

SOLUTION BRIEF

Securely Access Any Application from Anywhere with Comprehensive Zero Trust via Fortinet Universal ZTNA

Executive Summary

Today's hybrid workforce and work-from-anywhere (WFA) users are challenging organizations to provide them with adequate security and seamless connectivity. Additionally, networks are now highly distributed with resources spread across data centers and multiple clouds. Therefore, it's critical for IT teams to enable secure access from anywhere to any application while applying consistent security policies. That's why enterprises must evolve remote access from legacy virtual private networks (VPNs) to zero-trust network access (ZTNA) solutions.

Fortinet goes above and beyond the industry's standard ZTNA in offering Universal ZTNA. It provides application access control for all locations where a user might be working. Much more than just a remote work solution, Fortinet Universal ZTNA conducts user and device checks for every application session for users in the office, in the home, and on the road. The Fortinet solution includes a set of products that integrate into the Fortinet Security Fabric, enabling easy management and end-to-end visibility.

Fortinet Universal ZTNA Advantages

ZTNA rose to prominence during the pandemic when many organizations shifted from VPN to a ZTNA solution. Most ZTNA solutions are cloud-based and focus on the remote worker use case. However, when employees returned to the office for at least a few days a week, IT leaders found they required two application access policies—one for remote users and one for on-premises users.

Having two access policies opens the door for errors and misconfigurations, as well as doubles the IT team's workload. A zero-trust solution is the answer to these challenges. ZTNA can be used for all locations. IT leaders can extend the zero-trust principles onto their campuses, not just for remote workers. Using ZTNA in all locations is called Universal ZTNA.

Fortinet has integrated our ZTNA application gateway into several different products, including FortiGate Next-Generation Firewalls (NGFWs). It enables ZTNA enforcement points to be located in many places across an organization's hybrid networking infrastructure.

Fortinet can apply ZTNA to remote users, home offices, and campus and branch offices by offering controlled remote access to applications. It's easier and faster to initiate than a traditional VPN. This gives users a better experience while providing a more granular set of security protections. It doesn't matter if applications are in the data center, private cloud, or public cloud. Users and applications can be geographically independent and still have secure and reliable connections.



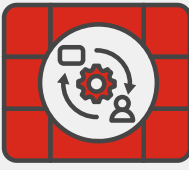
Over 60% of organizations will embrace zero trust as a starting place for security by 2025.¹



Fortinet Universal ZTNA Components

The Fortinet Universal ZTNA solution is made up of:

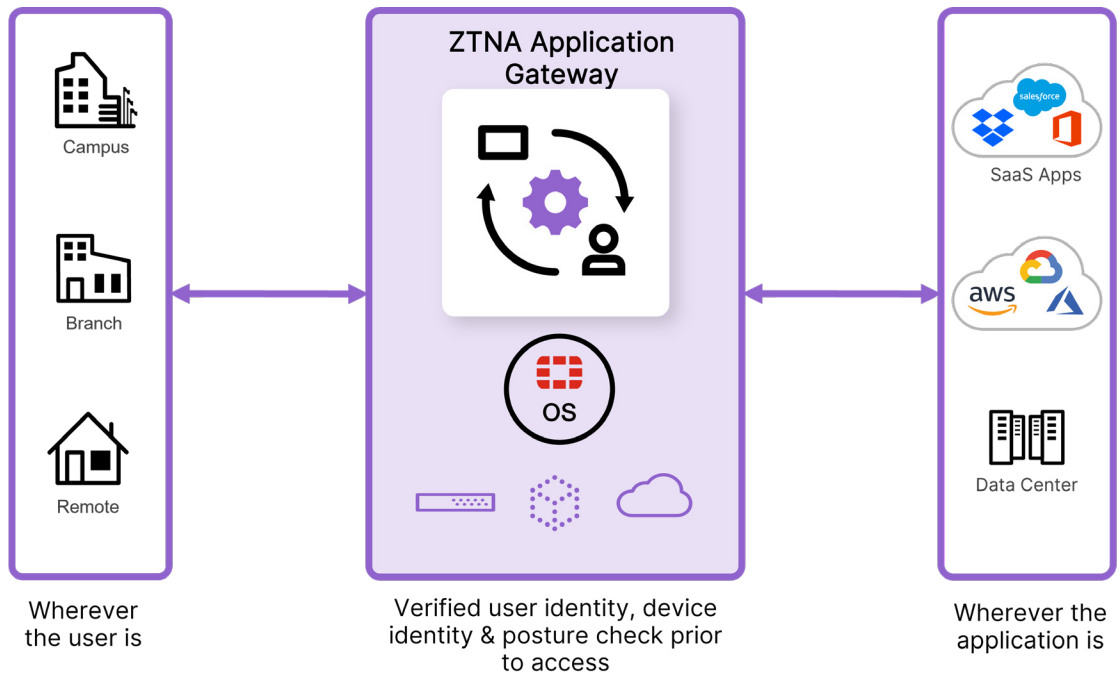
- **ZTNA application gateway:** These ZTNA enforcement points provide the encrypted tunnel termination and enforce the application access policies for every requested session, looking at the contextual information about the user and device in use to determine if access should be granted. ZTNA application gateways exist in several products, including FortiGates, FortiSASE, FortiWeb, FortiADC, FortiProxy, and FortiPAM.
- **FortiClient agent:** FortiClient acts as a ZTNA agent and is installed on the endpoint device. It creates automatic, encrypted ZTNA tunnels to the application gateway and performs the device posture assessment, as well as the single sign-on (SSO). FortiClient is a unified agent that also includes the VPN agent, which simplifies the transition from VPN to ZTNA.
- **FortiClient Enterprise Management Server (EMS).** EMS plays a critical role in configuring the ZTNA agents to orchestrate the ZTNA solution. FortiClient EMS is included with all licensed versions of FortiClient.



Existing FortiGate and FortiClient customers can use ZTNA as soon as they update to FortiOS 7.0 or later. There are no additional licensing fees.

Optional elements of Fortinet Universal ZTNA:

- **Fortinet identity and access management (IAM):** This solution provides the services necessary to securely confirm the identities of users and devices as they enter the network. It includes:
 - FortiAuthenticator to provide centralized authentication services, including single sign-on (SSO)
 - FortiToken to confirm the identity of users by adding a second factor (two-factor authentication)



Our unique approach, delivering Universal ZTNA as part of our operating system, makes it uniquely scalable and flexible for both cloud-delivered or on-prem deployments, covering users whether they are in the office or remote.



How It Works

The Fortinet solution enables ZTNA capabilities by leveraging the ZTNA application gateway in FortiOS and by using FortiClient as the ZTNA agent. To protect traffic over the internet, the FortiClient ZTNA agent on the device creates an encrypted, secure tunnel from the device to the ZTNA application gateway.

This tunnel is created on-demand and transparent to the user, which solves a major pain point of VPN remote access. Now, users don't need to remember to start their VPN. Additionally, the internal connections will also be protected as the same tunnel is created whether the user is on or off the network.

This architecture has benefits on the application side as well. Because the user is connecting to the ZTNA application gateway, which then connects to the application, the application can exist on-premises, in a private cloud, or in a public cloud—all while hidden from the internet. The application only needs to accept connections from the ZTNA application gateway, keeping it hidden from prying hackers or bots.

Secure Remote Access for Today's Distributed Networks and Users

Fortinet makes it easy to transition from traditional VPN to ZTNA. With the technology built into the FortiOS operating system, Fortinet simplifies consistent and secure application access, regardless of where the user or application is located. It's a better experience for the end-user and easier to manage for the network admin. Moreover, the attack surface is reduced via ongoing verifications and hidden applications. The Fortinet ZTNA solution delivers more secure remote access than a traditional VPN, while enabling a better user experience.

¹ Gartner, [Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality](#), December 6, 2022.

