cost. In a report from 2009, Cisco found in a survey of its own home workforce that "approximately 69 percent of the employees surveyed cited higher productivity when working remote, and 75 percent of those surveyed said the timeliness of their work improved."

IBM, in turn, is reported to have saved nearly $100 million in real estate costs because of telecommuting.

Working from home requires a somewhat different set of guidelines and requirements than working from an office, however. One key requirement, logically, is an adequate connection back to company systems, applications and data. Until now, that requirement has essentially meant a connection to the Internet.

Who Are These Telecommuters?

According to the latest statistics from Workplace Analytics, the largest block of those full-time employees who work from home are from the federal government, accounting for 3.3 percent of the total federal workforce. Close behind it is the non-profit sector, with 2.9 percent of its employees telecommuting.

The for-profit world isn't far behind, though, with 2.6 percent of its overall full-time workforce working from the home.

It isn't a surprise to find out that the federal government leads in this area — after all, in 2013 it passed the Telework Enhancement Act, which requires federal agencies to do what they can to make it easy for employees to work from home.

That fits with how *The New York Times* described the average telecommuter in an article from March 2014: "The typical telecommuter is a 49-year-old college graduate — man or woman — who earns about $58,000 a year and belongs to a company with more than 100 employees."

Not surprisingly, many pieces of advice about an Internet connection for a home worker revolve around getting broadband, and what kinds of broadband services work best for what kind of work. For example, do employees need symmetrical download and upload speeds, or will asymmetrical (faster download than upload) work? How fast does the connection need to be if you are often doing bandwidth-intensive activities such as videoconferencing?

But, more frequently these days, the discussion includes concerns and options around making the work-from-home Internet connection secure. An article about making the case for working from home quotes David Heinemeier Hansson from his book, *Remote: Office Not Required*, on the need for data security:

> *But data is not necessarily secure just because people are working in an office together. Employees take laptops home, they carry company data in their personal smartphones, they go on business trips. If there are security gaps the company needs to address, that is a serious issue whether you are working at home or not.*

Many methods can enable workers to connect to the Internet from home. Each comes with security concerns — and options to address those concerns.

Connection Choices

There are essentially two ways to connect from a home office to the Internet — a wireless cellular connection or a wired copper or fiber connection. Each has benefits and drawbacks.

The Cellular Option

The main benefit of using a cellular connection is that it allows employees to work from anywhere a connection exists to a cellular tower. That includes being able to move around anywhere in the home, or taking work on the road to a café or a hotel and not having to worry about what kind of

connection is available.

Concerns include cost (the minimum connection would be 3G wireless, and 4G wireless would be much more useful) and security. One of the drawbacks of broadcasting work signals to the Internet is that they can be intercepted. And that's true whether or not the remote computing device has a cellular modem built in or the cellular device is used as a Wi-Fi hot spot.

Wired and Wi-Fi Options

A wired connection eliminates that concern — unless, as is very common, employees are connecting to home broadband modems or routers via Wi-Fi signals. Wi-Fi connections are vulnerable to anyone with a decent mobile antenna. (Google demonstrated this vulnerability when it attempted to map local Wi-Fi hotspots while taking StreetView pictures for Google Maps, and wound up allegedly capturing user data from some of those home Wi-Fi routers.)

If employees do connect via Wi-Fi in a home office, the base minimum level of security they must have is a password requirement to access the connection. Two Wi-Fi protocols are most common to do this: WEP and WPA (or now WPA 2). WEP stands for "Wired Equivalent Privacy," but it never truly lived up to that name. These days, WEP security can be hacked easily.

WPA (Wi-Fi Protected Access) provides a better level of encryption, and WPA2 boasts Advanced Encryption Standard (AES) encryption of the wireless connection instead of using temporary key, as was the case with the original WPA. Still, just last March it was reported that WPA2 security can be breached, so the Wi-Fi connection risk remains.

Connecting a computer to the Internet via a wired connection eliminates many of the concerns that come from Wi-Fi — a malicious actor would have to physically tap into the wires somewhere along the line. But cable broadband connections do share a pipeline among multiple households to the shared junction box somewhere on a

Google demonstrated the vulnerability of Wi-Fi connections when it attempted to map local hotspots and wound up allegedly capturing user data from home Wi-Fi routers.

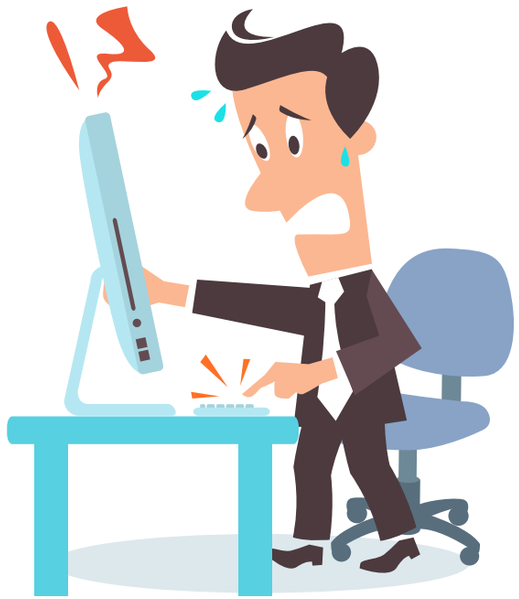
neighborhood utility pole, called a Point of Presence (PoP).

