Britannic FORTINET

How to Securely Access Applications from Anywhere

A Buyer's Guide to Zero-Trust Network Access

Challenges

With the rise of the hybrid workforce, organizations need to secure employees who access the corporate network and applications from both on-site and off-site locations.

In addition, applications are located not only on-premises but are increasingly accessed in the cloud along with SaaS applications.

This shift to hybrid work and cloud has significantly increased the attack surface, created security gaps with inconsistent security models, and increased network and application protection complexity.

Using virtual private networks (VPNs) to secure hybrid workforce access to enterprise applications is no longer sufficient.

VPNs are designed to provide network-level access. This is often broader than what is necessary for users to access specific corporate applications and increases the risk of lateral threat movement to the corporate network through a compromised endpoint device. In addition, VPNs are usually aggregated at a central location, adding latency issues for people working from home or other remote locations.

Users are increasingly accessing SaaS and other distributed applications in the cloud, and there has been a significant rise in shadow IT, which is the use of unauthorized applications. IT security teams need visibility into all the SaaS applications being used and to control the type of data stored or accessed via these applications.

ZTNA: Evolving Secure Access

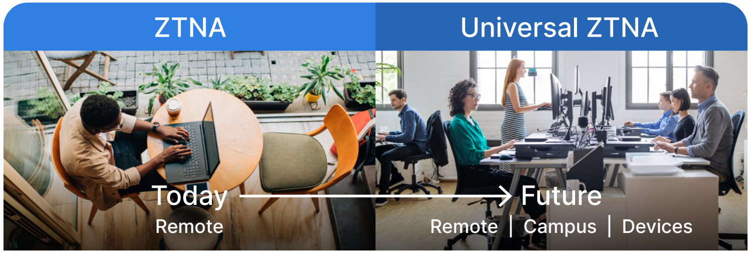
Zero-trust basics: "Never trust, always verify."

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 (ZTNA) 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.

ZTNA policies verify user and device identity, continuously validate posture, and provide explicit access to specific applications on a per-session basis.

Moving from ZTNA to Universal ZTNA



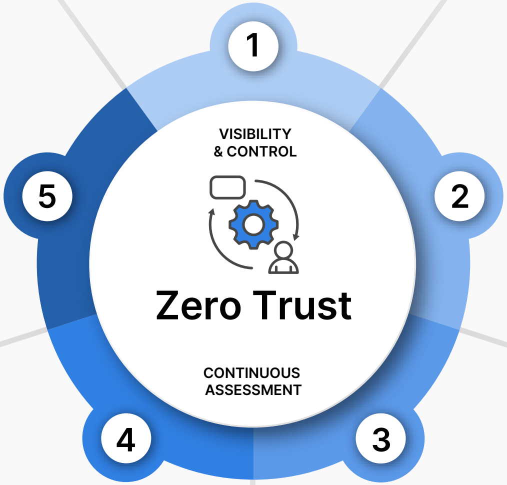
Beyond remote access

While the ZTNA use case was initially for remote work, organizations are looking to apply ZTNA and use consistent security for on-premises users as hybrid work becomes the norm. However, not all ZTNA solutions can effectively deliver Universal ZTNA. Cloud-only solutions steer all traffic to the cloud, introducing latency for on-premises access. Look for ZTNA solutions that support hybrid deployment models with local enforcement options.

> 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



Device Trust

- Identify and authenticate the device
- Authorized device or BYOD?
- Approved for access? Revoked?

User Identity

- User identity should be verified
- Strong MFA
- Role-based access controls

Posture Check

- Adaptive and conditional access
- Security compliance
- Device vulnerabilities

Application Access

- Verify application access rights
- Application-specific access
- Application not available on internet

Encrypted Communication

- End-to-end encryption, even on-prem
- Data protection
- All communication is logged

The Many Benefits of Switching to ZTNA

Prevent lateral malware movement

ZTNA provides specific app access using concepts of least privilege, which reduces risk and allows threats to move laterally.

Enhance security posture with transparent access

ZTNA integrates device posture checks into its policy and is transparent to end-users. This improves overall security posture and provides a better user experience with reduced latency and login issues that users face with VPNs.

Malware protection

ZTNA solution should be capable of reducing lateral malware and ransomware propagation and provide full inline traffic inspection to block the download and upload of malware. Unlike VPN, ZTNA operates inline, so communication between the end-user and application can be inspected for malicious content.

Consistent security and user experience

Whether users are accessing from a corporate device or a BYOD from any location, they should get secure access to applications wherever they are hosted, with a consistent user experience and single sign-on (SSO) support.

Better visibility and control

ZTNA provides detailed insights into application and user access. Applications are moving from on-premises servers to private and public clouds. With a ZTNA application gateway (access proxy) in place, IT teams should get complete control and visibility over where these connect.

Reduced operational complexity and TCO

ZTNA solutions enforce policies via application access proxy. If your existing NGFW ADC, WAF, or proxy can enforce ZTNA as an in-built feature, it eliminates the need to deploy and manage a separate component. In addition, if your current VPN agent integrates ZTNA and endpoint security, it can further reduce TCO with deploying and managing multiple agents.

