FORTINET

How to Securely Access Applications from Anywhere

A Guide to Zero-Trust Network Access

Work-from-Anywhere Is Here to Stay

Undoubtedly, the global pandemic was a massive challenge that accelerated digital transformation for enterprises. Many industries had to change how they worked quickly to ensure productivity and viability.

Enabling a remote workforce was a smart move for businesses not requiring hard labor.

This trend represents a paradigm shift in hiring. Recruitment Research reveals that 76% of companies surveyed said that hiring is no longer company-office dependent. And the Microsoft Digital Defense Report relays that enterprise organizations started moving to a hybrid workplace in 2021, with 31% already fully adopted.

In the FBI's 2021 Internet Crime Report, cybercriminals who used social engineering tactics to break into remote offices stole over $6.9 billion.

Today, most organizations have continued their work-from--anywhere (WFA) policies with remote workers using cloud apps to access the network from just about anywhere they can get online. As a result, cyberattack surfaces have expanded, and attackers have taken notice with new tactics.

For instance, it is easier for bad actors (hackers) to intercept the data of remote users and steal their credentials using sophisticated techniques. Once inside the network, these attackers can employ malware and hold critical data for ransom. It's a lose-lose situation.

Nevertheless, all types and sizes of businesses and organizations have adopted a WFA strategy due to its many benefits. For example, Dow Chemical, British Telecom, and Best Buy discovered that remote workers are 35–40% more productive than their office counterparts.

Today, the digital WFA model is here to stay but not without some major secure-access considerations. We'll be covering those in this guide as well as how to enable remote work securely in a WFA environment.

Threats Inherent with a Remote Workforce

The weakest links: passwords and vulnerable networks

For simplicity's sake, most people rely on weak passwords and the built-in security of their company's network, which may not be up to date. Remote employees or contractors may use public Wi-Fi to access company resources. Threat actors can easily hack Wi-Fi over vulnerable networks using sniffing tactics such as man-in-the-middle (MITM) attacks. As a result, working from anywhere makes company networks more susceptible to malicious attacks.

BYOD increases threats

The shift to remote work during the pandemic created new attack surfaces for cybercriminals to exploit. For example, many companies support bring-your-own-device (BYOD) policies in which the workforce can use personal devices, such as smartphones, laptops, and tablets for work-related tasks. However, when BYODs connect to the corporate network, they can deliver malware or malicious scripts that open the door to attackers.

Everyone is vulnerable to social engineering tactics

Regardless of whether they are using corporate devices or BYOD, all users are susceptible to social engineering attacks that exploit emotions to manipulate the target into some form of interaction. During the attack, the victim is fooled or coerced into giving away sensitive data, login credentials, or other information that compromises security. The most common social engineering tactics include phishing, baiting, scareware, and pretexting.

VPNs Were Not Designed for Work from Anywhere

For more than 20 years, virtual private network (VPN) technology has been the primary choice for companies to provide remote employees with secure access to corporate files and systems. Virtual private networks were designed to secure a connection between two entities: the remote user and the client, with most data transfer encrypted for protection. They were not designed to secure access to apps for today's WFA users.

This is because WFA requires organizations to provide secure connections to the applications employees need, whether they are in the office, at home, or on the road. Virtual private networks often provide more access than a user needs to an organization's network. This expands the attack surface, making it easier for an attacker with stolen credentials to access critical resources.

In contrast, zero-trust network access (ZTNA), an extension of NIST's zero-trust architecture (ZTA), augments traditional VPN technologies for application access to allow employees and partners to connect and collaborate securely. Zero-trust network access enables secure and granular access that improves security and the user experience—anywhere, anytime.

Zero-trust network access is part of a SASE strategy and supports the rapid expansion of secure remote access. Gartner predicts that most businesses will switch from VPNs to a ZTNA model in 2023. The following sections explain why organizations are replacing VPNs with ZTNA.

VPNs compromise privacy

One major shortcoming of VPNs is that they don't encrypt all data or ensure anonymity. If a VPN is configured to disable split tunneling, all personal and public activity will occur on the corporate network. This creates a vulnerability that enables attackers to exploit VPNs to drop ransomware.

