Return to the VPLS Blog

Blog Post

A Closer Look at Technologies Enabling Remote Work: VDI vs VPN

John Headley

Filed under

Cybersecurity, VDI, VPN

Government shelter-in-place orders due to COVID-19 have forced organizations to transition their employees to remote work, often for the first time. Unexpectedly, many of these organizations are seeing benefits to this new work-from-home policy—so much so, that leaving in place the ability to work from home even after the orders have lifted is now on the corporate roadmap.

Whether temporary or permanent, there are challenges to implementing work-from-home successfully and securely—internet and infrastructure stability, user access control, and securing company data, just to name a few.

With these challenges in mind, two of the most popular options for setting up a remote workspace are VPN and VDI. It's important to know the differences between each option in order to select which, if not both, is the right fit for your business.

What is VDI?

to any physical computer or even an inexpensive piece of hardware called a "thin client" or "zero client".

After the user authenticates successfully, they will be taken to their personal virtual desktop instance, which provides the user the same experience as if they were using a normal PC. Since the virtual desktop is hosted within the corporate infrastructure, users will also have secure access to corporate applications and files.

What is VPN?

VPN or Virtual Private Network technology focuses on extending the corporate network to a remote PC or remote office. This is accomplished by creating a secure "tunnel" over the Internet between the corporate office and the remote location, which not only secures all data that goes between the corporate office and the remote employee, but also allows the remote employee's PC or office to logically act like it is part of the corporate network.

By simply installing VPN client software or even just using a web browser on the remote PC, the user can access business applications and files just like they were sitting at the office.

Is VPN or VDI right for your organization?

In the context of remote work, both solutions have similar value propositions: they allow your employees to securely work from home. However, this is where the similarities end. Below are some key differentiators to consider when selecting a solution for your business.

SECURITY

The security of a remote access solution gets first priority in this debate. Both VPN and VDI ensure confidentiality and integrity of data transferred to and from the corporate network, and user authentication can optionally be secured with multi-factor authentication in both solutions.

However, VDI does have an advantage if the organization needs to allow users personal devices.

Even with this advantage for VDI, since VPN can be restricted to only corporate-issued devices—and that's the restriction that many of our customers want—we will have to award security as a tie overall.

Winner: Tie

DEVICE TYPE SUPPORT

As mentioned above, VDI provides remote access to a virtual desktop from any device, which is quite convenient, but it provides access ONLY to this virtual desktop. For employees that have non-PC corporate devices, like a desk phone, corporate cell phone, or IOT device, VPN is the only solution that can provide remote corporate connectivity for them.

Note that this type of VPN setup typically mandates a physical VPN gateway appliance be deployed at the user's home office in lieu of the VPN client software we described above.

Winner: VPN

BANDWIDTH

With VPN, the secure tunnel is set up between the user's remote PC and the corporate network, and any attempts to access resources at HQ requires data to traverse this tunnel. This puts bandwidth demands on both the user's home Internet connection and, as the number of users increases, the Internet connection at HQ too.

VDI has less bandwidth requirements compared to VPN because the virtual desktop is already on the corporate network. Only minimal data is sent between the remote user and the virtual desktop itself.

Winner: VDI

USER EXPERIENCE & TRAINING

Users will have to be onboarded and trained when VDI is deployed, as they are

VPN software, but generally speaking, the user experience won’t change for them—their computer (and any other devices) will look and feel the same.

Winner: VPN

IT MANAGEMENT OVERHEAD

Both solutions have similar overhead when it comes to maintaining policies related to user authentication and access control, but if you consider managing the remote users’ endpoints, then VDI and VPN do differ.

With VPN, a responsible organization would have to ensure a remote user’s PC is “locked down” through the use of Microsoft Group Policy and/or MDM software, since it will be this PC that will be actually connecting back to the corporate network.

With VDI, all the virtual desktops are configured and managed in one place: within the VDI infrastructure. This centralization allows for the flexibility of the virtual desktops to be reconfigured or reimaged at any time, with or without the user being present. This is just plain harder to do with remote physical machines.

Winner: VDI

And the winner is…
The goal of this blog post was to share some insight into why VPN and VDI are leading in today’s work-from-home options, and with the benefits discussed above we hope it is easy to see why. Which one is right for your organization depends on your business’ unique structure and requirements, and often our clients will utilize both technologies to satisfy the needs of their diverse workforce.

