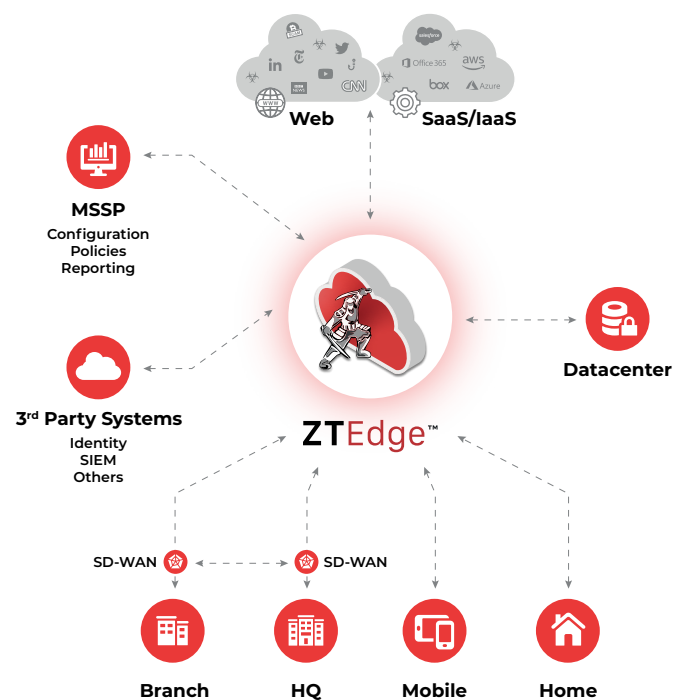


Protect Your Organization with Enterprise-Class Zero Trust Security, Delivered as a Hassle-Free Cloud Service





















The ZTEdge security platform leverages a Zero Trust security approach to protect what matters for your midsize enterprise or small business: your users, your network, your data, your applications and your customers.

Designed with simplicity in mind and operating at the cloud edge, the platform is flexible to evolve as your business grows and transitions to the cloud. Delivered on a distributed, scalable enterprise-class cloud infrastructure, ZTEdge is available as a service provided by certified, market-leading ZTEdge MSSP partners.

- **Simplify secure user access** with passwordless or MFA password-based identity and access management systems that enforce least privilege access.
- **Protect against web-based threats, zero-day exploits, and phishing sites** with secure web gateway and remote browser isolation, fed by real-time threat intelligence.
- **Secure remote access to private apps, desktops and networks** from any location and any device with Zero Trust Network Access (ZTNA).
- **Reduce risk from stolen credentials** by limiting access to public cloud applications like Office365 to authenticated users access apps from dedicated IP addresses.
- **Discover anomalous behavior** and other signs of compromise promptly with continuous network monitoring.
- **Securely connect between company sites, and between remote users and company sites** without costly private MPLS lines. **Secure branch** internet breakouts eliminate frustrating, costly backhaul.



Defend What Matters with ZTEdge

Access Security		Threat Prevention & Compliance		
 DNS Security	 ZT CASB	 Threat Intelligence Network	 File Sanitization (CDR)	 Cloud Data Loss Prevention (DLP) COMING SOON
 Security Web Gateway	 Identity & Access Mgmt.	 Remote Browser Isolation	 IDS/IPS	 Micro-segmentation
 Cloud Firewall	 Remote Desktop/Host Access	 Anti-Virus	 Ransomware Prevention	 Network Traffic Analysis
 ZT Network Access	 SD-WAN	 Anti-Phishing	 SSL Inspection	 Data Anonymization COMING SOON

