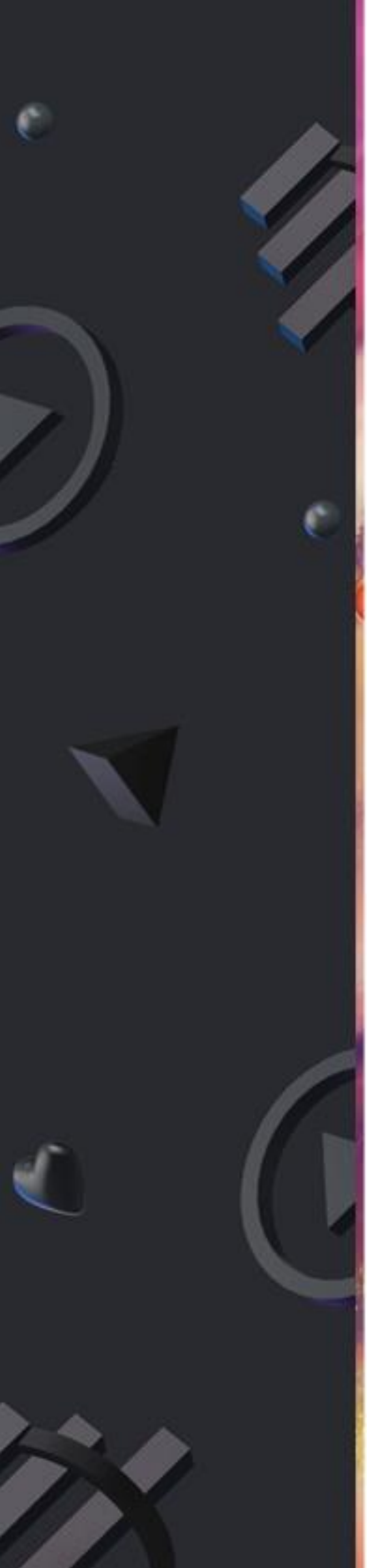


HYSOLATE

Coronavirus: Enabling users to work-from-home safely

Table of Contents

Executive Summary

Due to the COVID-19 (coronavirus) epidemic, more people than ever are working from home to physically isolate themselves and prevent cross-contamination. The good news is that it's easier than ever to enable workers to remain productive while not in a physical office. However, special considerations should be made to secure those remote workers.

The Achilles heel of a remote workforce are the endpoints that remote workers use to connect to corporate and hyper-sensitive environments. Endpoints are vulnerable, especially when they're being used in less-controlled networking environments like homes, libraries, and coffee shops. In some cases, remote workers are allowed to connect from their personal laptops, but this introduces risk as these devices do not normally have the necessary security controls and can be easily compromised in a variety of ways.

To stay in business, organizations must be prepared to enable their workforce to work remotely in a secure and productive manner. They must also take into account the cost, scalability and manageability of the various work-from-home methods.

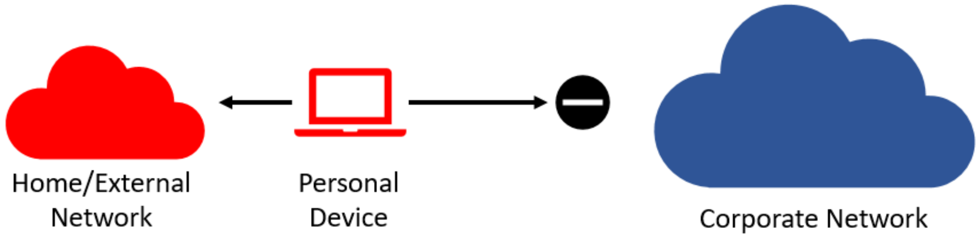
This paper will review 5 work-from-home methods that organizations are employing today and discuss pros and cons of each.

Work-from-home Methods

Method 1: Simply don't support it

Some organizations on the extreme end of the spectrum do not allow employees to access corporate apps or data from home. This applies to some government/military organizations but also to some more conservative enterprises, etc.

Due to the security-conscious nature of these organizations, they should find a secure-by-design solution to enable employees to work remotely in a way that doesn't risk their sensitive networks and can be provisioned immediately without requiring provisioning of new laptops to users.