For example, the US Cybersecurity and Infrastructure Security Agency (CISA) Advisory explains how a cybercrime group called the "Daixin Team" employed ransomware to encrypt servers by gaining initial access to victims through VPN servers. This attack compromised victims' services for electronic health records, diagnostics, imaging, and intranet.

VPNs open an all-access pass in the network

Unlike ZTNA, legacy VPNs open an all-access pass in the network. All data can be exchanged between two entities, even if the VPN encrypts this connection. Attackers accessing users' VPN credentials can spread threats across the organization. Plus, applications exposed to the internet are visible to bad actors and could be breached.

VPNs have poor scalability that degrades the user experience

When too many remote workers access corporate resources on the VPN, it causes congestion, which reduces performance. Plus, VPNs are usually deployed at a central location, which adds latency issues for people working from home or in different parts of the world.

In general, users don't like disrupting their workflows to log in to a VPN. Plus, accessing two-tier apps (billing or CRMS) requires a client on the end-user device with application protocols that require significant bandwidth. These apps quickly overload VPNs, degrading app performance and subsequently the user experience.

These types of productivity issues are why users don't like using VPNs.

VPNs are not designed for BYOD

Virtual private networks have poor support for mobile devices. So, whenever a mobile's screen goes dark, the VPN connection breaks, and the employee needs to reconnect. As well, VPNs don't ensure ongoing BYOD updates, device compatibility, or compliance, which puts a strain on IT resources and infrastructure to manage.

With BYOD, it is difficult to secure the endpoint. Virtual private networks do not provide flexible security policies for BYOD devices. They may require the use of corporate devices at home. Furthermore, third-party vendors that manage employees' HR, payroll, and administrative functions have their own devices and policies external to the VPN.

VPN complexity adds new risks

Virtual private network technology is needlessly complicated. It requires complex policy configuration or an unmanaged endpoint system. Remote employees are given different access methods based on their position (such as employee, administrator, or vendor), but multiple VPNs must be set up for each role.

VPNs lack flexibility and are bound to physical hardware and locations

Virtual private networks usually have on-premises components with hardware limitations that restrict them. As a result, they lack flexibility, which limits the number of concurrent users. With remote workers adding onto the load, they experience bottlenecks and lose productivity.

ZTNA: The Smart Choice for Secure Remote Connection

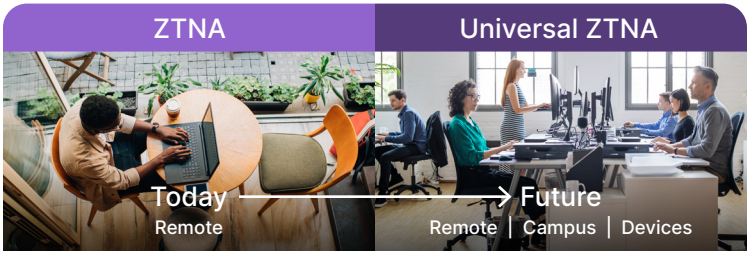
Zero-trust basics: “never trust, always verify”

Zero trust assumes no implicit trust is granted to user accounts or assets based solely on their network or physical locations.

Zero-trust network access implements a zero-trust security model that maintains rigid access controls and distrusts anyone by default, even if they are already inside a network perimeter. It functions as a security framework that grants secure remote access to services and applications on defined, explicit access control policies.

While existing ZTNA policies are for remote work, there is a need for Universal ZTNA, which means that ZTNA should be applied everywhere, regardless of the network or user’s location, including inside the company network.

