Solution Brief

Military Interoperability: Connect Your Coalition Partners & MPE

The Answer for GFE and Unmanaged Devices

Contents

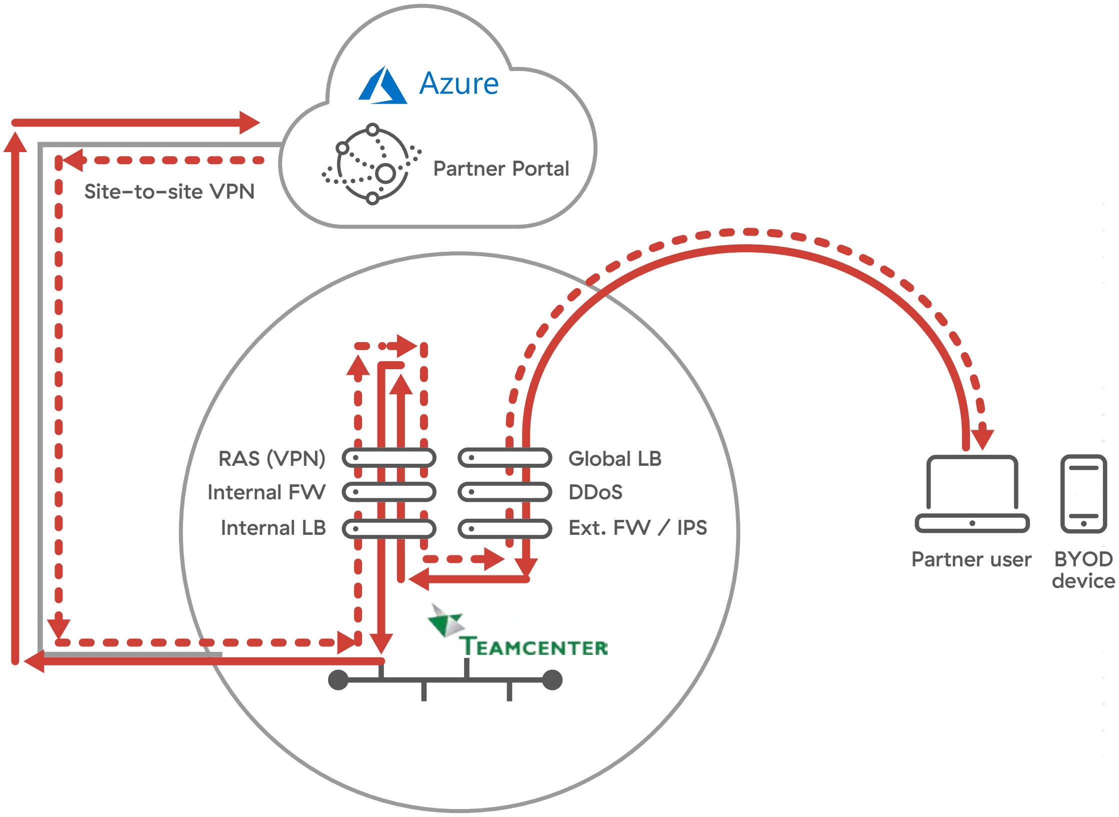
How Partner Access Was Done Before

In the past, partner access was achieved through partner portals leveraging a traditional remote access VPN. A third-party mission/coalition user must download the VPN client onto their managed or personal device, the IT admin manually provisions access through the firewall and ACL policies, and the user will VPN into the other enterprise's network. Once on the network, the third-party mission/coalition user was able to access the entire network with minimal restraint due to limited regulation.

Why Change Is Needed

Enterprises shouldn't have to choose between placing third-party mission/coalition users on the network or allowing no application access at all. When third-party users connect to the network they receive full network access, expanding the attack surface of the network and creating another point of vulnerability for invasion. Quite simply, existing security practices give third-party mission/coalition users far more freedom than necessary. In a zero trust architecture, segmenting the network is not a viable alternative and also leads to additional complexity.

In many cases third-party mission/coalition users are connecting in from untrusted devices on untrusted networks. If a user's device is infected with malware and connects to the network, the entire network is placed at risk. This can lead to data breaches that cost millions—not to mention a heavy hit to brand reputation and a potential negative impact to mission success.



Partner users and BYOAD devices connect into the network and receive full and lateral network access. These overprivileged users heighten network vulnerability by increasing the attack surface area and therefore risk of breach. Yet, beyond these significant risk factors, one would think that your partners would at least be given a good user experience since so much liberty is given… think again. The process of gaining application access is frustrating since most users will need to switch between different VPNs from multiple organizations. In the end, third-party mission/coalition partners still need a way to access internal applications that addresses the issue of the over-privileged users and their associated risk.

Embracing a Modern Approach to Securing Third-Party Access for Mission/Coalition Partners and Application Access, (Not Network Access)

Mission/coalition partners should never be placed on the network. Why introduce the unnecessary risk of granting them network access if they only need access to internal applications?