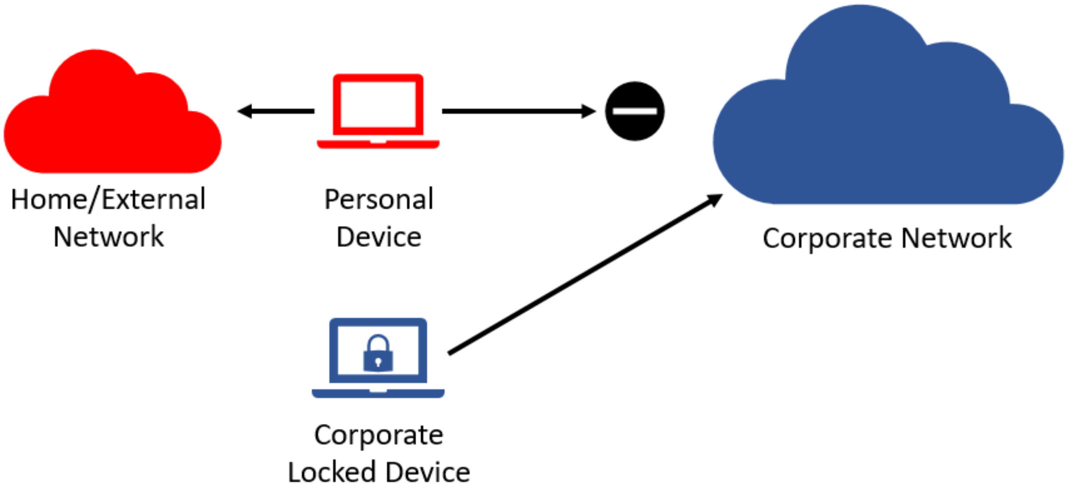
Visualization of Method 1: Simply don't support work-from-home

Method 2: Provide employees with corporate locked-down laptops

Corporate laptops are managed laptops with many restrictions, e.g. they are forced to only connect to the corporate network via an “always-on” VPN solution, users don’t have local admin rights (which prevents installing many productivity applications), they cannot plug in thumb drives, they cannot browse the full web, etc.

Employees are typically frustrated with these locked-down laptops as they are less useful at home. For example:

- Users might not be able to use that laptop to simultaneously work with corporate-related apps and personal apps, which forces them to constantly switch between multiple devices - a factor that degrades productivity and frustrates users.
- Users typically don’t have two sets of peripherals (e.g. multiple monitors, keyboard, mouse, power supply …) at home. This means that switching between their personal laptop and their corporate laptop at home requires them to reconnect peripherals to a different device.
- When users travel, they might need to carry an additional laptop with additional power supply just to be able to work with corporate apps.
- Users might not be able to print with their home printers as the VPN solution doesn’t allow connectivity to their home network and USB policies prevent the connection of USB printers.
- Always-on VPN solutions might introduce friction with various WiFi networks that require authentication or present a “captive portal” before the user can access WiFi.
- Troubleshooting issues with malfunctioning corporate laptops is trickier when done remotely. A corporate laptop that fails to connect to a VPN or received a faulty Windows Update and therefore doesn’t boot, requires re-imaging or re-provisioning of the laptop/OS remotely, which is a time-consuming and complex operation.



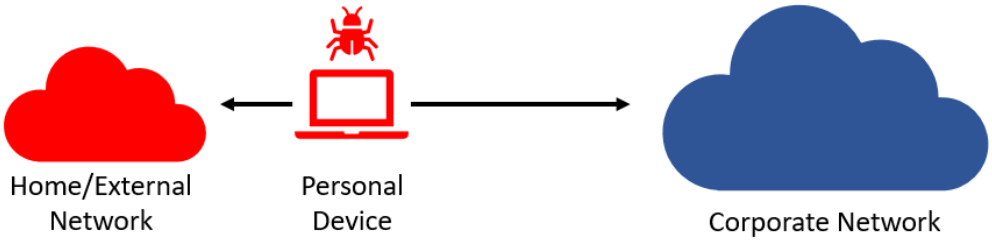
Visualization of Method 2: Provide employees with corporate locked-down laptops

Method 3: Allow employees to use their personal laptops/desktops to directly connect to corporate apps and data

Organizations using this approach might require users to connect through a cloud-based access broker (AKA “Zero Trust”) or simply allow direct connectivity to cloud-based apps like Office365, G-Suite or Salesforce. This approach is typically convenient to users. They might need to provide additional authentication (2FA) to connect, but they can use their existing personal devices (e.g. laptops/desktops).