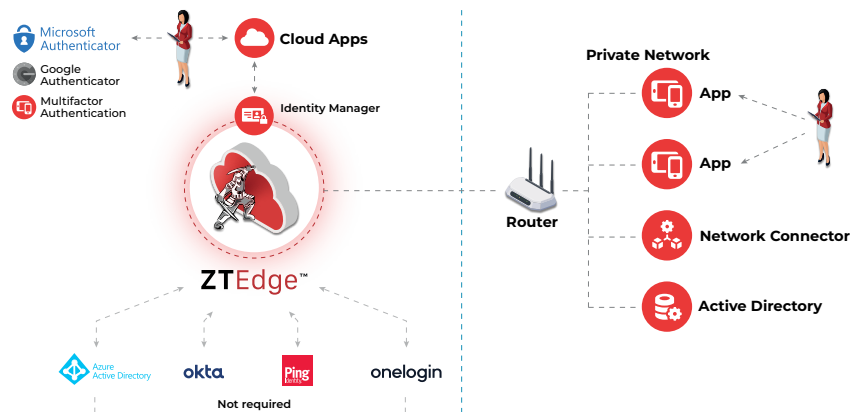
Frictionless Identity and Access Management

ZTEdge Identity and Access Management (IAM) is the authentication database for ZTEdge cloud security services, and can also serve as an organization's primary user identity solution. Using passwordless or password-based multi-factor authentication, ZTEdge IAM enforces least privilege access controls for both cloud and on-premise applications, for a unified user experience. It makes authenticating frustration-free and nearly invisible to users, with single sign-on for all resources.

In addition to controlling access based on user identity, ZTEdge IAM further manages access based on additional factors such as device, user location and time of request.

ZTEdge IAM integrates seamlessly with cloud service authenticators such as Microsoft and Google Authenticators, as well as Active Directory for on-premise resources. For organizations using it as their primary user identity database, ZTEdge can broker authentication requests with existing SAML-supported IAM directories, such as Okta, Ping and others, as well as Azure Active Directory, to enable single sign-on across all resources.

- Passwordless or MFA password-based authentication to ZTEdge cloud, cloud apps, and on prem applications
- Single Sign-on (SSO) for cloud apps and SaaS solutions
- Controls access based on user location, device and time as well as user identity
- Extends authentication and identity to other solutions as needed
- Integrates in a few clicks with any current SAML or authentication solution

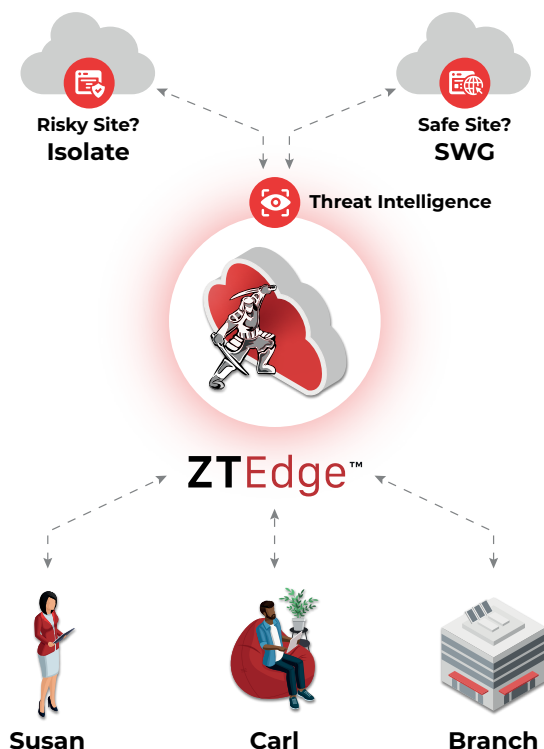


Secure Internet Access

ZTEdge Secure Internet Access integrates leading threat prevention technologies to ensure that users can securely browse the web, click email links, and download files without risk of downloading ransomware or other malware, including malicious droppers and installers that enable further infection of endpoints and networks.

Cloud-delivered ZTEdge Secure Internet Access analyzes all web traffic – even encrypted web traffic – and selectively blocks, isolates, and/or sanitizes content, as needed, before it reaches endpoints. Using integrated threat intelligence from proprietary sources, real-time ZTEdge data, and information from world-class threat databases, ZTEdge Secure Internet Access optimizes protection for each website, attachment and email, to maximize security while delivering a seamless user experience.

Remote browser isolation (RBI), content disarm and reconstruction, cloud data loss prevention, secure web gateway, ransomware protection and anti-virus are among the technologies leveraged to protect organizations from internet-delivered threats.