Why VPN Isn't Enough

To help solve some of the security concerns with wired and wireless connections, nearly all remote workers connect back to their offices via virtual private networks (VPNs). A VPN connection essentially creates a secure, private "tunnel" through the public Internet to a corporate office at the other end. This allows home workers to run server-based applications, such as Microsoft Outlook or Lync communications and collaboration, as though they were in the office.

The VPN solves the problem of shared Internet connections, as is the case with most cable broadband connections to the home. Workers may share the connection with their neighbors, but they don't share the tunnel or, more importantly, the data that travels back and forth through it.

But there are still problems with using a VPN — one of which is common to all users and one is specific to certain industries. The common problem is performance. Using a VPN will increase the latency of the broadband connection, in some cases by a lot. Back when connections to the Internet were slow, that latency wasn't very noticeable. But with modern broadband connections in the U.S. hovering around 30.7 Mbps, that latency has become a real concern.



Even if sensitive data doesn't live on a remote worker's computer, malicious software might.

The industry-specific concern with a VPN comes from highly regulated industries such as financial or health care. If someone is working from home and accesses patient data regulated under the Health Insurance Portability and Accountability Act (HIPAA), that home worker's computer should be connected by VPN as well as encrypted as it would be in the main office. After all, the Internet tunnel the VPN creates may be secure, but once that data resides on the home worker's computer, that VPN security is moot.

Even if the data doesn't live on the remote worker's computer, malicious software might. The Backoff Point-of-Sale malware, for example, which was used in data breaches at Home Depot, Neiman Marcus, Goodwill, Target and others — came in to the retailers' point-of-sale computers via remote workers accessing them to do IT work.

And very recently, the U.S. Postal Service suspended indefinitely its remote worker program and shuttered its VPN following its own

data breach. The USPS won't say that remote access caused the data breach, but the need to shut down its own VPN is a strong indicator that it may have played a role.

EPL: An Emerging Option

One new solution for addressing these connection security concerns is an Ethernet Private Line (EPL) to the premises, which allows a company to sidestep Internet-related concerns.

One of the first companies offering that option is Comcast Business. As the nation's largest cable broadband company points out, Ethernet to the home addresses the primary concern for businesses with employees accessing company resources and information from home — security.

The service allows the employee to access company assets via a private connection, bypassing the Internet altogether, which eliminates an external intrusion point and the need to encrypt the data to and from the worker's home. Since the EPL is Ethernet, there is no need for additional routers or protocol conversions, making the work-at-home experience feel the same as being in the office.

The EPL connection sidesteps the common cable broadband requirement that a home worker has to share the Internet connection, at least to the point of presence. That EPL link is a direct line to the base office, essentially no different than if the home worker had an Ethernet cable tens or hundreds of miles long, plugged right into the office Ethernet switch.

Finally, EPL is provided over a service provider's private network, where it controls all the transmission variables. Therefore, the provider is confident enough to offer a service level agreement for performance and availability, something no user gets with the Internet.

As the price of dedicated Ethernet lines to the home via copper or fiber continues to drop, expect to see it become a more powerful driver of the move to working from home for more employees.

But there are other technologies on the horizon, which affect both how home workers connect and how they might increase security.

Ethernet Private Line service allows employees to access company assets via a private connection, bypassing the Internet altogether.

A Glimpse into the **Future**

The increasing availability and declining cost of fast broadband to the home will drive further adoption over the next few years.

Cable broadband providers aren't sitting on their collective hands when it comes to speed and security. The current DOCSIS standard, 3.0, which defines cable network speeds, was adopted in late 2010 and allows for download speeds of up to 1 Gbps, with upload speeds of up to 245 Mbps. That means broadband cable providers are able to compete with new entrants to the game such as Google Fiber, as well as the increasingly common municipal utility Gigabit fiber connection. And with the latest DOCSIS 3.1 standard going into testing this year, those speeds jump to a possible 10 Gbps down and 1 Gbps up.

It's one thing to offer fast, plentiful Internet bandwidth, but it's another to offer Ethernet (and the associated bandwidth) over it. Comcast is currently the only DOCSIS standard supporter to offer Ethernet Private Line over its broadband.

Emerging Security Options

When it comes to security, one of the increasingly popular solutions in the mobile world is also poised to come to the home workforce: containerization. Already the concept of containerization — in which a single app, a collection of software or even an entire computing device is wrapped in a secure "container" through which only trusted connections and activity are allowed — has moved out of the mobile arena and into the cloud, with news that Amazon Web Services supports apps being wrapped by the containerization service Docker.

Containerization may see increased use as home connections grow in popularity. The approach also can provide greater security for a home worker's computer even on a wired broadband connection.

And for home workers connecting through Wi-Fi routers, containerization, combined with any extra secure connection such as a VPN or EPL, should provide nearly all the security an enterprise would need — not counting those federal regulatory requirements mentioned previously.

However the home worker connects to the Internet to get the job done, there are solutions available now for proper security, and more innovative solutions on the near horizon. ■