

Secure Remote Access for the Modern Workplace

Enable your employees to work securely from anywhere

timus
ZERO TRUST NETWORK PROTECTION

Introduction

It's no secret that the rapid pace of technological change has fostered a preference for remote working. Over the last two decades, there have been signs of a growing, albeit gradual, shift to remote work, and this trend increased exponentially during the COVID-19 pandemic. The change was rapid and completely unprecedented, taking many organizations that lacked the necessary security infrastructure by surprise. Many organizations quickly adopted hybrid and remote working policies to maintain their operations and protect employees. Since then, IT departments have continued to employ business applications and desktops in the cloud while allowing remote employees to use unmanaged devices and insecure networks. But no matter which endpoints (laptops, smartphones, tablets, servers, etc.) employees are using, accessing company databases from external locations can pose novel forms of risk.

Whether your company has only a few remote employees or a large remote workforce, every additional endpoint is potentially vulnerable to cyberattacks without the right counter-measures. But with cloud-based secure remote access solutions, you can bolster your overall cybersecurity strategy and protect your networks and data from being compromised.

© Timus Networks, Inc. 2025. All Rights Reserved.

If any novel technology has come to the fore during the pandemic, it's remote access technology, due mainly to the prevalence of hybrid working conditions. Before the pandemic, IT departments relied mainly on virtual private networks (VPNs) to provide distributed workforces with secure remote access. But with increasing scalability demands from remote users, new security architecture requirements of SaaS and web-based apps, and advanced cybersecurity threats in the cloud, VPNs and traditional network security tools are no longer sufficient.

In today's modern work environment, "secure remote access" refers to security procedures and solutions to prevent unauthorized access to digital assets and stop data theft. A secure remote access solution may be comprised of several different methods. As companies look into the future of hybrid work to boost user productivity and ensure granular security in remote work environments, many are now moving away from VPNs in favor of "Zero Trust" architectures to secure their hybrid infrastructures.

If you're not familiar with this approach, this white paper will help you better understand the concept of secure remote access and the difference between ZTNA and traditional VPNs. It will also explain how to secure all your remote work activities within a cloud-based, zero trust framework.

If any novel technology has come to the fore during the pandemic, it’s remote access.

© Timus Networks, Inc. 2025. All Rights Reserved.

Contents

What is Secure Remote Access? 4

How does Secure Remote Access Work? 5

Why is Secure Remote Access Important for Today's Workplace? 6–7

Which Key Technologies are Used for Cloud-Based Secure Remote Access? 8

Legacy VPNs vs. Cloud-Based Zero Trust Secure Remote Access 9–10

Conclusion 11

© Timus Networks, Inc. 2025. All Rights Reserved.

What is Secure Remote Access?

What it means to provide secure remote access has changed considerably in recent years because of new technologies and the pandemic. In its most basic sense, secure remote access means having location-agnostic connectivity among enterprise users, centralized applications, resources, and systems, especially cloud-based ones.

With the increase and prevalence of internet-connected devices, an organization's workforce no longer has to be squeezed among the walls of a physical office. Instead, employees can connect to their organization's internal network and access sensitive data from anywhere in the world. This means that traditional access security measures are no longer sufficient and must be replaced with security measures that provide employees and other authenticated users with safe and secure access – from any location and any device, at any time.

What is secure remote access? The answer is very different today than in 2019.

The first step toward implementing secure remote infrastructure is to ensure that employees have consistent and secure remote access to all necessary applications, resources and services. No matter how flexible your remote work environment is, remote access security represents a core element of your infrastructure. A solid secure remote access strategy can mitigate risk, improve the user experience, and provide a competitive advantage in the digital world.

The goal of secure remote access technology is to connect geographically distant users to the resources they need to do their jobs without compromising network security. Until recently, a typical organization only provided remote access to a limited number of IT administrators – and even fewer business users. But following the emergence of the global pandemic, secure remote access became a requirement for almost every employee.

As one Gartner analyst has put it, the answer to the question "What is secure remote access?" is very different today than in 2019. Because today, secure remote access means that any employee can access any application anytime, anywhere. IDC estimates that, by 2023, ongoing digital transformation and continued business volatility will prompt some 70% of G2000 organizations to employ remote or hybrid-first work models. In other words, the need for secure remote access is here to stay.

© Timus Networks, Inc. 2025. All Rights Reserved.

How does Secure Remote Access Work?

By 2025, 70% of the global workforce will work remotely for at least five days a month. Wherever they happen to be working from, meanwhile, you can help your remote employees stay productive and secure them against any possible threats. A well-designed remote access tool can provide the secure connections to target systems and prevent unauthorized access. The following steps describe a general secure remote access process and apply it to most enterprise remote access architectures.

1 **Policy**
Security policies regarding access to corporate resources should be established and applied to all employees. Guidance should be provided to employees to help them establish secure access to the organization's networks.

2 **Authentication**
A remote access session begins with the authentication of users and other entities, such as systems and applications, through an identity and authentication process.

3 **Authorization**
Before authorizing a remote access session, it's imperative to define who can access which system, at what time and from which device, and what actions can be performed.