- Intelligently isolate risky sites and risky categories to protect against malware
- Sanitize downloads to keep weaponized files off devices and networks
- Guard against exfiltration of sensitive data
- Enforce acceptable web use policies
- Create and apply granular access policies based on user, user groups, website categories and more

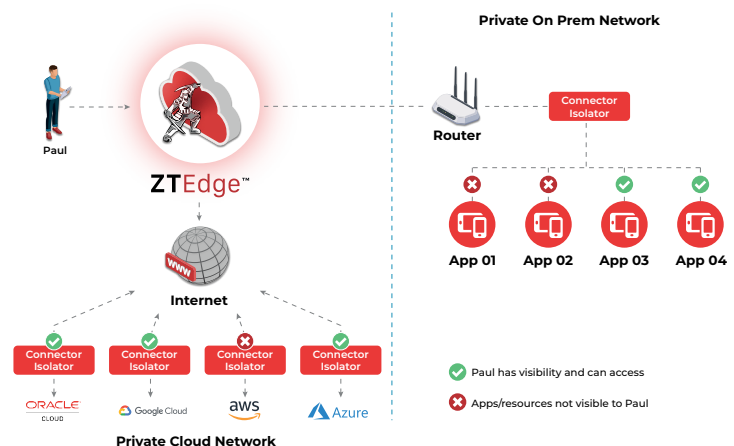
Simplified Remote Application Access

ZTEdge Zero Trust Network Access (ZTNA) addresses the challenge of enabling hassle-free access to the local network resources that remote users are authorized to use while barring access for all unauthorized parties. It is a simple cost-effective and far more secure alternative to VPNs and RDP access.

Remote users authenticate to the ZTNA cloud where their details—IP address, device, location and/or usage patterns—are checked in an authorization database. If the details check out, policy information for that user is sent an internal network connector isolator, which virtually microsegments the network to enable each user to access only the limited set of resources they are authorized to use. All others are cloaked so the user does not even know they are there.

Granular access policies are essential for enforcing least privilege access, a pillar of Zero Trust Security. But building granular access policies from the ground up is an onerous and time-consuming task – and one that must be frequently reviewed and updated. To facilitate true least privilege access, ZTEdge Zero Trust Network Access (ZTNA) includes an automatic policy generator that sets and updates policies based on each authorized user's behavioral patterns.

- Zero Trust access to private apps and resources on organization LANs or in private clouds
- Passwordless or MFA password-based authentication to network and authorized apps
- Policy-based least privilege access enforcement
- Replaces vulnerable VPNs and RDP connections
- Behavior-based automatic policy generation enables true least privilege approach



SaaS Application Access Controls

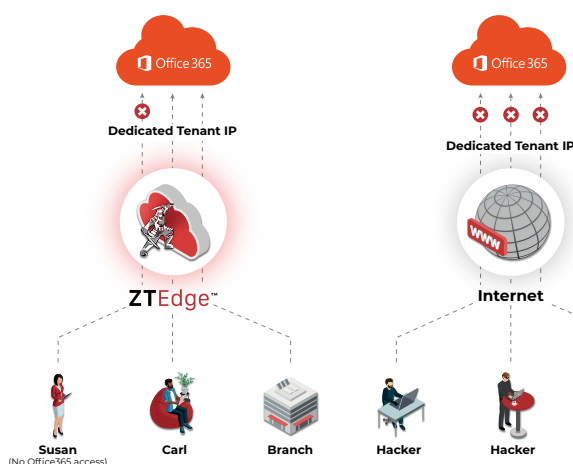
ZTEdge secures SaaS applications by leveraging SaaS app configurations that restrict each user to connecting from a user-specific, “portable” IP address.

Each tenant on the ZTEdge Cloud is assigned a dedicated, unique personal IP address by the Cloud Access Security Broker (CASB). When the user logs in to an app via the cloud, their “location” is always the same, regardless of where they actually are. Configuring SaaS app access to be restricted to this portable IP address means that a cybercriminal cannot log in to the user's workplace SaaS apps via the public internet even if a user's valid credentials are stolen or exposed, since the IP address is unique only to a specific user.