ZTNA: Moving to Universal ZTNA



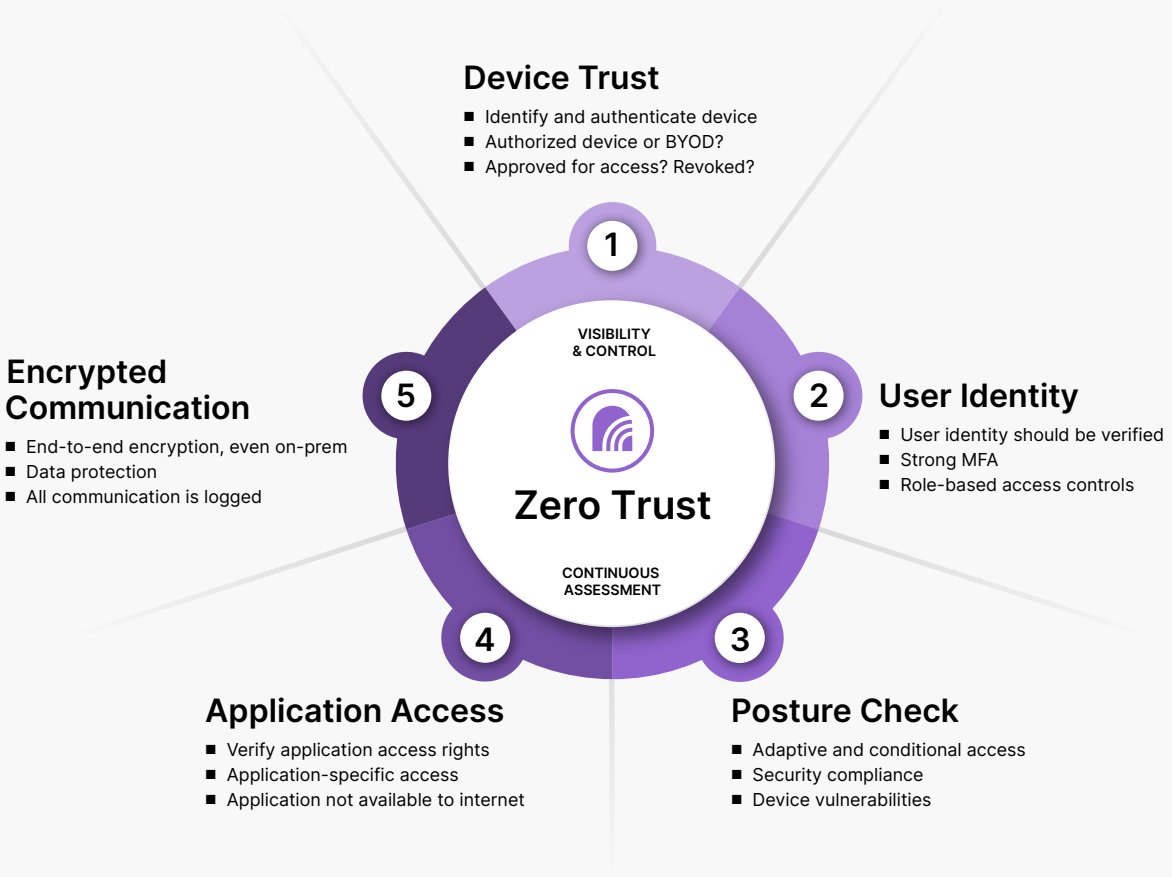
Why ZTNA?

Data confidentiality, integrity, and availability are challenging due to evolving cyberthreats. Legacy VPN solutions cannot guarantee the security and privacy of corporate digital assets and remote employees. Scalability limits also cause latency issues for users. Therefore, enterprises need an appropriate solution, like ZTNA, to offer secure remote access.

> Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.
>
> – National Institute of Standards and Technology

Reducing the Attack Surface

Granular application control



The Many Benefits of Switching to ZTNA

More controlled access

Zero-trust network access provides specific app access using concepts of least privilege, which reduces risk and the ability for threats to move laterally.

Enhances security with transparency

Zero-trust network access eliminates lateral movement, integrates device posture checks into its policy, and is transparent to end-users. This boosts productivity and is a better user experience than the latency and login issues they face with VPNs.

Malware protection

A ZTNA solution should be capable of automatically stopping the download and upload of malicious threats without requiring software to be downloaded on end-user systems. Unlike VPN, ZTNA operates inline, so communication between the end-user and application can be inspected for malicious content.

Consistent user experience

Whether they are using BYOD or company resources from any location, end-users get secure access to apps wherever they are hosted, with a consistent user experience, user-based security, automatic secure tunnels, and continuous verification with Single Sign-On (SSO) support.

Better visibility with easy management from anywhere

Zero-trust network access provides detailed insights into app usage and user management. Apps are moving from on-premises servers to private and public clouds. With a ZTNA access proxy in place, IT has complete control over where these connect.

