Remote Access Security – Going Beyond VPN

A VPN Security Brief

from **AmZetta Technologies, LLC**

amzetta.com
v42021.1

Reacting to Our New Normal

The COVID-19 pandemic of 2020 will ultimately lead to permanent changes in how all of us live our lives. We're seeing that impact most immediately at work. Many of us that were lucky enough to retain our jobs after the pandemic hit were sent home. Our employers, in turn, have adopted what some are referring to as asynchronous work – the flexibility to perform our tasks when and where we can, at any location, using any device, during both traditional and non-traditional working hours.

The pandemic didn't just push everyone out of the office - it changed how we organized our days, how we care for our children, our parents and elders, and how we interface with our communities. This has made, as the BBC succinctly recently put it, working on the same clock as everyone else in our organization nearly impossible.

To accommodate the new post-pandemic work-from-home paradigm, our IT leaders scrambled to find solutions that would keep businesses secure and employees productive. A lot of companies and orgs (perhaps your own) doubled down on virtual private networks (VPNs), securing new licenses and asking remote staff to use this familiar technology to access required corporate applications, data, and computers (via RDP).

More than a year later, employees are still stuck at home, and companies are still using VPN access as the primary method for remote user access connectivity. Don't expect that to change anytime soon – consider some statistics recently published in Forbes Magazine:

As of February 2020, only 3.4% of Americans worked from home. A year later, that number grew to 42%.

In a study cited by Forbes, more than 65% of workers would like to continue working remotely once the pandemic has run its course (with 31% in favor of a hybrid work-from-anywhere model).

It appears working from home is here to say. For IT Professionals, the challenge now shifts to shoring up gaps in security and enhancing control of users/devices accessing the corporate network, apps and data.

IT Focus on Security & Access Control: More Important Than Ever Before

IT decisions around security have always been important. They are now absolutely and undeniably mission critical. Think about one of your employees working at the local Starbucks, utilizing VPN, that opens the door to cyberattack on their laptop because they've failed to keep their anti-virus software up to date. The negative outcomes are legion – customer data exposed, brand reputations ruined, and revenue lost. These incidents aren't new, you see it in the news on a weekly basis. Security has become a top-of-mind concern for most IP Pros.

The options available to create the right infrastructure to support work-from-anywhere have been around for years. There are pros and cons to each depending on which vendor you engage. Some companies have doubled down on their VPN licenses. While others have adopted or expanded their use of Virtual Desktop Infrastructure (VDI) solutions. Whereas others have adopted a hybrid approach – using a combination of technologies including Secure Gateways to deliver the most optimal solution for all parties: remote users, their managers, IT Pros, and senior business leaders.

The goal of this VPN Security Brief is to help IT Pros and business leaders from companies of all sizes understand the options available to them to enhance security for remote access users. We're also here to provide an opinion. Drawing on our own experiences as a global Digital Workspace vendor, combined with recent research conducted by the Tier 1 analysts at ESG (Enterprise Strategy Group), we aim to demonstrate that you can create the right mix of security and user experience by combining what you already use with a few strategic additions.

These additions, offered by companies like AmZetta, don't have to be purchased all at once. Nor do they take months to implement. In this 10-minute read, we illuminate options to help you enhance your remote access security and close a multitude of security holes within your existing infrastructure. Quickly, effectively, without breaking your 2021 budget.

We hope you find this content educational. When you're done reading, we hope you'll give us a look. Flexibility is what we provide. And we do it through a range of Digital Workspace technologies that can easily plug into whatever set up you're currently using.

Thank you for your time and attention.

The AmZetta Team – *Digital Workspace Experts*
https://amzetta.com

Examining VPN:

The Traditional Approach

IT Pros have been using VPNs for more than 20 years as a frontline solution to protecting identity and keeping corporate assets secure from common threats. VPNs have always been at the center of the "Castle & Moat" strategy for IT infrastructure. It's no surprise why so many companies large, medium, and small made the decision to double down on their VPN investment when the quarantine took effect.