This approach, however, is the riskiest security-wise:

- Personal devices can easily become infected, in a variety of ways – web browsing, email, infected external devices, malicious user-installed apps, pirated software, malicious networks, etc.
- Once the user’s device is compromised, the attacker can fully impersonate the user and take over his accounts, steal corporate data or harm corporate systems.
- OS health checks (that some zero trust solutions perform) would not help against persistent attackers as they rely on the integrity of an infected OS.
- This architecture makes it easier for insiders to leak data at scale.



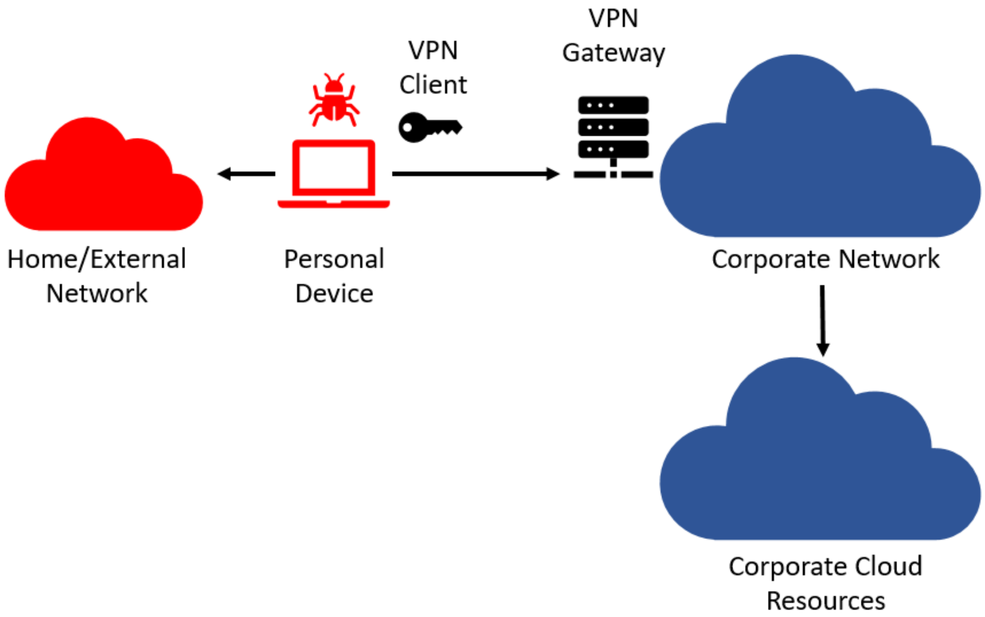
Visualization of Method 3: Allow employees to use their personal laptops/desktops to directly connect to corporate apps and data

Method 4: Allow users to connect from their personal devices, but via a VPN client

This popular traditional option forces users to connect through a VPN for users to access corporate apps and data. On top of the issues mentioned in method 3, this introduces additional challenges:

- The user’s experience might be degraded if his home network connectivity (bandwidth and latency) is not fast enough. Some applications suffer when the network conditions are not ideal (e.g. data-intensive apps).

- If the connection to enterprise cloud-based resources is done via the VPN as well, the user must undergo an unnecessary hop in the network through the corporate network before reaching the final destination in the cloud, further increasing latency and bandwidth issues.
- If the enterprise doesn't allow "split tunneling" (allowing the user to simultaneously connect to the corporate network via VPN and to his home/external network), the user cannot enjoy direct access to cloud resources such as videos and music while accessing corporate resources over VPN. On the other hand, if the enterprise does allow split tunneling, it gives more flexibility to malware that can communicate with a C&C/exfiltration server on the internet (via the home network) while it is also actively connected to the corporate network – this essentially connects the corporate network into the wild internet.