Likewise, since users must authenticate via the ZTEdge Cloud to be “located” at the IP address that enables them to log in to SaaS apps, restrictions on data access and use can be applied.

This method also offers security operations teams granular insight into who is logging in to business SaaS apps, from where, at what time, and to access what—all questions that must be addressed to ensure Zero Trust security.

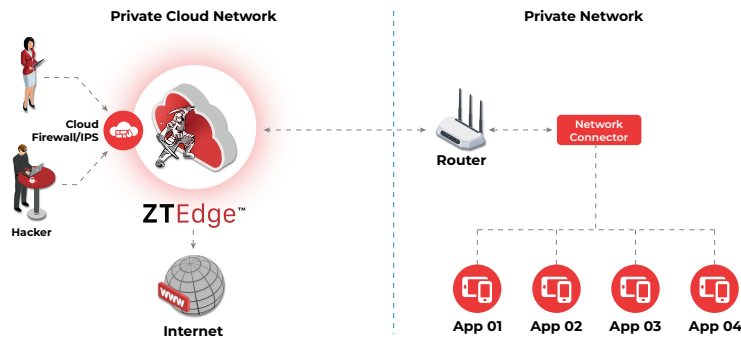
In addition to IP-address-based access controls, ZTEdge can enforce policybased restrictions on access to specific cloud applications for all users, individual users, or certain groups or locations. Alternatively, rather than blocking access completely, data sharing functions such as uploading/downloading files or entering data into cloud applications, can be restricted or entirely disabled. Additionally, file downloads from file-sharing applications can be scanned for malware to protect devices from being infected.



- Prevents access to business apps from the public internet
- Eliminates risk of external access via stolen credentials
- Enables enforcement of user, group, location and/or device-based policies for SaaS applications
- Supports restriction of user sharing and exfiltration of app reports and data
- Blocks malware in infected file downloads
- Prevents lateral movement if an attacker succeeds in accessing network

Network Protection and Visibility

ZTEdge Cloud-Delivered Firewall and IPS moves deep packet traffic inspection and malware blocking from within an organization's offices and branches outward to the cloud. It eliminates the need for on-premise firewall and IPS devices in every branch location while ensuring that malware is blocked from entering local networks. The solution's traffic analysis dashboards and reporting provides valuable insight into your network activity.



- Eliminates need for costly on premises firewalls
- Centralized firewall/IPS management for all connected branch and corporate offices
- Performs deep packet inspection to prevent intrusion attempts
- Monitors network traffic and user activity
- Provides inbound and outbound protection
- Managed service removes updating patching burden from IT

All traffic inbound to and outbound from the network gets routed to the ZTEdge Cloud proxy, where deep packet inspection detects malware present in any packet. The firewall rejects inbound traffic if threats are found, preventing it from entering the network perimeter.

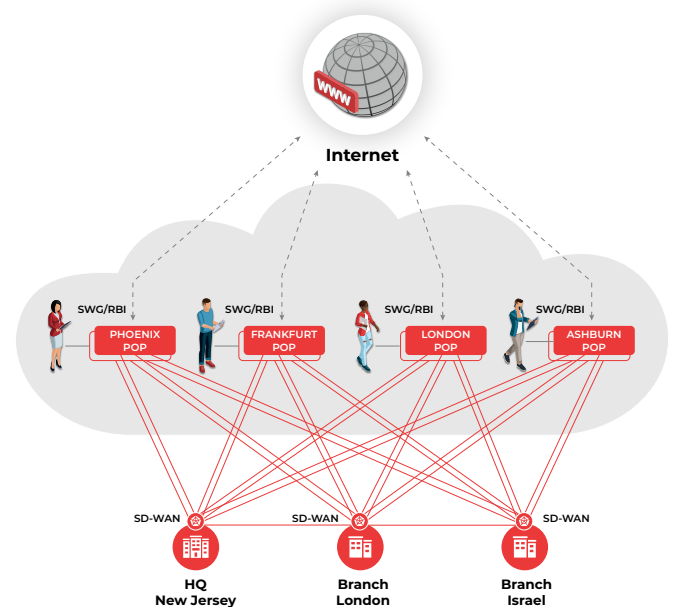
In addition to protecting organizations from malicious inbound traffic, the ZTEdge Cloud-Delivered Firewall/IPS can examine outbound traffic to ensure that sensitive information is not being exfiltrated. Inspection and traffic control policies can be configured based on user, group, location or other factors. Traffic found to violate policies is blocked from proceeding and, if desired, automated alerts can be issued, and potential malicious activity remediated.

