ZTEdge™
By Ericom Software

ZTEdge Desktop

Remote Desktop Access that Won't Expose Your Organization's Networks and Data

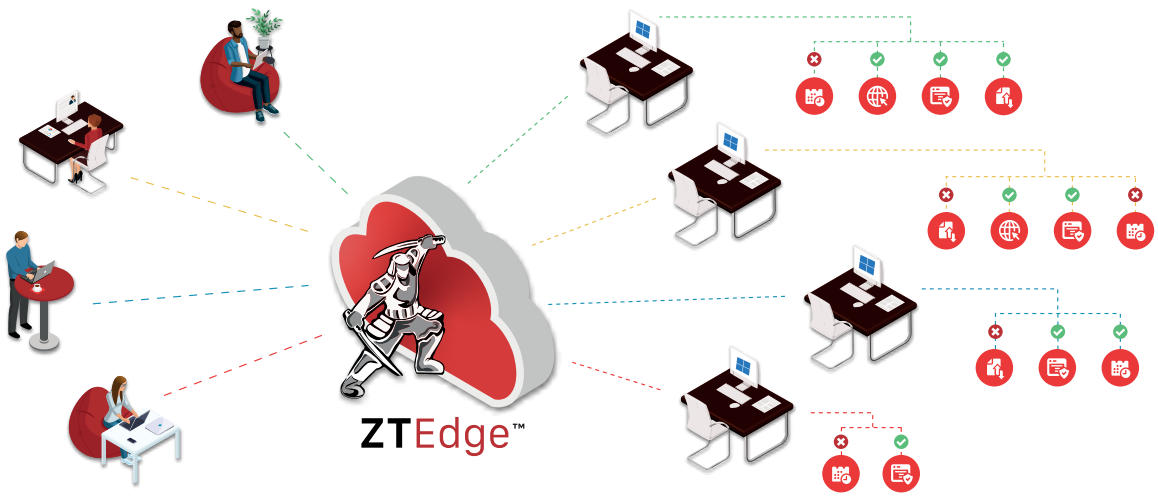
Eliminate the costs, complexity and vulnerabilities associated with RDP/RDS

Enabling remote access to your users' desktops has never been more important – or more fraught with risk. Cybercriminals or malicious insiders who gain access to desktops via malware, brute force attacks or phished credentials can quickly move laterally through extended networks, injecting and spreading ransomware, disrupting operations, and exfiltrating data. Responsible users may also inadvertently expose your organization to risk through actions that may be as simple as clicking a bad link in an email or downloading an infected file from a website to the desktop.

Most remote desktop access solutions provide just that: Access to desktops. Once a user – or someone who's gotten hold of the user's credentials – is logged in, they are free to act just as if they were physically present at their desk. With this type of access, the desktop can be used as a jumping-off point to launch a wide variety of attacks.

While some remote access solutions may block user logins from unknown IP addresses or known-problematic geographies, clever hackers can navigate around these types of baseline controls. You need a more comprehensive, security-aware remote desktop access solution – one that enforces "never trust, always verify" and least privilege access principles that are the basis of Zero Trust security.

Network app access via desktop



The Solution: ZTEdge Desktop

ZTEdge Desktop empowers your organization to take a Zero Trust security approach to remote desktop access. Remote users attempting to access in-office desktops are first authenticated via built-in Identity & Access Management capabilities or your existing identity solution.

Once authenticated, each user is granted access to only their in-office desktop and the other network-connected applications that they are explicitly authorized to use. Cloud-based microsegmentation controls, powered by firewall and Zero Trust Network Access (ZTNA) capabilities, ensure that Zero Trust access is enforced.

Intrusion Prevention System and Network Monitoring capabilities are built into ZTEdge Zero Trust Desktop Access to help your organization keep its networks safe.

ZTEdge Desktop is simple to deploy and simple to use, with no on-premise equipment or software that would take time and money to patch and maintain.

ZTEdge Desktop Highlights

- Transition from vulnerable VPNs and RDP/RDS
- Simpe, secure remote access to in-office desktops
- Eliminate lateral movement and ransomware risk by limiting user access to only the apps they are permitted to use
- Enforce Zero Trust least privilege access from user desktops
- Apply firewall and intrusion prevention
- Leverage built-in identity solution or easily integrate with your existing identity solution
- Get continuous fine-grained visibility into user behavior and network traffic with easy-to-use dashboards

> *ZTEdge offers a unique value proposition for organizations, delivering a comprehensive set of integrated Zero Trust security capabilities via a simple and affordable always-on cloud platform.*

Kamalika Sandell,
Chief Information Officer
at the New Jersey Institute
of Technology

NJIT

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 ZTNA, Apps and Network

A simple, modern and secure approach to remote access that enables your organization to retire costly, complex and vulnerable VPNs

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