Secure third-party access needs to be founded on the principle of least privilege, where only named users have access to specific named applications using micro-segmentation.

Least Intrusive Security for Mission/Coalition Partners

Yes, the enterprise and tactical environments need to protect their internal mission applications from threats, but third-party mission/coalition users need to be able to access them seamlessly. IT should not be forced to choose between first-class security or a great user experience. Third-party mission/coalition access needs to encourage strong partnerships by enabling quick and easy access to private applications, while never granting access to the actual network.

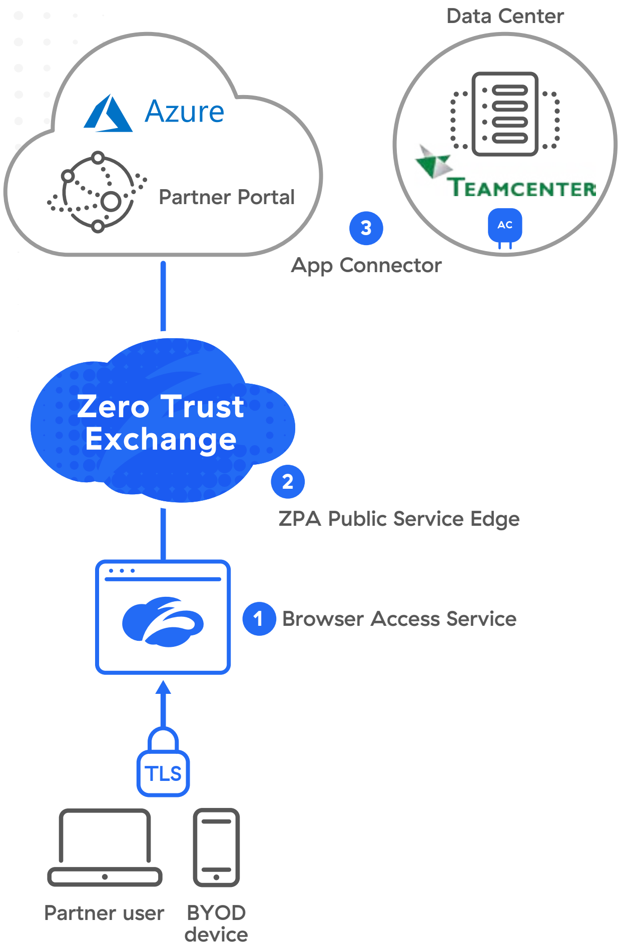
IT Empowerment

IT needs to take back visibility and control over application activity and access. Visibility no longer should be defined as user IP address and port data, and network segmentation cannot provide the level of access control needed for IT. Visibility needs to be contextual, informative and in real time. IT needs to have the means to control activity down to the granular user, device, and named application level.

Eliminating Third-Party Mission/Coalition Risk with Zscaler Private Access (ZPA)

With increasing business integration requiring third-party mission/coalition access, and threats continually becoming more advanced and aggressive, the risk from partners only escalates. As the network-centric approach to securing partner access continues to become less secure and less effective, software-defined access to private applications will only increase in necessity as IT seeks to minimize risk.

Zscaler Private Access (ZPA) takes a user and application-centric approach to security by default. Whether that user be an employee, vendor, contractor, or third-party mission/coalition partner, ZPA ensures that only authorized users have access to specific internal applications without ever giving access to the network. IT no longer has to worry about partner's exposing their network to risk because users are never placed on the network. IT can create and enforce granular policies for users to access only specific applications through inside-out connections. These connections are fully encrypted and spun up on-demand to enable application segmentation. This means no more over-privileged third-party users. With ZPA's browser access capability, partner access is truly effortless. The feature allows third-party users to freely use their own BYOD devices to seamlessly and securely access an internal web application leveraging any web browser with no client needed on their devices.



1. Browser Access Service
- Redirects traffic to IDP for authentication
- Removes need for client on device

2. ZPA Public Service Edge
- Secures the user-to-app connection
- Enforces all customized admin policies

3. App Connector
- Sits in front of apps in cloud and data center
- Listens for access requests to apps
- No inbound connections; responds with inside-out connections only

The Next Frontier in Private Mission/Coalition Application Security: Zero Trust Cloud Browser Isolation for Private Mission/Coalition Applications for Unmanaged Mission/Coalition Devices

Zscaler Cloud Browser Isolation to private mission/coalition applications reimagines security by stripping attackers of their most advanced tools and techniques. By isolating users and endpoints from all active web-based content, security teams can gain peace of mind that their enterprise is protected from zero-day vulnerabilities, ransomware, unsanctioned plug-ins, and other sophisticated threats. Separating users from sessions also helps stop accidental and malicious data leakage. Make web-based attacks and data loss things of the past.

The Ultimate Expression of Zero Trust for Safe SaaS Web and Private Mission/ Coalition Application Access

Zero trust is built on the premise that all network and user activity should be untrusted by default. It's time to accept that the web is an untrusted but necessary resource. With Cloud Browser Isolation, you can extend the definition of zero trust to everything users do on the internet, in SaaS, and through private apps.