4 **Controlled Access**
After successful authentication, the user is granted controlled access to designated systems in the corporate network, based on least privilege or role-based access control principles.

5 **Encryption**
Remote access sessions (RDP, SSH, SQL or VNC) should be tunneled via secure, encrypted paths without the need to provide any credentials.

6 **Tracking**
Admin teams must be able to block or terminate suspicious remote access sessions, and secure remote access tools must give alerts in the event of abnormal activities.

7 **Monitoring**
Audit logs can be sent to security-information and event-management (SIEM) systems to provide insights into remote access sessions.

8 **Training**
As part of their security and compliance training, all employees (and anyone else with access to corporate resources) should be reminded not to click on any unsolicited emails or any links contained therein.

© Timus Networks, Inc. 2025. All Rights Reserved.

Why is Secure Remote Access Important for Today's Workplace?

The number of companies operating remotely, either fully or partially, has skyrocketed since the emergence of the COVID-19 pandemic, and many employers intend to keep it that way. The 2021 PwC survey found that 83% of employers believe their shift to remote working has been successful, while 55% of employees say they would rather work remotely – at least three days a week – in the post-pandemic period.

In preparation for a permanent shift to a hybrid or remote work model, employers must take appropriate security measures to protect business data wherever their employees happen to work.

IT departments must provide secure and reliable cloud-based access options.

1. Access to all data center and cloud-based applications
2. High-quality user experience
3. Threat protection for all devices, locations, and networks
4. Streamlined deployment and centralized management
5. The ability to scale up or down in line with changing business needs



In the post-pandemic period, 55% of employees prefer to work remotely at least three days a week.

© Timus Networks, Inc. 2025. All Rights Reserved.

Using secure remote access systems has four key benefits.

Secure access from any device

Users can enjoy the same high level secure access that they formerly had when they worked in an office. Authorized users can access company networks, specific applications and data based on their roles and responsibilities. That is the most important benefit of a secure remote access strategy, as many people will continue to work remotely.

The shift to remote work has allowed companies to protect and modernize their cybersecurity systems. In this context, companies should invest in updating their cybersecurity policies and educating their workforces on the importance of secure access.

Safe internet browsing

Organizations rely on a range of web-based and internet-oriented applications. As a result, users need protection when they're connected to an organization's on-premises resources and any time they're online. Secure cloud-based remote access protects employees from web-based threats, such as phishing, ransomware and malware, whenever they log on to your company network. Such cyber threats can lead to unauthorized access by outsiders and the loss and theft of corporate and personal data.

Robust endpoint protection

Secure remote access is of little value unless all endpoints are equally protected. As employees use more and more devices to perform their work, it is also critical to protect laptops used to log in to video meetings, tablets used for inputting data, and smartphones used to reply to emails. A secure remote access solution can protect all the devices linked to your company's network and systems. Employee-owned devices must also be installed with the same endpoint security features as those provided by the organization.

Improved efficiency

Employers can ensure their data security with secure cloud-based remote access solutions, while IT and engineering specialists can troubleshoot users remotely. Whenever a technical problem arises, a specialist can remotely access the user's device and help them find a solution without a need for face-to-face interaction or bringing the device to the office.



© Timus Networks, Inc. 2025. All Rights Reserved.

Which Key Technologies are Used for Cloud-Based Secure Remote Access?

Secure remote access is not a single technology; rather, it is a collection of technologies that together provide the security needed whenever users work from home or from other locations. There are several options for securely accessing devices or applications from distant locations, some of which may be used simultaneously, depending on the level of access and security required. The following are some of the more common types of secure remote access systems.

Virtual Private Networks (VPNs)

VPNs provide a layer of security for any device working remotely. They provide secure internet access for users by routing connections through encrypted tunnels. Users can then work via home or public Wi-Fi networks and access their business applications.

Endpoint Protection (EPP)

Devices on a company's network, including mobile phones, laptops, desktop computers, and servers, can be protected by using endpoint security solutions. Typically, antivirus and firewall software are installed on every device to ensure security.

Zero Trust Network Access (ZTNA)

ZTNA provides secure remote access to applications and services based on organization's predetermined policies. Organizations can enforce their policies granularly based on the location or type of device being accessed, allowing them to limit access from undesired devices and networks.

Network Access Control (NAC)

This is usually determined by an organization's administrators. It allows them to restrict access to external users – as well as users within the organization – who do not require access.

Single Sign-On (SSO)

This is a user authentication process that grants users access to multiple devices or applications through a single set of credentials. The software allows the user to log on to their computer, email, mobile phone, or any other system or device, with the same credentials. SSO lets users sign into their devices faster, while allowing the organization to manage access rights easily.

Privileged Access Management (PAM)

This is a set of tools that administrators use to secure and monitor access to system data from various accounts. It allows them to see which users are accessing which applications on the system, ensure that they are secure and identify any suspicious activity.

© Timus Networks, Inc. 2025. All Rights Reserved.