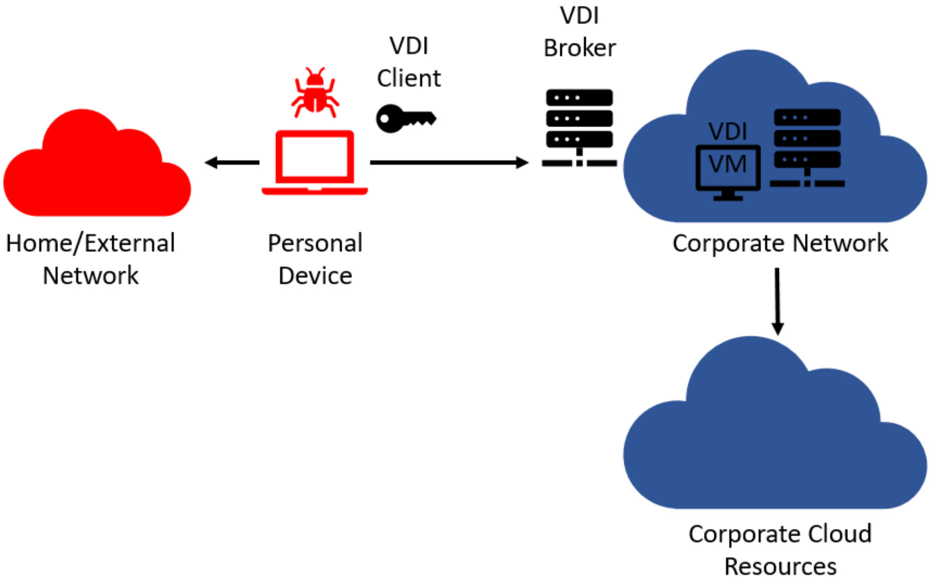
Visualization of Method 4: Allow users to connect from their personal devices, but via a VPN client

Method 5: Allow users to connect from their personal devices, but via VDI

Users will operate their personal laptop for their personal apps and a remote VDI desktop for corporate apps. On top of the issues above, this option introduces additional challenges:

- The user experience of VDI over a bad network connection is terrible - every user interface action the user performs has additional latency which leads to immense frustration for users.
- Some applications such as VoIP, video, 3D and others, don't work properly in a VDI environment.

- The organization’s VDI infrastructure (either on-prem or in the cloud) might not be ready for a massive number of users connecting simultaneously. This means that the user’s experience would be further degraded - applications would not respond, the network would be choked, and the data center underlying storage devices would not be able to serve data for VDI fast enough.
- Users cannot continue working on corporate apps/documents offline.
- The solution is expensive, especially if it needs to support a massive number of users.
- With VDI, malware can still take over the VDI desktop by controlling the user’s physical device.



Visualization of Method 5: Allow users to connect from their personal devices, but via VDI

Key Requirements to Consider

When building a sustainable work-from-home solution, there are some key requirements you should keep in mind to ensure users are productive, risk is mitigated, and IT can easily manage the solution.

User productivity

- Users should be able to use a single device with a single set of peripherals for both personal and corporate access.
- For the best experience, users should be able to connect directly to their apps and data (both corporate and personal) as much as possible, without additional hops.

- The solution must work under bad network conditions with high latency, low bandwidth, and even offline.
- The solution must provide a responsive UI experience to users.
- Users should be able to access resources on their home/external environments, such as network/USB printers, WiFi captive portals, etc.
- Users must be able to have a good experience during peak hours too and when a massive number of users connect simultaneously.

Security

- Access to corporate resources must be done from a safe and trusted operating system.
- The solution must protect against a variety of endpoint-related attack vectors, such as OS vulnerabilities, app vulnerabilities (both corporate and 3rd party apps), network vulnerabilities, browser/mail vulnerabilities, USB/external device vulnerabilities, insider threats, etc.
- The solution should make it hard for malware to simultaneously access corporate network resources and have direct unfiltered access to the internet.
- The solution should assume personal devices can easily become infected.
- The solution must be compliant with the requirements of the organization’s clients, including financial/government entities.

Manageability

- IT must be able to support remote devices and be able to recover in case of endpoint failure.
- The cost and operational overhead of the solution, including data center/cloud/network costs, should be low.
- The solution must be scalable to support a massive number of users.
- It should be possible to provision the remote work solution immediately.

Hysolate provides innovative and secure workstation software solutions that can meet the requirements listed above and enable the enterprise workforce to work remotely in a secure, productive and cost-effective manner. The solution uses industry-standard virtualization technologies to create a strong VM boundary between the operating systems. This allows remote workers the ability to instantly connect into corporate environments via a secure and isolated operating system. With complete OS separation and isolation, the Hysolate solution ensures that even if the users general operating system is compromised, the corporate operating system will remain intact.

With whatever method you choose, it’s important to provide your remote workers with a secure, productive and manageable solution.