But as we'll outline within this Security Brief, remote users accessing the corporate network, on-prem computers, apps and data via VPN is a major security concern – a ticking timebomb that will ultimately lead to a host of negative business outcomes.

To that end, here is a high-level overview for business types reading this Brief about VPNs. Which, at their core, establish a secure, private connection between two different networks.

When a remote user uses VPN, they create a secure tunnel that allows them to access the corporate network. Before VPN can be used, a local client needs to be installed on the specific device the employee is using that particular day to access the corporate network (device use, in this era of BYOD, can vary).

The VPN must have policies configured for routing the remote user to the appropriate destination within the corporate network. These policies become complex and a burden to manage by the IT Department as a lot of remote users wear multiple hats, requiring different levels of access to various data sets, apps, network folders, systems, etc. Most VPNs initiate the connection with single-factor authentication. Meaning, the employee only has to prove who they claim to be in a single-step process - enter username and password. Done.

VPNs weren't designed to support the new paradigm we're living in post-pandemic. They were meant to support a handful of disparate remote users, and to give any employee the ability to access the corporate network when working outside of the physical office. They were designed to support temporary connections to the localized corporate data center. The problem is that VPNs were not designed to support a remote workforce fulltime.

VPN Security Holes:

Your Corporate Environment is Exposed

It's no surprise the majority of IT Pros reached to the very familiar VPN solution when COVID-19 hit. It's what most of us know. Like we noted earlier, VPNs have been around since the dawn of the digital age.

How many of us have been at one of our kid's games while logged into the corporate network through a VPN client installed on a personal iPhone? Most of us. And with asynchronous work accelerating, these kinds of situations are set to increase. Exponentially.

IT Pros accessing the VPN while watching their daughter play softball are likely to be cognizant about their personal behaviors and their potential impact on security. Most remote users outside of IT just don't think that way and are largely oblivious to the threats and risks that come from accessing the corporate network away from the office on an unsecure connection via a personal device.

Let's take a look at some specific, and potentially deadly, VPN-related security threats. Three stand out:

1. Cyberattacks on the Corporate Network

The vast majority of VPNs deployed are L3/L4 VPNs. When remote users are connected to the corporate network through an L3/L4 VPN, the endpoint device is bridged to the network. This joins the endpoint device to the network as a trusted device from a trusted outside network. The endpoint device is issued a virtual IP address which is routable within the corporate network.

This is a major security issue as anything and everything present in the endpoint device and on the remote network, from malware to keylogger software, will have the same corporate network access as the user. In this context, any malware attack at the endpoint or remote users network is capable of spreading and infecting the entire corporate network and all the other devices connected within the corporate network.

The exposure of the corporate network also allows malware to discover the internal network topology for the planning of future attacks (think WannaCry ransomware). Thus, despite providing seamless connectivity, VPN vastly increases the potential to let malware into the corporate network.

Your Corporate Environment is Exposed *(cont.)*

Cybersecurity has emerged as one of the major concerns for organizations in the remote work scenario. Generally, cyber-attackers choose an inherently trusted end user's device – be it a laptop, notebook or any home device. The end user can be anyone, an employee, a consultant, a student, a vendor - anyone with VPN access (often referred to as "frenemies" in the cybersecurity industry).

Basically, anyone who has VPN access to an organization's network in any form can be an entry point for malware. Once in the network, the malware spreads. The threat level has significantly increased during the pandemic with so many users working remotely, utilizing a host of different networks and devices. Your safety is in the hand of less aware employees that may or may not heed the directions from IT leaders around virus and firewall protection.

Scary indeed! Let's move along to the second most common VPN security risk.

2. Unsecure Devices, Local Company Data at Risk

When connecting via VPN, the user is accessing corporate applications with original corporate data stored in the endpoint device. The very stealthy, malicious forces residing in endpoints (unseen and unnoticed by remote users) now have full access to any corporate files stored locally. That opens the door to theft or corruption of company-owned customer data. If VPN access is initiated from an endpoint device that is not secure, then the risk of a malware or cyberattack looms large. How can you ensure that every device is secure and clean before it opens a VPN tunnel into your network?

You can't.