Reduces operational costs

Fortinet delivers Universal ZTNA as part of FortiGate Next-Generation Firewalls (NGFWs), covering users when they are remote or in the office. A FortiGate NGFW and the FortiClient ZTNA endpoint agent are all that's needed to enable more secure access and a better experience for remote users, whether on or off the network.

Decreases administrator workloads

Fortinet Universal ZTNA capabilities are automatically enabled on any device or service running FortiOS 7.0 and higher. This includes hardware appliances, cloud virtual machines, and the FortiSASE service. Zero-trust network access technology consolidates the required remote tools, and their configuration complexity is also very low, resulting in a decreased administrator workload.

Low-cost, flexible migration

Universal ZTNA does not require the traditional rip-and-replace of hardware and software. Moreover, ZTNA can work in parallel with existing technology during migration. With a ZTNA access proxy in place, IT has complete control over where these connect. Apps can move to the cloud, between clouds, and back to campus without impacting the user experience. This enables organizations to easily migrate their applications off of VPN and onto ZTNA.

While ZTNA was responsible for under 10% of remote access deployments in 2021, Gartner estimates that the percentage will rise to at least 70% by 2025.

What Makes a Quality ZTNA Solution?

The following are the essential features of ZTNA to consider in context of your enterprise and users.

Identity and access management

Alongside modern multi-factor authentication (MFA) and SSO, unified access policies across servers and applications bring identity and access management (IAM) into a centralized, secure, and manageable place for security professionals both on-premises and in cloud environments. Identity access management helps companies consolidate identities. A reliable ZTNA solution must encompass identity-based authentication to significantly reduce the enterprise's attack surface.

Agentless deployment options for BYOD

Zero-trust network access can provide secure access to contractors and third parties who are authorized to use corporate resources, including BYOD. Versus corporate oversight of third-party BYOD, agentless deployment ensures third parties have secure access to only the apps and services they need, as well as privacy on their personal devices.

Performance

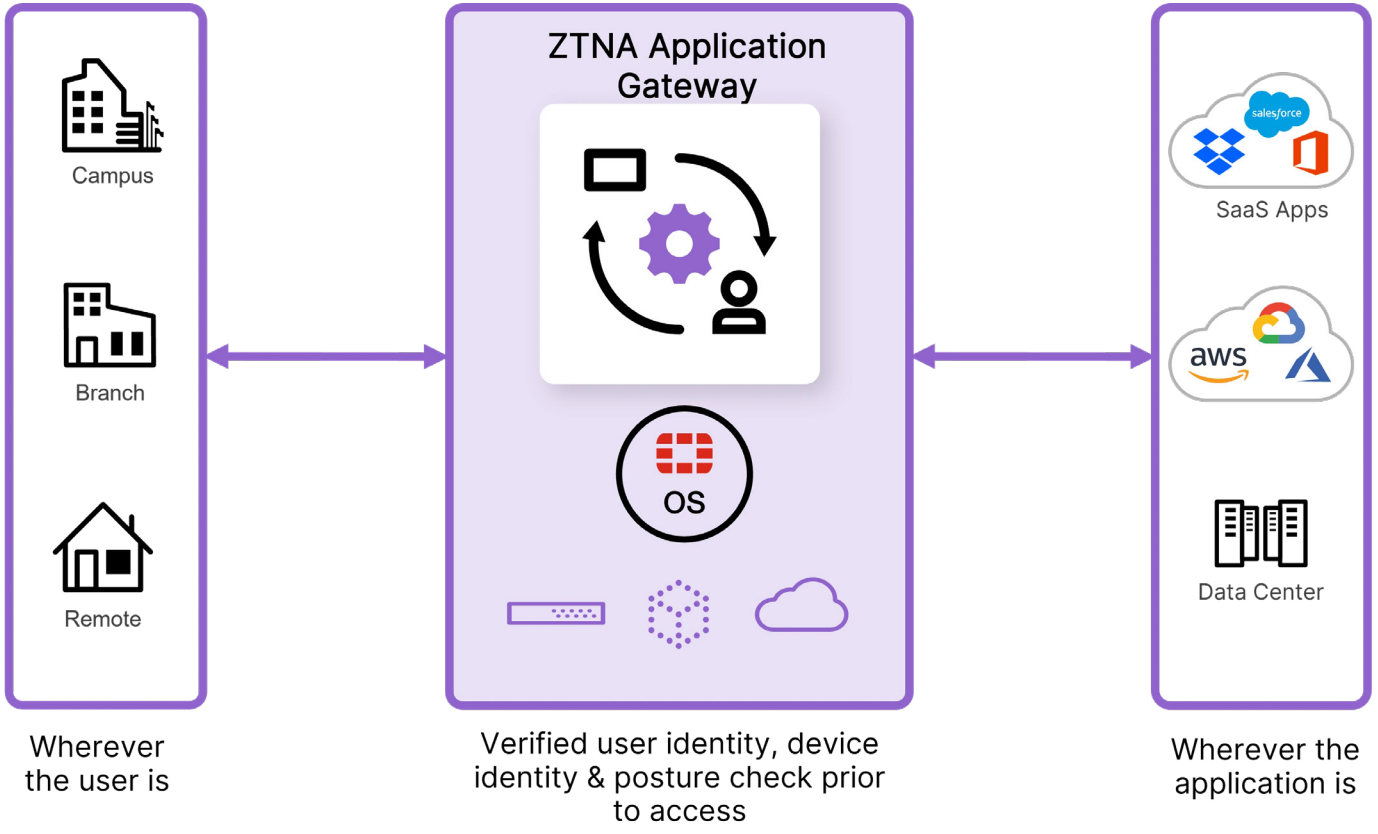
During the pandemic, remote work put a massive burden on VPNs because all traffic has to be routed back through the VPN concentrator and then back to the user. Zero-trust network access provides a much more direct connection between user and app. This is why ZTNA is a better solution to prevent overloads while ensuring a more secure and consistent user experience from anywhere.