Moving firewall and IPS functions to the cloud reduces network complexity and eliminates the need to purchase, upgrade and replace costly equipment. Centralized management improves visibility and significantly reduces burden on IT staff, while policies configured for each individual location provide the flexible protection organizations require.

SD-WAN Enabled Secure User, Branch and Internet Connectivity

ZTEdge provides simple, secure, cost-effective user-to-site, site-to-site and secure user-to internet access via SD-WAN. It can be used in branch offices to enable local secure internet breakouts, eliminating the need to backhaul traffic over costly MPLS circuits to enforce security policies. Branch users can go directly to the web and cloud, knowing that ZTEdge will inspect all traffic in line and enforce all threat prevention and acceptable use policies.

ZTEdge's distributed architecture, redundant gateway design, and tunnels to branch locations ensure reliable user access to on-site resources and, because ZTEdge SD-WAN-enabled Connectivity is provided as a service, it is affordable and requires minimal IT support.























- Secure branch office internet breakouts eliminates traffic backhauling and costly MPLS circuits
- Multi-PoP architecture for rapid user-to-site access from any location
- High-speed site-to-site access via private cloud tunnels
- Elastic, scalable replacement for VPNs
- Inspection of all traffic for malicious content

“

“ZTEdge has a broad set of affordable, always-on security capabilities, including a Zero Trust Network Access service that will reduce the complexity of remote application access for our teams, improving user experience and security compared to legacy VPN solutions.”

Brandon Nokes, Director of IT, Devada

Capabilities

	Secure Web Gateway	Secure internet access with web traffic inspection and URL filtering for enforcement of acceptable web and internet use policies
	Identity & Access Management	Robust authentication service with MFA. Used by ZTEdge platform and can also serve as a centralized ID database for your organization
	Cloud-Delivered Firewall	Control traffic flows of every connected device, location and user via flexible firewall policies
	Cloud-Delivered SD-WAN	Secure user-to-site and site-site access and connectivity for local internet breakouts.
	Zero Trust Network Access	Simplify remote access with secure 1:1 connections between users and apps
	DNS Security	Enforce web access policies based on DNS-level information
	Zero Trust CASB	Control access to SaaS apps using IP restrictions (dedicated ZTEdge IP address), deny lists, and other techniques. and limit data sharing functions
	Remote Desktop/Host Access	Securely access remote desktops and on-premise legacy host systems
	Threat Intelligence Network	Leverage URL threat intelligence data curated from multiple industry sources combined with info from global ZTEdge user community
	File Sanitization (CDR)	Sanitize web downloads and email attachments to remove threats in weaponized documents
	Network Traffic Analysis	Monitor and analyze all network traffic traversing the ZTEdge Platform, using dashboards and drill-downs, to quickly gain full visibility
	Remote Browser Isolation	Isolate risky web content in remote cloud containers to protect endpoints from ransomware and other web threats
	Intrusion Prevention/Detection	Monitor and analyze traffic to detect known and unknown threats, with automated alerts/remediation upon detection
	Microsegmentation	Restrict lateral movement on LAN by microsegmenting apps and resources
	Anti-Virus	Scan web content and downloads for known threats, and block harmful content before it reaches endpoints
	Ransomware Prevention	Improve ransomware detection with enhanced threat intelligence
	Cloud Data Loss Prevention (DLP)	Prevent sensitive data like SSNs and these bottom ones need to be indented credit card numbers from being shared on the web or in cloud apps (coming soon)
	Anti-Phishing	Block known/suspected phishing websites based on URL, source IP, signatures and more
	SSL Inspection	Identify and block malware hidden in encrypted packets with policy-based web SSL traffic inspection
	Data Anonymization	Anonymize organization's personal data to comply with PII/GDPR and avoid sanctions