ZTEdge™
By Ericom Software

Remote Host Access

Secure Remote Access to Host Systems, Without Exposing Them to Security Risks

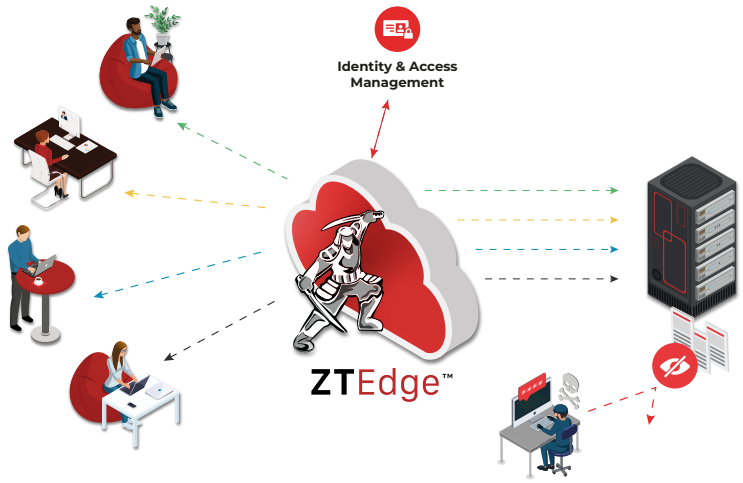
Now more than ever, remote users need secure access to critical apps on legacy host platforms and mainframe systems

For the many organizations that depend on mission critical apps and data housed on legacy hosts and mainframe systems, the move to remote work has been a particular challenge. Faced with the need to rapidly enable large-scale remote access to terminal emulation software, organizations ramped up VPN use as a quick and familiar way to access on-premise terminal emulation apps.

VPNs, however, increase cyberattack risk, as demonstrated by the 2000% bump in VPN-related attacks following the move to hybrid workplaces. VPNs expose network IP addresses to the internet, often have vulnerable unpatched software, and are easy for threat actors to find. Using brute force attacks or stolen credentials, cybercriminals can penetrate host systems, and the networks they are connected to, through VPNs. Mission critical apps and sensitive data are typically housed on mainframe and legacy systems, so they are a prized ransomware and data theft target of cyber criminals. And of course, once they have penetrated into your environment they can freely move throughout the network, searching for other valuable targets.

The result of attacks? Downtime, breaches and data loss, business disruption, compliance violations, fines, damage to the brand and more.

Organizations that depend on host system access need a simple, secure remote access solution that won't expose resources and networks to cyber risk.



The Solution: ZTEdge Remote Host Access

ZTEdge Remote Host Access combines reliable Ericom PowerTerm host system access with the robust Zero Trust access controls provided by the ZTEdge Apps & Network module of the ZTEdge platform. The solution applies a Zero Trust Network Access (ZTNA) approach to enable users to easily access the host systems, apps, and data they need securely from any location, without exposing host systems and networks to cyber threats.

Using built-in identity and access management (IAM) and multi-factor authentication (MFA), remote users connect to the ZTEdge Cloud where their identity, location, and other details are checked and authenticated. Policy-based access is granted to only the host systems and apps that are explicitly authorized. Because of this granular permission-based access approach, IT admins can set "default deny" remote access policies on their host systems, making them invisible to any external user who has not been granted access through the ZTEdge Remote Host Access system. The solution's microsegmentation capabilities also strictly limits authorized users' IT resource visibility, ensuring each individual can only see and access the specific set of resources they are explicitly authorized to use.

Within the ZTNA session, PowerTerm enables simple clientless and client-based access to host systems and apps. To rapidly identify malicious lateral movements attempts, ZTEdge Remote Host Access provides monitoring of all connections to host systems.

ZTEdge Remote Host Access Highlights

- Zero Trust remote access controls protect your host systems, apps, and data from cyber attack
- Zero Trust Network Access (ZTNA) eliminates the security risks of VPN-based access to mainframes and legacy hosts
- Cloud-based service includes IAM, MFA, and microsegmentation
- Provides visibility into host system connections

ZTEdge™
By Ericom Software

Remote Host Access

Web and Application Isolation Highlights

- Ideal for protecting private web or cloud apps that service contract workers and other third parties who use unmanaged devices
- Keeps dangerous content from endpoints from reaching a web app. Any malware from endpoints is isolated in the cloud and destroyed when the session ends
- Protects web-facing surfaces from cybercriminals and bots probing for vulnerabilities in page source code, developer tools or APIs
- Limits data sharing functions of web apps for third-parties to prevent data exfiltration
- Reverse proxy including NGFW/SWG enforces secure Zero Trust access to web apps through user verification, device authentication and least-privilege access, for access that is vastly more secure than VPNs
- Integrated CDR disarms documents that are uploaded by users in isolation before transmitting them to web app or website

> *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 New Jersey Institute of Technology

ZTEdge Capabilities

Access Security	
DNS Security	SaaS App Access Control
Secure Web Gateway	Identity & Access Mgmt.
Cloud Firewall	Secure Remote Desktop Access
Zero Trust Network Access	SD-WAN

Threat Prevention & Compliance		
Threat Intelligence Network	File Sanitization (CDR)	Cloud Data Loss Prevention (DLP)
Remote Browser Isolation	IDS/IPS	Micro segmentation
Anti-Virus	Ransomware Prevention	Network Traffic Analysis
Anti-Phishing	SSL Inspection	Data Anonymization

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