With VPN, BYOD policies and remote access from third-party networks create a potential disaster and a nightmare scenario for your IT Pros responsible for security.

3. Data Breech or Theft by Remote Users

VPNs do not provide any features or functions to prevent data sharing between the user endpoint device and the corporate network. Remote users can do anything from their endpoint devices that they could do while working from the office – they can copy & paste data, take screenshots of highly sensitive data, record screens. If this happens, the IT Department won't have any control and the company is left wide open to massive leaks of highly sensitive customer, product, patient and/or employee data. It happens on an almost daily basis.

The pandemic has been a boon to a legion of immoral hackers who are chomping at the bit to take advantage of remote users using less-secure home and public networks. They are looking for any opportunity to get inside. Once they've accessed someone's corporate network, they can wreak sever damage or hold the business hostage in return for some kind of ransom payout.

Here at AmZetta, we've supported customers that have contracted the WannaCry Ransomware through basic VPNs. The virus created complete chaos and brought productivity to a screeching halt for days (even weeks). WannaCry attacks are silent. The ransomware works its way into the customer's storage backups (local snapshots, disaster recovery, etc.). In our experience, cybersecurity experts had to be brought in to fix the damage. These highly skilled resources don't come cheap; we're talking hundreds of thousands of dollars here.

With VPN, BYOD policies and remote access from third-party networks create a potential disaster and a nightmare scenario for your IT Pros responsible for security. Continued reliance on VPN as a permanent solution to for remote work plays right into the hands of the hackers. Relying on VPN as a permanent solution to support remote work plays right into the hands of the hackers.

Houston, we have a problem with VPNs for Secure Access.

VPN Security Mitigation:

Filling in the Security Holes

Now that we have a baseline understanding of the main security issues associated with long-term reliance on VPN, let's take a closer look at the options available to IT Pros that go beyond VPN.

Here are eight specific steps you and your organization can take right now to improve security while you still have a VPN in place.

STEP 1.

Prevent VPN L3 and L4 Access

Move to a VPN L5 to L7 access to deliver applications to remote users and devices. Instead of allowing access to the entire Corporate Network, this allows IT Pros to limit remote user access to only those apps they need to do their jobs. If a virus, malware, or any other threat, does manage to get into a remote user's device or home network, there is no threat to the corporate network as there is no longer a connection from remote users to the backend corporate network. This is a great first step towards developing a Zero Trust Network Architecture.

STEP 2.

Endpoint Onboarding & Identification Verification

You can onboard remote user personal devices quickly using an HTTP Secure Browser. Push the URL to the users and they won't have to install anything themselves on their local device. The remote users can login to the browser and access their apps and data. This is a very fast, highly efficient and secure method to onboard new users and devices. If your users require the full software client to be installed (for enhanced video and audio) on their endpoint devices, then you can auto-identify and cleanse the remote users' devices to remove any pre-existing viruses, malware or keyloggers prior to allowing the device to join the network. Only allow clean and authorized secure devices to connect to the VPN L5 to L7 Access for strict device control and security. Make it part of your BYOD policy.

STEP 3.

Endpoint Security Access Level Monitoring

Inspect and verify the security access level of all endpoint devices when they login and throughout every active session. Any endpoint devices that can support split tunnelling should not be allowed to join the network.

STEP 4.

Contextual Based Access

Parameters such as geolocation, login time and source IP address should be activated to monitor endpoint devices. Only allow access to trusted onboarded devices for connectivity to folders/files, apps, URLs and etc. Setup rules within the VPN L5 to L7 for real time approval or rejection of remote access. Convert to a "never trust, always verify" model that's based on context, and grant the minimum amount of access privileges required for each individual remote user.

STEP 5.

Implement MFA (Multi-Factor Authentication)

Enable MFA for all remote users. MFA is a secure authentication verification step that goes beyond username and password. MFA challenges the user to provide additional security information to prove who they are before they are granted access to the corporate network or corporate apps. Options for MFA include: A) OTP (one-time password) available via the remote user's mobile device, email or "push" notifications and B) biometric verification via fingerprints or iris scans. Companies must support an Identification and Access Management (IAM) solution as a further means of protection from external threats.