It’s important to keep in mind that either solution can be set up quickly by an experienced engineer and can be architected to support any number of users an organization requires, both now and into the future.

If your organization wants to discuss the unique work-from-home challen you are facing, such as not having the proper staff to get a solution deployed

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

More from this Author

‹ PREVIOUS
VPLS Advisory – Coronavirus (COVID-19)

NEXT ›
What is EDR? – A Primer in 5 Minutes

BLOG POST

5 Reasons SOC-as-a-Service

Will Give You Peace of Mind

If you're not sure if outsourcing your SOC is worth it, here are some SOC-as-a-Service features that provide peace of mind

5 Reasons SOC-as-a-Service Features Help You

March 29, 2022

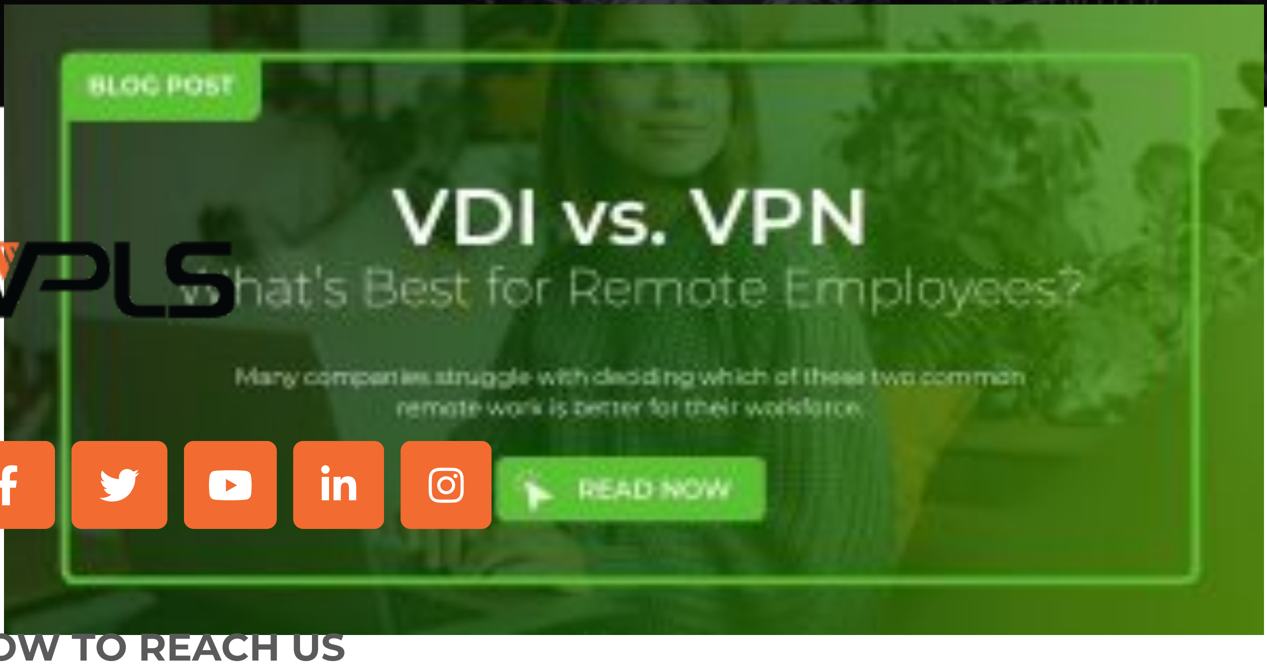
Read More »

What is SOC-as-a-Service?
SOC-as-a-Service (SOCaaS) functions as an extension of a company's IT department and helps take the guesswork out of cybersecurity.
READ NOW

What Is SOC-as-a-Service?

March 28, 2022

Read More »


BLOG POST
VDI vs. VPN
What's Best for Remote Employees?
Many companies struggle with deciding which of these two common remote work is better for their workforce.
READ NOW

VDI vs. VPN: What’s Best for Remote Employees?

February 14, 2022

Read More »

HOW TO REACH US

Corporate Headquarters
600 West 7th Street, Suite 510
Los Angeles, CA 90017

24/7/365 Customer Service
+1 (888) 365-2656

+1 (888) 365-2656
sales@vpls.com

WHAT WE DO

Cloud
Hosting
Colocation
Network Services
Managed Services
Professional Services
VAR

WHO WE SERVE

Financial Services
Healthcare and Life Sciences
Media & Entertainment
Telecom
Startup
Enterprise
Public Sector