Low-cost, flexible migration

ZTNA does not require the traditional rip-and-replace of hardware and software. ZTNA can work in parallel with existing VPN technology during migration. With a ZTNA application gateway, IT staff have complete control over where these connect and can prioritize ZTNA roll-out with key business applications. Moreover, applications can move to the cloud, between clouds, and back to campus without impacting the user experience.

According to the Gartner® 2024 Zero-Trust Adoption survey, 63% of organizations worldwide have fully or partially implemented a zero-trust strategy.[1]

What Makes a Quality ZTNA Solution?

The following are the essential features of ZTNA to consider in the 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 on-premises and in cloud environments. IAM helps companies consolidate identities. A reliable ZTNA solution must encompass identity-based authentication to reduce the enterprise's attack surface significantly.

Agentless deployment options for BYOD

ZTNA can provide secure access to contractors and third parties authorized to use corporate resources, including BYOD. Unlike 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. ZTNA provides a much more direct connection between the user and the app. This is why ZTNA is a better solution for preventing overloads while ensuring a more secure and consistent user experience from anywhere.

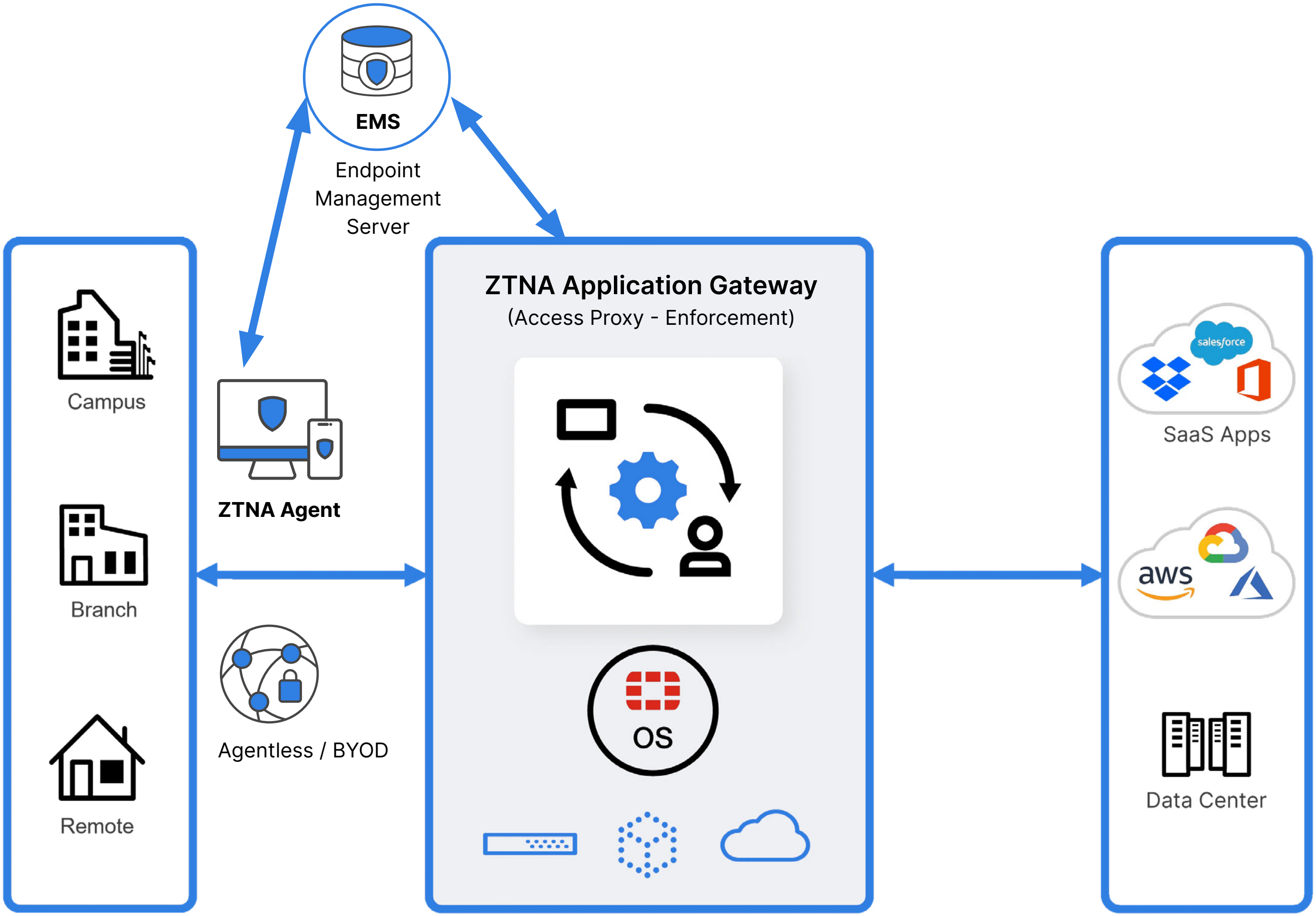
Robust data loss prevention

ZTNA 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

ZTNA 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 platform is important.