Filling in the Security Holes *(cont.)*

STEP 6. Ditch the Desktops & Host the Apps

If your users are accessing in-office desktops or corporate apps, then deploy Virtual Desktops (VDI) and Virtual Apps. Reclaim the desktops and move the corporate apps into a virtual app hosting environment. In this situation, the remote user can only access their specific VM within the VDI infrastructure.

In the event of a virus or malware attack, only that specific VM is affected. The VM can be purged and a new VM can be spun up in minutes using the VDI template. With VDI, the virus or malware is contained to the specific VM tied to the user with the security issue. This ensures no data corruption or data loss that comes from data stored within the VDI Server (and not within the users VM). Thus, any virus attack will fall flat and the VDI solution will remain secure – operating at full capacity.

A major advantage of VDI is the centralized storage of data and reduction of IT management responsibilities. All the data is stored within the centralized VDI solution where it is scanned by the IT Department's virus protection software/tools and backed up for redundancy. No longer is user data stored locally on users' devices where it can be compromised. ESG's parent company – Tech Target – does a good job of explaining VDI in layman terms:

TechTarget

"VDI was designed to stream virtual computing desktops to nearly any PC or smart device. One advantage of VDI is that, with VDI access, the user's hardware compartmentalizes everything performed within this virtual computing environment. This makes VDI much more secure from the perspective of data loss prevention."

A VDI solution is centralized, and all management takes place on the VDI Server, no longer on the endpoint devices. That means software updates, device updates and user issues are no longer remote support headaches as everything is centralized with VDI and Virtual Apps. This makes it much more efficient from an IT management perspective. Go ahead IT Pros: head out to a ballgame this evening and get back to your life outside of the corporate IT Department!

STEP 7. Session Cleansing

Implement a process that deletes or cleanses all session data (temp files, cookies, browser history, etc.) when a user logs out or their session times out.

STEP 8. Keylogger Detection

Prior to an active session, you can enable a check to detect keyloggers on the endpoint devices. If any keyloggers are identified within an endpoint device, then that device will be restricted from accessing the network.

Okay, so now we know the 8 steps to help you mitigate the security threats exposed from using a VPN for remote access. It's one thing to know about a cure. It's another thing altogether to implement them.

We'll show you how in this next session. Don't worry – these fixes are really easy, fast, and cost-effective.

Implementing the VPN Security Mitigation Steps

We want to stress the point, through this Brief, that we don't believe you need to rip out your current VPN. It still has an important role to play. But as demonstrated, VPNs do have security holes. The technology just wasn't invented to support the new post-pandemic normal. VPN security can be enhanced by adding additional layers of security through the adoption of other infrastructure technologies. Some companies may choose to ditch VPN altogether to avoid paying for any new user licenses. Many will make the wholesale change to a more secure access control solution. In this section, we explore two options so you can make an informed decision that's right for your organization.

Option 1.

VPN + SECURE SOFTWARE GATEWAY

The first option is to combine your existing VPN with a secure software Gateway. A secure software gateway represents one component of a larger digital workspace solution. It offers a secure path for remote users connecting from any network using any device. Secure Gateways also provide a much higher level of containment and enhanced security.

Once the connection has been established by the remote user, they will only be able to access the corporate resources that have been assigned to them. This is where App Tunneling comes into play – users can only access those apps that have been deemed necessary by their managers. This "containment" feature will block all malware and viruses from entrance. The secure software gateway can be accessed via a browser or from a software client installed on the remote user's endpoint device(s). The secure software gateway includes a multitude of baked-in features like Multi-Factor Authentication (MFA), Single Sign-On (SSO, and much more.

A secure software gateway also provides a base level of analytics into how remote users are spending their time. Something people managers want post-pandemic.

The VPN + secure software gateway combination works well for those businesses that have their current IT infrastructure on premise but are planning to bring them into the cloud over time. We call this a Hybrid IT Infrastructure as apps, data and workloads are split between On-Prem and Cloud environments. In this scenario, the VPN is used as a point-to-point connection between the On-Prem and the Cloud.

