ZTEdge™
By Ericom Software

Zero Trust Network Access

The Zero Trust Network Access (ZTNA) Solution That has Identity Management and MFA Built-In

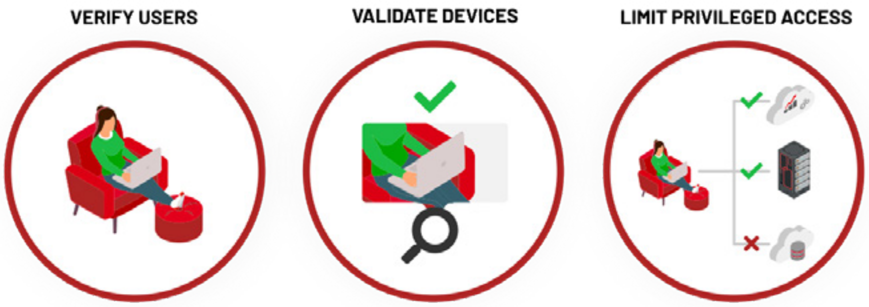
Eliminate the costs, complexity and vulnerabilities associated with legacy VPNs

Enabling remote users to securely access applications, workloads and data on office networks and remote desktops is a complex challenge. That's why, when faced with the sudden pandemic-driven need to keep entire workforces connected, familiar VPNs and RDP were a reasonable short-tem solution for enabling organizations to stay somewhat productive.

Now, however, with hybrid and remote work here to stay, this approach leaves organization's networks and resources at increased risk of attack: VPNs expose network IP addresses to the internet, often run on outdated software with unpatched vulnerabilities, and are easy for threat actors to find. Using brute force attacks and stolen credentials, cybercriminals can penetrate organizations' networks via VPNs and RDP. And once in, they are free to move laterally through the network, searching for valuable data and critical ransomware targets.

To truly secure remote access, organizations need two types of protection: First, controls to ensure that only authorized, authenticated users can access their network, and second, comprehensive policy-based restrictions on resource access.

ZTNA for Corporate Applications and Desktops



The Solution: Zero Trust Network Access

ZTEdge makes it simple for your distributed workforce – and even third parties – to securely access the apps and resources they are authorized to use, regardless of whether they are located on premises or in the cloud. It is a simple, cost effective and far more secure alternative to VPNs and RDP access.

No network reconfiguration is required, and ZTEdge ZTNA comes with built-in Identity and Access Management (IAM) and MFA to simplify implementing identity-based least privileged access. Alternatively, if you already have an IAM solution in place, ZTEdge ZTNA can be easily configured to work with it.

When a user attempts to access an application, they are first identified and authenticated by the solution's identity manager. If policies dictate, MFA can be used to further verify the user's identity.

Once a user is authenticated, the network is virtually microsegmented to limit user access to only the resources they are authorized to use, based on their individual policy information. 1:1 secure temporary connections enable users to access the resources they need. All other resources are cloaked so users do not even know they are there, eliminating lateral movement and risk of ransomware infection and spread.

Granular access policies are essential for enforcing least privilege access, a pillar of Zero Trust Security. But manually creating granular access policies from the ground up is an onerous and time-consuming task – and one that must be frequently repeated as user responsibilities change and employees and third parties join or leave. To facilitate true least privilege access, the solution replaces manual policy configuration with an Automatic Policy Generator that sets and updates policies based on each authorized user's behavioral patterns, without burdening IT staff.

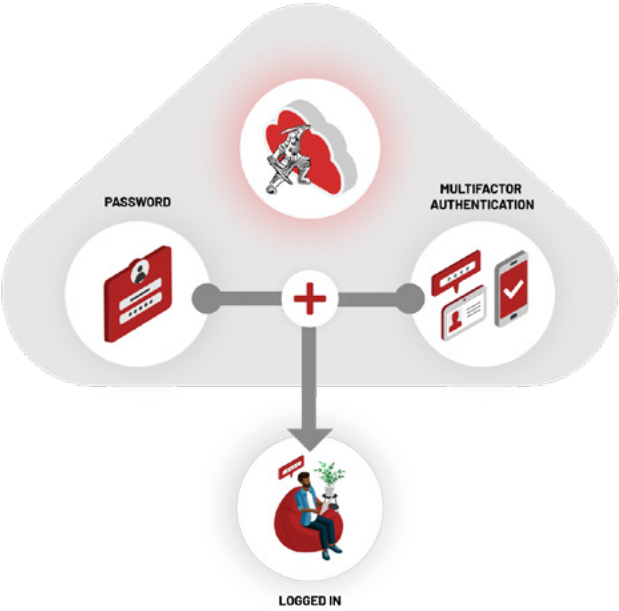
ZTEdge™
By Ericom Software

Zero Trust Network Access

Zero Trust Network Access Highlights

- Transition your organization from costly, complex and vulnerable VPNs
- Boost productivity and accelerate digital transformation initiatives with integrated access to on-premise and web-based apps
- Simplify secure access for remote users
- Eliminate lateral movement and ransomware risk with 1:1 microsegmentation
- Free IT resources from onerous policy building with patent-pending Automatic Policy Builder that enables efficient, hassle-free creation and maintenance of granular policies for each user
- Leverage built-in identity solution (IAM with MFA) or easily integrate with your existing solution
- Get continuous fine-grained visibility into user behavior and network traffic with easy-to-use dashboards

Identify, Authenticate and Authorize with Built-In MFA



Additional ZTEdge Security Solutions for Organizations Adopting A Zero Trust Security Strategy

ZTEdge Web Isolation

Strong remote browser isolation-based web security that protects your users and data from ransomware and phishing, and works with existing SWGs

ZTEdge Web Security

Intelligent remote browser isolation-based web security that protects your users and data from ransomware and phishing, with integrated SWG

ZTEdge Desktop

A Zero Trust solution that eliminates the remote desktop access vulnerabilities that leave your networks and data exposed

www.zerotrustedge.com
info@zerotrustedge.com

Americas:
T +1 (201)767-2210

UK & Western Europe:
T +44 (0)1905 777970

Worldwide:
T +972-2-591-1700

Follow us