Any Location

Verified user identity, device identity, and posture check prior to access

Any Application

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?**
    - ZTNA uses least privilege, which is a step above typical segmentation. Companies create granular access policies around users and their devices with restricted application access.

3. **Does the solution use behavior-based techniques to protect against zero-day threats?**
    - Can the ZTNA scan files for malware in real time?
    - 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 users or applications are located?**
    - Not all ZTNA solutions support Universal ZTNA. Ensure your ZTNA can provide low latency access for users both on-premises or remote and to applications both in the cloud and data centers without having to backhaul all traffic to cloud.

5. **Does your ZTNA solution offer a unified VPN/ZTNA agent? What endpoint protection capabilities are included?**
    - It is important to avoid having to deploy multiple agents from different vendors for VPN, ZTNA, basic hygiene, and EPP. Having a unified agent improves security, reduces operational complexity and provides a seamless transition from VPN to ZTNA.

6. **Does ZTNA continuously monitor and dynamically adjust connections when the threat risk of the device or user changes?**
    - How often are the ZTNA continuous posture assessment done (60 seconds vs. 5-15 min.)? This is very important to halt any significant data breach from occurring. Also, existing sessions must be blocked 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 TCO with on-premises, cloud-based, and hybrid options.

To simplify deployment, many organizations already have the products in the fully integrated Fortinet Security Fabric that comprises the Fortinet ZTNA solution. This enables a full platform 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 via a lightweight ZTNA application gateway.

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

The ZTNA application gateway enforces ZTNA policies. It is a feature of FortiOS and available as part of FortiGate, FortiADC, FortiWeb, and FortiProxy, as well as as a standalone ZTNA application gateway VM.

Fortinet IAM helps IT teams securely manage all company resources' identity authentication and authorization access policies. It enables the 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 location, with unified firewall, networking, and security policies while allowing for centralized management and visibility through a single pane of glass.

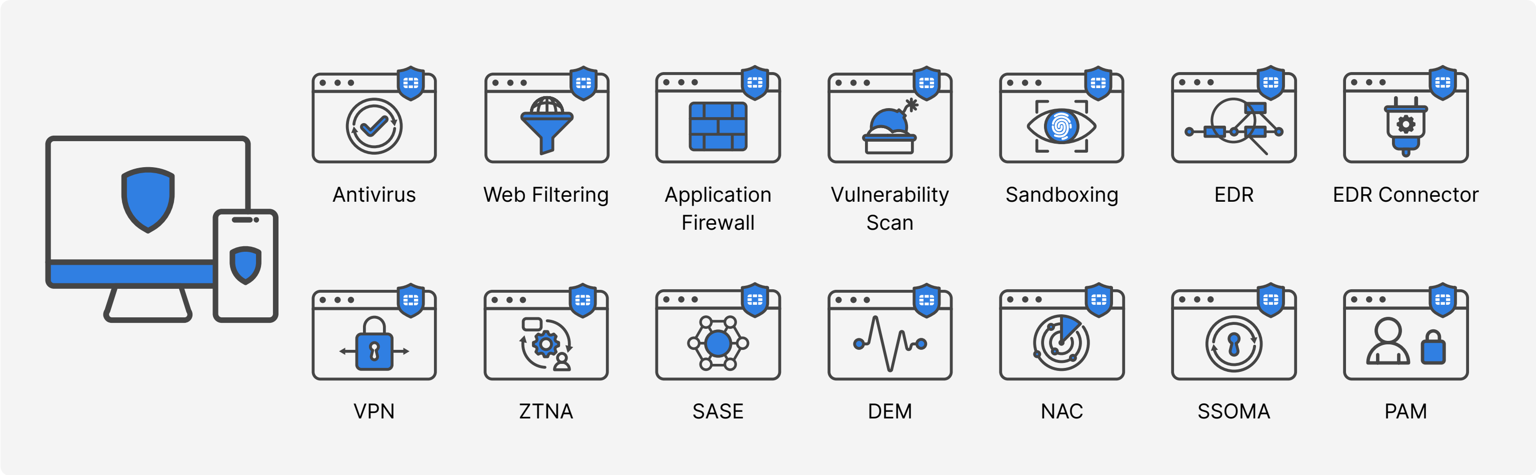
FortiClient is a unified agent for endpoint remote access and control. A single client enables a wide range of functionality.

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

FortiAuthenticator is for SSO and access management.

FortiClient Unified Agent

Unified agent reduces security gaps, costs, and operational complexity



Antivirus

Web Filtering

Application Firewall

Vulnerability Scan

Sandboxing

EDR

EDR Connector

VPN

ZTNA

SASE

DEM

NAC

SSOMA

PAM

[1] Gartner, 2024 Zero-Trust Adoption survey.

November 7, 2024 10:14 AM

MKTG-291-0-0-EN