Option 2.

RIP-AND-REPLACE THE VPN

Depending on the size and type of your business, a wholesale switch away from VPN to a secure software gateway can be the best option for the company and the IT department. Implementing a Zero Trust Network Access (ZTNA) solution is top-of-mind for a lot of midmarket companies today. ZTNA uses the secure software gateway to make the entire infrastructure more secure. Implementing ZTNA focuses on enabling advanced security features that creates a "trust no one, verify everything" structure.

For example, accessing the network automatically requires a full security sweep of the device that's trying to gain access. Based on that sweep, a device is placed into a specific threat category, further restricting or granting specific access. Security on top of more security. Enable the MFA and you've got a serious hedge of protection around your business, giving you the security you need as your business scales over time.

But will a Secure Software Gateway really close all the Security Holes in my VPN?

Absolutely, in both Option 1 and Option 2 outlined above, the secure software gateway will resolve all the VPN security holes identified within this brief. Further, the secure software gateway will provide a comprehensive, zero-trust-based end user computing solution, enabling secure and instant access to business applications from anywhere, any device and any network.

A VPN Security Brief:

Finding the Right Secure Software Gateway Solution

AmZetta is a full-service Digital Workspace vendor that offers customers multiple components within a secure software gateway solution. The AmZetta Digital Workspace suite includes End-user Computing Virtualization via application & desktop virtualization (VDI), zero trust-based Application Access Gateway and Identity & Access Management solutions (which helps organizations to roll out a remote work solution swiftly within hours).

Integrated MFA, device entry control, data leakage prevention, contextual access, user experience and monitoring features make it perfectly suitable for Work-from-Home (WFM) and Hybrid Remote user scenarios as well. It takes care of all remote access, application virtualization, VDI, MFA, identity federation, SSO and even thin clients, sparing organizations the need to juggle multiple products or manage multiple vendors. The AmZetta Digital Workspace solution is highly modular to fit the needs of businesses of all sizes, providing seamless access to modern web applications, SaaS applications, client-server applications, legacy applications, virtual applications and virtual desktops.

AmZetta has the complete end-to-end Digital Workspace solution you need. Period.

Digital Workspace – Installation, Configuration & Training – Under 4 Hours

Digital Workspace solutions are not hardware solutions. They are a software-defined solution that can be installed in any virtualized environment, on any virtual machine (or as bare metal on any server). The installation and configuration is simple and most production environments can be installed, configured and tested in under four hours. At AmZetta, we start with the authentication server and the assignment of proper access controls. Virtualized application and integration for the VDI and hosted apps will also be established. Finally, the gateway client and secure browser functionality will be used to validate remote connection and access. During the configuration, MFA will be enabled to demonstrate user and endpoint authentication for ensuring user access and permission methods are configured to meet defined security requirements.

Following the configuration, we focus on training you and your team to manage the Digital Workspace. You will learn to configure users and groups and assign users to controlled virtual applications and virtual desktops. Next, we will train you on the MFA options available. We also walk you through a demo of profiles so you and your team can see the flexibility of authentication management and access control. We will train you on the virtual applications and virtual desktops as well as the available management functionality required to fully support VDI. We will wrap up the training with a review of the reporting server, showing you how to navigate and capture various environment metrics, logs, and graphs. The goal is to give you full visibility into users, desktops, and applications.

malware attack at the endpoint or remote users network is capable of spreading and infecting the entire corporate network and all the other devices connected within the corporate network.

The exposure of the corporate network also allows malware to discover the internal network topology for planning the attack in the future (think WannaCry ransomware here). Thus, despite providing seamless connectivity, VPN vastly increases the potential to let malware into the corporate network.

A VPN Security Brief:

Finding the Right Secure Software Gateway Solution

Now that we've laid out a range of options for improving security around your current VPN investment, we think it's important for readers to have a sense as to the direction of the overall market. The data is clear: more and more, businesses and organizations are turning away from VPN in favor of alternative solutions.