Robust data loss prevention

Zero-trust network access must enforce data loss prevention (DLP) policies for downloading and uploading on-premises resources. It should support advanced DLP scenarios such as regex or exact data match. Instead of raising an alarm, the DLP security control should be capable of providing real-time support to prevent data loss.

Granular visibility and reporting

Zero-trust network access solutions must display detailed information and real-time visibility and control to demonstrate compliance and enable security audits. Reporting must include comprehensive logs of files, users, and application activities for managed and unmanaged devices. This is why integration with a security information and event management (SIEM) platform is important.


Campus
Branch
Remote
Wherever the user is
ZTNA Application Gateway
OS
Verified user identity, device identity & posture check prior to access
SaaS Apps
Data Center
Wherever the application is

ZTNA Critical Capabilities: 6 Questions to Ask Your Vendor

The following are some questions to ask vendors when considering ZTNA solutions for your organization.

1. **How do I set up granular access controls for each end-user?**
   - Companies need to understand their users before implementing ZTNA. For example, how should they log in, and what can they do with their access?

2. **How can ZTNA help set up granular access to shrink the attack surface?**
   - Zero-trust network access uses least privilege, which is a step above typical segmentation. Companies create granular access policies around a user and their device(s) with restricted application access.

3. **Does the solution use behavior-based techniques to protect against zero-day threats?**
   - Can the ZTNA scan files in real time for malware?
   - Does it have an advanced detection engine? This is important because signature-based detection of known malicious code cannot detect unknown threats.

4. **Does the solution provide easy and seamless access regardless of where the application is located?**
   - Ensure your ZTNA can provide controls for applications both in the cloud and data centers—and ensure a consistent user experience—without having to backhaul traffic.

5. **Can the solution scale with the organization's growth and workplace changes?**
   - Scalability is a necessary component that needs to be present in the ZTNA solution. An organization must be capable of supporting an ever-increasing number of users to avoid disruptions due to overloading IT infrastructure.

6. **Does ZTNA continuously monitor and dynamically adjust connections when the threat risk of the device or user changes?**
   - This is very important to halt any significant data breach from occurring. Connections must be monitored proactively to stop malicious activity.

Fortinet: Reliable and Secure Connectivity Everywhere

Fortinet Universal ZTNA is a robust and reliable means to implement a ZTNA solution with rapid deployment and low total cost of ownership (TCO) with on-premises, cloud-based, and hybrid options.