Legacy VPNs vs. Cloud-Based Zero Trust Secure Remote Access

The security needs of businesses have evolved markedly in recent years. Today's workforces are adept at securing traditional workforce models but require solutions that can authenticate users outside the network and prevent unsecured devices from accessing company data.

Legacy Security Solutions are No Longer Effective

Traditional security solutions are no longer effective. For example, passwords remain the most widely used form of authentication, but they are also the leading source of data breaches. Password managers may look safe, but they can be cracked by hackers. Many businesses rely on two-factor authentication as a security measure, but 2FA does not solve all authentication problems. A fourth solution is using VPNs, which made their debut in the late 1990s with a view to digitizing TCP/IP network access for connectivity.

VPNs grant access to the whole network

In use for decades, VPNs provide encrypted tunnels between corporate networks and users' devices. The user has access to all the services and devices in the network as if they were working at the office, because VPNs grant access to the whole network instead of specific targets in the network.

Any program running on the device of a user, be it an authorized user or malicious hacker, can connect to the company's network through the VPN connection. It only takes one bad actor to infiltrate a system, carry out an attack, and potentially damage your company's network.

While VPNs provide remote access to corporate networks and resources, they do not prevent risks associated with passwords and offer little in terms of overall security.

So, what is the best course of action for remote workforces in terms of network security?

© Timus Networks, Inc. 2025. All Rights Reserved.

Better Solutions to Secure Your Remote Workforce

Company executives are responsible for protecting their organization's data, systems, and intellectual property. It is critical to use the right technology to ensure that system access is secure and convenient. Passwords should be complemented with extra measures that are simple to implement and unobtrusive to the end-user.

These requirements are met by risk-based authentication (RBA) solutions. This approach evaluates a risk score for each access request, protects against sophisticated security breaches, and mitigates issues associated with passwords and one-size-fits-all authentication methods.

To mitigate risks associated with bring your own device (BYOD) and ensure compliance with a zero trust architecture, security standards must be both practical and enforceable, especially in terms of mobile devices. Without a method for enforcing your organization’s mobile device policies, you will continue to lack the essential security needed to protect against password-based attacks.

With the threat landscape becoming more complex and workplaces changing to accommodate remote users, many modern businesses use a zero trust security architecture to prevent, detect, and respond to cyber threats. This requires all users, both inside and outside an organization's network, to be authenticated, authorized, and continuously validated with security configuration and posture checks before being granted access. These simple principles will help protect against identity-related and access-based security risks.

Don’t inherently trust any device, user, or transaction

Zero trust is a strategy that replaces traditional perimeter-based security. It focuses on users, devices, apps, and assets. Extending trust policies beyond network access can go a long way toward improving corporate security. Attack surface is reduced by constantly forcing users and devices to authenticate and limiting access only to files and data needed for a given task.

© Timus Networks, Inc. 2025. All Rights Reserved.

Zero trust protects applications and data from new threats by relying on robust user authentication and device validation, in addition to network and endpoint security. It focuses on application and surface-area protection rather than security enforcement at the boundaries of a network. Users and devices are not automatically trusted just because they're within the corporate perimeter or connected to a trusted network.

While every company may approach zero trust differently, the fundamentals remain the same. These include validating trust in each access request and enforcing granular access privileges across all applications and networks.

Conclusion

The cloud revolution has drastically changed the way most businesses function. In the past, offices were entirely independent, and everyone accessed data locally. But as remote working becomes the new norm in the post-pandemic period, employees will no longer be confined to a single physical locatio. Company assets now reside in the cloud in order to take advantage of this newfound mobility, with employees able to easily access them from wherever they happen to be at the time.

Remote working not only helps organizations reduce travel and office expenses, but also provides a convenient and flexible work routine for employees. However, remote access to company resources has also given rise to novel security risks, which require new and improved security methods. Using a VPN may seem like a good defensive strategy, but VPNs alone are not a full proof solution for dealing with today's cybersecurity risks.

The best secure remote access involves striking a balance between optimal security and a great user experience. Otherwise, employees will spend more time checking in than actually working, leading to higher costs, less productivity, and ever more calls to the IT Help Desk.

VPNs initially helped companies manage small numbers of employees and third-party contractors who needed to access certain systems while working remotely. The use of VPNs on a large scale, however, led to a degree of unpredictability, and created headaches for IT departments due to larger surface areas for potential attacks.

For many businesses, remote working has become the new norm.

© Timus Networks, Inc. 2025. All Rights Reserved.

The truth is that remote access security is a much more elaborate process, requiring a variety of security strategies and protocols and having the latest technology in place.

Whether it's completely replacing VPNs or merely supplementing them with other safeguards, organizations must implement alternative security methods better suited to protecting collective remote work activity. Which strategies a particular organization can adopt will inevitably vary depending on factors such as posture and risk appetite. In the meantime, most security experts agree that ZTNA (Zero Trust Network Access) is likely to be the first choice among businesses in the foreseeable future.

timus

timusnetworks.com

About Timus

Timus Networks simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Our premier product, Timus SASE, transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE is purpose-built for the MSP/MSSP Channel. It offers simplicity and rapid deployment, with installation in under 30 minutes.