ZTEdge™

SaaS Application Access Control

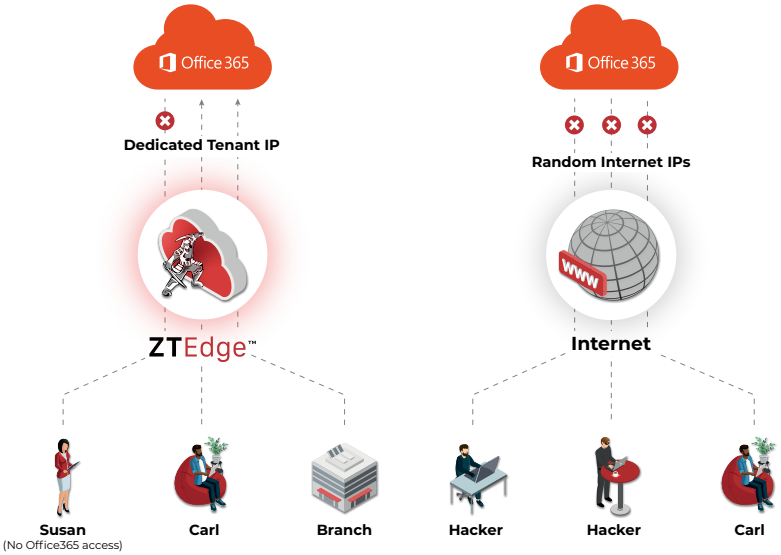
Zero Trust Answers to the *Who, What, When, Where,* and *How* of Secure Access

How Secure are Your Apps?

Businesses have eagerly adopted SaaS applications, yet the insufficient security controls they apply to those applications and to users who access them expose the companies to risk. User credentials are often exploited by threat actors who obtain them through business email compromise (BEC) or phishing attacks; purchase credentials that have been exposed through breaches and double-extortion ransomware attacks; or simply discover them in brute-force attacks. Once in, those threat actors have full access to sensitive data and can cause extensive damage.

Most SaaS applications address credential reuse via security controls that force users to log on only from specific IP addresses. While this can help prevent cybercriminals from accessing those applications with stolen credentials, this solution also restricts valid users' ability to access their apps when working from home or on the road.

Businesses must also act to prevent unsanctioned exfiltration of sensitive data stored in SaaS apps. Authorized users who log in via unmanaged devices may download data to their devices, save them to their personal cloud storage app or otherwise expose them, either maliciously or through negligence.



The Solution: 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 policy-based 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.

ZTEdge SaaS Application Access Control Highlights

- 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

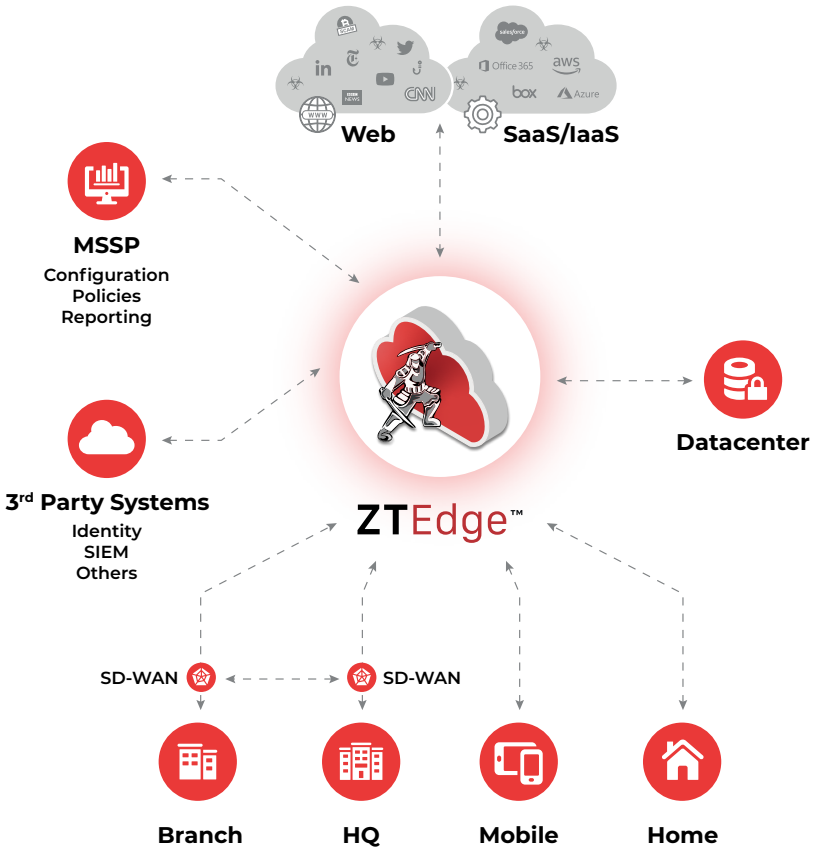
ZTEdge™

SaaS Application Access Control

Enterprise Zero Trust Security for Midsize Enterprises and Small Businesses

ZTEdge is built to protect what matters for your midsize enterprise or small business – your users, data, applications and customers. The platform cuts complexity, reduces cyber-risk, and improves performance, all at a dramatically lower price point than alternative solutions.

> *"Given the large enterprise orientation of most security solution providers, we wanted a right-sized solution that provides a simple, cost effective way for MSEs to quickly implement their own SASE strategy. The ZTEdge platform is the solution to do just that and is a valuable addition to the market."*
>
> Mark Mahovlich, Vice President of Strategy & Execution, ICM Cyber



ZTEdge Capabilities

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

www.zerotrustedge.com

Americas:
T +1 (201)767-2210
E-mail: info@zerotrustedge.com

UK & Western Europe:
T +44 (0)1905 777970
E-mail: info@zerotrustedge.com

Worldwide:
T +972-2-591-1700
E-mail: info@zerotrustedge.com

Follow us