To simplify deployment, many organizations already have the products in Fortinet's fully integrated Security Fabric that comprise the Fortinet ZTNA solution. This enables a full platform play with a comprehensive product portfolio: the ability to support hardware, software, virtual machines, containers, and cloud-based deployment options.

In addition, Fortinet's automated Security Fabric supports a wide range of security capabilities, including ZTNA, SWG, FWaaS, CASB, SD-WAN, DNS, and EDR.

Fortinet Universal ZTNA ensures secure access to all applications for all users with consistent policies for a positive user experience. Fortinet delivers Universal ZTNA as a part of the FortiGate NGFW or through a lightweight ZTNA Application Gateway.

Universal ZTNA includes the following capabilities of the Fortinet Security Fabric:

Fortinet IAM helps IT teams securely manage identity authentication and authorization access policies for all company resources. It enables adoption of least privilege to mitigate risks associated with account-based security threats.

FortiTrust is a subscription-based service that provides every element needed to implement ZTNA to the FortiGate-based network. It is a secure means of delivering application access control.

FortiSASE secures remote users and their devices, regardless of their location, with unified firewall, networking, and security policies while allowing for centralized management and visibility through a single pane of glass.

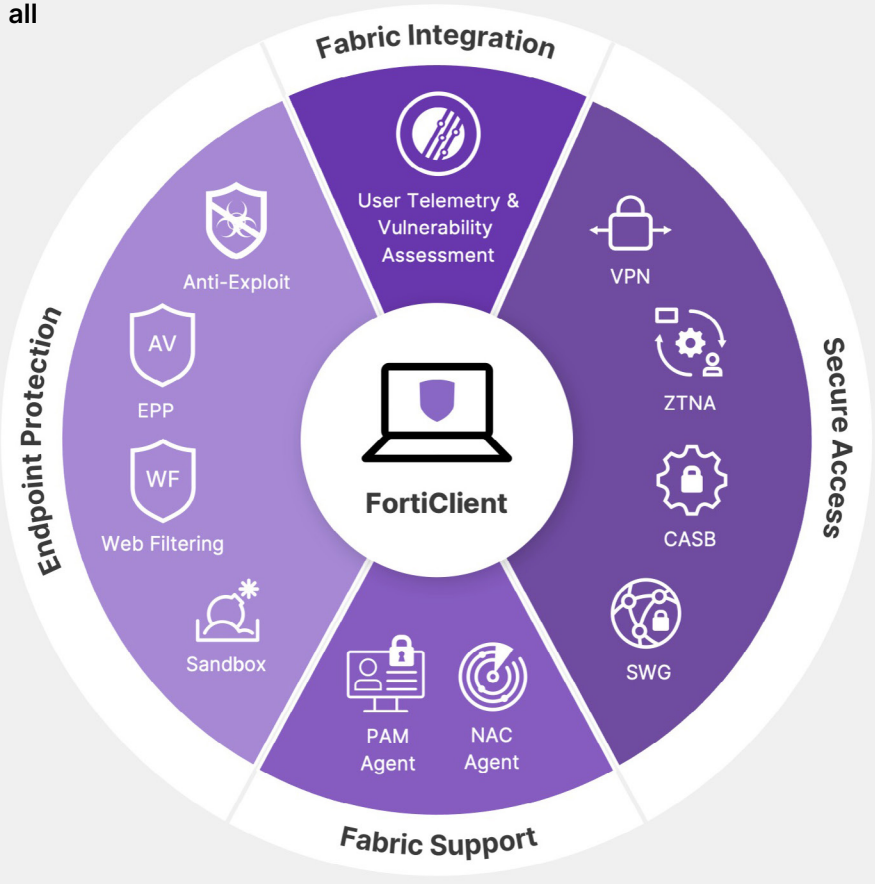
FortClient is a unified agent for endpoint remote access and control. A single client enables a wide range of functionality.

FortiToken is a tool to implement MFA controls tied to your ZTNA deployment.

FortiAuthenticator is for SSO and access management.

FortiClient Unified Agent

One agent to rule them all



If you are looking to deploy a ZTNA solution, contact a Fortinet ZTNA expert to help you get the best protection for your organization's secure access challenges.

www.fortinet.com

July 24, 2023 8:11 AM

2275118-0-0-EN