To that end, we recently reviewed a new piece of research from senior analysts at the Enterprise Strategy Group (ESG). In November of 2020, ESG published findings from a 2020 survey in a paper entitled **ESG Research Report: Trends in Digital Workspaces, VDI and DaaS** ("desktop-as-a-service" which is the cloud hosted, managed service version of VDI).

In the survey, ESG engaged with 354 IT Professionals across a range of North American businesses and public sector organizations. ESG's sample pool did NOT skew towards large global entities. The data cohort for the survey included growing mid-market organizations (past startup, but not quite North of $100m to $200m), as well as some smaller orgs comprised of less employees. Those surveyed came from a broad variety of verticals including financial services, manufacturing, tech, retail, government (state/local/federal), and services.

In the survey, respondents were asked to identify their "biggest priority" when it comes to delivering applications, data, and desktops/devices. Given the circumstances of the pandemic, one would think security would top the list.

The Top Three Responses from Those Surveyed:

1. Improving employee collaboration.

We interpret that as "keep these remote users productive, engaged with colleagues and happy".

2. Detecting security incidences, vulnerabilities, and risk.

Interpreted as "keep us secure while everyone is working from home accessing the corporate network, apps and data". A very close second to employee collaboration (difference of a single percentage point).

3. Managing user expectations of access, device choice, and application preference.

This one didn't surprise us. Remote users - working strange, asynchronous schedules – are likely to use every device in their home: their company-issued laptop, their own tablets, their personal phones, etc. Onboarding all of these BYOD's became a major support headache for a lot of IT departments.

The trend lines are clear: businesses are moving beyond VPN into Digital Workspace solutions that more closely resemble the Zero Trust Network Access (ZTNA) model. Remote work is here to stay. And as ESG found, IT Pros are looking to find solutions that make long-term remote user management easier, more secure, and better for the individual remote user.

A VPN Security Brief:

Wrapping Up

The developers and engineers at AmZetta understand the pressures facing IT Pros in the new post-pandemic world. In that spirit, we've made the eval process for our Digital Workspace suite very simple. You can choose to install it within your existing infrastructure, or you can test it in our AmZetta Cloud Demo instance. We only need about four hours of your time and a few VMs to install it in your existing infrastructure.

If you prefer the AmZetta Cloud Demo instance, we can provide instant access as soon as we receive the completed form below. We encourage you to give AmZetta a test drive. You will immediately see why it makes to use a Digital Workspace solution to plug all you know are sure to come as you continue to rely on VPN to support remote user access. Just click on the appropriate link below and a Solutions Engineer will be assigned to you promptly.

Digital Workspace Evaluation

https://amzetta.com/contact-us/proof-of-concept/
(Installed in your IT Environment)

Digital Workspace Cloud Demo

https://amzetta.com/demo/
(Access to a Live Digital Workspace Instance)

Digital Workspace Price Quote

https://amzetta.com/pricing/
(Configurator to Build Budgetary Pricing)

AmZetta Technologies

5555 Oakbrook Pkwy, Suite 280
Norcross, GA 30093 USA

Phone: 1-770-246-8750
Sales: 1-877-991-1809
Email: sales@amzetta.com

Citations

The following were sourced in the writing of this VPN Security Brief

1. November 2020: ESG Research Report: Trends in Digital Workspaces, VDI and DaaS
2. April 2021: BBC Worklife (www.bbc.co.uk/worklife)
3. May 2020: ITProportal.com "To VPN or Not to VPN?"
4. May 2020: Searchnetworking.com (TechTarget) "What's the difference between VPN and VDI services?
5. July 2020: Medium.com "Remote Access: The differences between VPN, RDS, and VDI"
6. July 2020: Hrexecutive.com "HR leaders play to embrace remote work post-pandemic"
7. October 2020: Entrepreuer.com "Here's why work from home has been ideal for introverts"
8. October 2020: Windowsreport.com "VDI vs. VPN: Which one is better & the main differences"
9. December 2020: Forbes Magazine "Could 2020 be the year Remote Working becomes the new normal?"
10. April 2021: Forbes Magazine "Why the Asynchronous Work schedule is the future of business"