THE WORK ANYWHERE DEVICE CONUNDRUM

EVOLVE IP

Enabling Productive Employees While Maintaining A Rock-Solid Security Posture

Work from home (WFH) use cases have exploded as companies look to comply with stay at home mandates. For some, this change is amounting to nothing more than "business as usual" from a professional perspective. For others, this is presenting a real challenge to not only be able to work from home but to remain as productive as they were when working from the office.

This challenge is rooted in the fact that corporate environments are sterile by design in order to balance security and performance. However, employees working from home want to keep personal devices customized to them in ways that are often far less secure than what your corporate best practices allow.

IT must bridge these two extremes to allow users to be productive during this time. Below are a few scenarios IT is likely to run into and some options of how to enable workers while maintaining an acceptable security posture.

Already Implemented Virtual Desktops or Remote Application Delivery

For companies that have already implemented desktop or application virtualization, this should be an easier exercise. There will be some items to check into before pulling the trigger. We'll assume for now that end users all have sufficient bandwidth at their home.

1. **End User Devices** – IT is likely to run into a multitude of different end user devices in the home office. If the current solutions are browser-based then users should be fine. If a client is needed, IT will have to lay out the types of devices that users will need to use to connect to the infrastructure. IT will also need to provide documentation for how to access the environment for any users that will be doing so for the first time.
2. **Additional Infrastructure** – The current solution may be designed to service 20% of the workforce for instance. So, IT may need to acquire additional data center hardware and software to facilitate all users. While writing a check is pretty easy, management needs to be cognizant that there may be hurdles to simply adding more hardware that could result in additional spending outside of the direct hardware and licensing costs. For example, to add the remaining 80% of the workforce, IT must acquire a new SAN as the current model will not support that much additional storage or horsepower.

Users on Laptops Today

For users that are on laptops today, their experience should be roughly the same assuming they are using a VPN to connect to the corporate network today. However, the business will still need to address their corporate voice solution, an issue which Evolve IP discusses in great detail on the Website at https://www.evolveip.net/business-collaboration.

Traditional Desktop Users

This is where the fun begins. Below are a few options for employees using a desktop at a home office to VPN back into the

corporate network. There are three dynamics with the VPN design that need to be addressed before moving on to how the device will be used at home.

1. **VPN Overload** – This is a factor that many providers cite as a possible issue. While it's unlikely that this will be a factor given that most enterprise firewalls can handle upwards of 10,000 connections, this should be something that IT looks into to ensure that all the new users, that used to be on the inside and are now on the outside, can connect to their resources.
2. **Split Tunneling** – If laptops are already present in the network this is likely something that is already addressed. Once you open the network to an employee's home device, whatever is on that device, and on the employee's home network and what they pickup when they browse on their local network is now a threat to the corporate network if split tunneling is allowed. Any solution that IT is looking into must address this possible security concern.
3. **Performance** – This could be a show stopper and is a very important aspect of the plan. These employees will be moving from a local network connection that is very fast to a remote connection that is potentially very slow in comparison. This is also introducing latency that may or may not be acceptable. If other employees fall into the laptop category above, this is something that IT can "test" pretty easily. There is also a difference between functionally working and practically working. If an employee's productivity is cut by 75% due to performance is this really a worthwhile solution?

Option 1 – Transport Your Existing Corporate Desktops

One option would be to have each employee take their desktop home. Not ideal but this could be an option. There are some considerations to think through in this scenario. First, let's assume that desktops are set up with dynamic IPs so that when employees get home, they can get out to the web and IT can connect remotely to the device. IT will need to ensure that VPN software is loaded on the PC before the employee heads home. In the current COVID environment, this typically hasn't been possible.

This means IT has a couple of options. If users have admin rights to the PC, IT can simply give them instructions for how to download the software and where to point to connect to the corporate network. However, this is against industry best practices and likely not the case for 75-80% of employees. Instead, IT will need to call each user, remote into their device in order to download and install the VPN software and get the employee connected. Another consideration is the logistics involved with each user taking their PC home.

Option 2 – Use Existing Personal Home Office Device

Another option would be for employees to use their own devices. While this removes the logistics of taking a PC home, and the associated configurations, it introduces a whole host of other possible issues that IT must figure out. Below are five items that will need to be addressed as IT builds out this strategy.

1. **OS Support** – If the corporate standard is Windows, and an employee is using a MAC, that certainly won't work as it stands. There are creative ways to run Windows on a MAC but that's another couple hours of configuration in itself. Similarly, if an employee has a Chromebook, there is no OS to install corporate applications on.
2. **Horsepower** – If the employee has a 4G desktop at their home, and the corporate applications require a desktop with 8G, this again will present a problem that cannot be overcome.
3. **Anti-Virus(AV)** – Chances are good that your employees are not running the corporate standard for AV. This may be an area where IT is willing to bend a bit and accept any AV that is up to date and running as acceptable. But, if the entity is driven by compliancy requirements such as HIPAA or FINRA or many others, the business will need to be more

stringent and remove the old AV before installing the new corporate AV solution.

4. **Management Tools** – Once an employee is using their home device to access the corporate network, IT must ensure that the OS and AV are up to date and stay up to date. To do this, IT must install management software on the device itself.
5. **VPN** – Once all of this is set up, the user will then need to connect to the corporate network and IT must take the considerations with VPN mentioned above into account.

It's important to note, that if either items 1 or 2 above are a "no", IT must purchase a new desktop and have it shipped to the employee. They will then have to complete steps 3 through 5 with the new unit once it arrives. As one can imagine, this could be a logistical nightmare when multiplied over the entire employee population. Especially when it takes roughly 1-2 hours at best to complete steps 3 through 5 as well as the possible outlay of capital for devices that need to be replaced that don't meet the corporate requirements to begin with.

It is also worth noting that while this approach accomplishes the goal of enabling an employee to be productive at home, IT will need to decide what to do after employees have largely returned to the office. Licensing requirements and/or costs along with legal exposure will likely dictate that IT return to each of these devices and remove all the corporate tools that have been installed.

Another Possible Solution

Evolve IP has been providing Work From Anywhere (WFA) solutions for 12 years now. While the most recent bout with COVID-19 has forced many organizations to hastily cobble together workable solutions, Evolve IP customers haven't skipped a beat.

Evolve IP's Workspaces solution allows for employees to work anywhere and expect the same collaborative experience from any device. This not only provides an emergency solution in times such as now, but in other non-pandemic situations such as inclement weather or simply tying up a few loose ends while on vacation away from the office.

The Workspaces solution is designed to give employees all the corporate tools and security protections while using a device that IT doesn't know, or need to know, anything about. The solution also right-sizes the toolset based on each user's specific needs to lower costs in comparison to the one size fits all virtual desktop world.

Learn more at www.evolveip.net/workspaces

About Evolve IP

At Evolve IP we Make Work Better™, ensuring employees are more productive, more mobile, more secure and less dependent on IT resources. We design Purpose-Built® solutions, tailored just for your business, that unify workspaces, collaboration and communications, and contact centers. Integrating blue-chip technology partners like Microsoft, Cisco, Citrix and VMware, with our intellectual property, Evolve IP's analyst-acclaimed solutions have been deployed globally to 500,000+ users and into the world's most well-known brands. All Evolve IP associates are focused on driving successful client outcomes and that has resulted in our scoring at the top of verified analyst and client satisfaction rankings.