ZTEdge™
By Ericom Software

Reliable, Secure Access and Data Sharing Controls for Office365

Optimize Use of Microsoft SaaS apps like Office 365 (O365) with enhanced data, endpoint and network security controls paired with high-performance Azure Peering

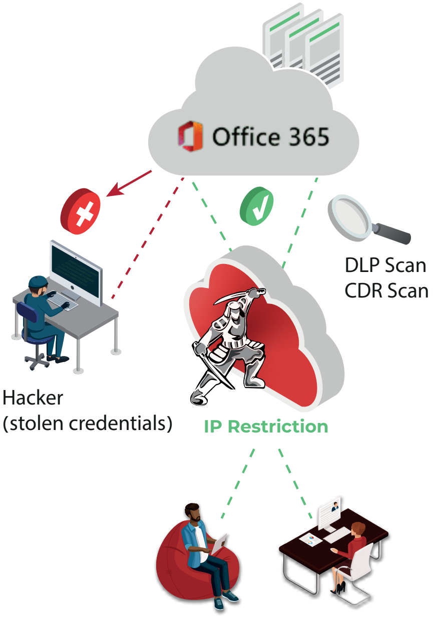
Spurred by distributed workforces and a severe shortage of IT professionals – and encouraged by cloud service vendors and plentiful bandwidth – organizations worldwide are opting to switch to SaaS versions of the apps they depend on for essential work tasks. O365 is a prime case in point, with more businesses than ever using hybrid or fully cloud versions of Word, Excel, Powerpoint and other key Microsoft applications.

While the cloud service model has many advantages, sailing is not always smooth. Service may be slow during times of peak internet use. From a security perspective, cybercriminals are continually trying to get their hands on O365 credentials to steal data. And browser clipboarding and printing functions make it simple for users to copy sensitive data for benign – but still risky – reasons, like for use when they can't be online, or for malicious purposes, like insider attacks.

Traditional perimeter-based data loss prevention (DLP) solutions are powerless to stop these types of data leaks. With no visibility into cloud traffic and the use of stolen credentials to access corporate O365 accounts, business can't keep sensitive info from being exposed – or even detect that it was.

O365, like most cloud apps, allows access to be restricted to specific IP addresses. But with users now working from almost any location, including open networks, such limitations are no longer practical. Worse still, infected files from user devices may be uploaded to OneDrive or Sharepoint and spread malware throughout company cloud storage and onto other user devices.

Turn O365 Dark to hackers while preventing data leakage and malware from downloads



The Solution: ZTEdge Web Security & CASB Controls

ZTEdge Web Security includes key SaaS application access controls that allow organizations to secure their O365 accounts and data. The solution integrates high-performance Azure Peering with ZTEdge Cloud Access Security Broker (CASB) controls, remote browser isolation (RBI), content disarm and reconstruction (CDR) and data loss protection (DLP) to ensure reliable and secure O365 use, by all users, wherever they are.

With ZTEdge, access to your corporate O365 tenants can be restricted by IP address, so only users that have been authenticated through your ZTEdge Web Security tenant, which has a dedicated IP address assigned specifically to your organization, will be permitted to enter their credentials on your O365 login screen. This means that any hacker who may have phished or stolen your users' valid credentials will be unable to use them. To anybody but your authorized users, your O365 tenants have been turned completely dark.

As an Azure Peering partner, ZTEdge ensures robust, high-performance, low-latency connectivity to the Microsoft cloud from any location. Users are ensured access to the Microsoft Global network via the nearest edge PoP, along the best-performing route.

Additionally, routing O365 sessions via cloud-based isolated containers enables ZTEdge to apply a variety of security controls:

Data Access and Sharing Controls: Since users connect to O365 through ZTEdge, policies can be enforced to control access. For example, IT teams can control what actions each user or user group can take, for each file or type of data. Policies can determine if file types like Excel or files in a specific directory can be downloaded or printed using browser commands, or if specific users can upload files to apps like OneDrive. For further protection, ZTEdge Cloud DLP policies can help protect sensitive data and PII, preventing users from sharing credentials, social security numbers, credit card info or other data in OneDrive, Outlook webmail, or websites.

Threat Prevention: The ZTEdge solution includes content disarm and reconstruction (CDR) so documents attached to incoming webmail, or which users download or upload to OneDrive can be scanned to remove any malicious payloads. Files are opened in an isolated container in the ZTEdge cloud, disarmed of any malicious content they contain, and reconstructed before being moved to their final destination with native functionality intact.

ZTEdge™
By Ericom Software

ZTEdge Web Security for Microsoft O365 Highlights

- ZTEdge dedicated user IP addresses enable IP-based access control to eliminate risk of remote access to O365 accounts via stolen credentials
- Enables enforcement of user, group, location and/or device-based policies for accessing O365 applications
- Supports restriction of data capture functionality like clipboarding, printing, downloading, etc.
- Enforces DLP policies to the subdomain, individual user, and PII field levels to protect sensitive and confidential information
- Anti-virus and CDR examine and, when needed, disarm and reconstruct documents in isolation before uploading or downloading them with desired functionality intact
- Global peering relationship with Microsoft Azure provides low-latency connectivity to MS Cloud and an excellent user experience
- User-friendly management and automatic policy builder simplify creation of highly granular controls
- Provides visibility into which users are accessing which O365 applications from where and at what times

> “
>
> *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

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 your existing SWG

ZTEdge ZTNA, Apps and Network

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

ZTEdge Desktop

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