Zscaler serves as an exchange between users, the internet, SaaS, and private apps, with the ability to inspect all traffic and enforce policy inline. As traffic traverses the Zero Trust Exchange, Cloud Browser Isolation isolates it in real time, transforming web content into a safe stream of pixels streamed to the user. Create an air gap between users and the web and maintain the experience users expect.

Benefits

Neutralize web based threats: Deliver safe browsing and web application access by creating a virtual air gap between users and web destinations in a fully isolated browser session.

Keep applications and data safe from compromise: Protect mission/coalition applications from exploitation and data leakage by controlling browser code and streaming sessions as pixels to users; do so agentlessly to secure unmanaged devices.

Enable a true expression of zero trust: Gain true zero trust security by eliminating the attack surface and giving users access only to applications themselves, obfuscating app metadata like host information, protocol, OS, and software and firmware versions.

Use Cases

Zero Trust Threat Isolation: Protect Against Advanced Threats
Stop zero-day vulnerabilities, patient-zero infections, ransomware, drive-by downloads, malvertising, and other attacks from reaching end users by isolating web traffic, thereby creating an air gap in front of web content.

Safely render Microsoft 365 documents (XLXS, DOCX, and PPTX) as PDFs to ensure malicious macros and other active content can't reach end users.

Fully integrated into the Zero Trust Exchange to get the highest level of security and visibility for all web traffic, whether it originates in a native browser or a Cloud Browser Isolation session.

Zero Trust Data Isolation: Stop Sensitive Data Leakage
Allow read-only access to web-based SaaS and private applications while restricting copy, paste, and print to prevent data leakage and theft.

Get granular control of upload/download activity across SaaS and private applications to protect confidential mission data.

Zero Trust Application Isolation: Secure Unmanaged Devices
Agentlessly secure SaaS and private app access for remote employees, contractors, and third-party partners on unmanaged devices to protect data.

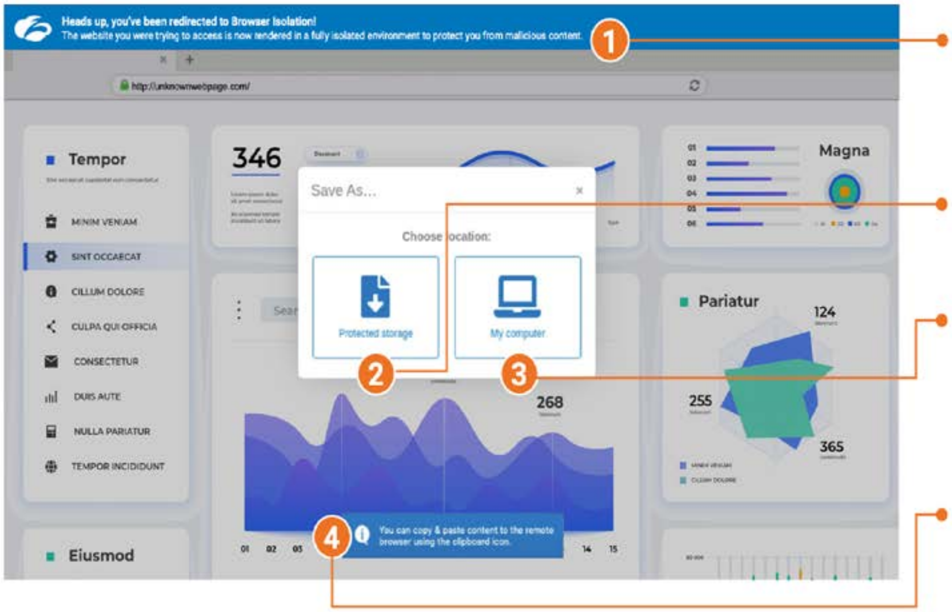
Isolate applications, without software installations, to stop attackers from using vulnerable clients and malware-infected endpoints to exploit apps.

Zero Trust Key Partner Isolation: Secure Highly Targeted Users and Missions
Provide an extra layer of security for users and missions that are targeted by attackers more often than others.

Define granular isolation policy based on user group such as, executives, senior leadership, contractors, warfighters, cyber, and IP holders.

Ensure an optimal web experience for highly targeted users to maintain mission productivity.

Users Will Hardly Notice It's There



Heads up, you've been redirected to Browser Isolation!
The website you were trying to access is now rendered in a fully isolated environment to protect you from malicious content.

You can copy & paste content to the remote browser using the clipboard icon.

1. Provide safe access to active web content by creating a virtual air gap between users and the internet inside a Cloud Browser Isolation session

2. Keep users protected from threats by confining downloaded files to the isolated environment

3. Protect against the theft of sensitive business data from file sharing services and private applications with granular policy to prevent file downloads

4. Stop data leakage by controlling user ability to copy and paste data inside SaaS apps

Key Capabilities

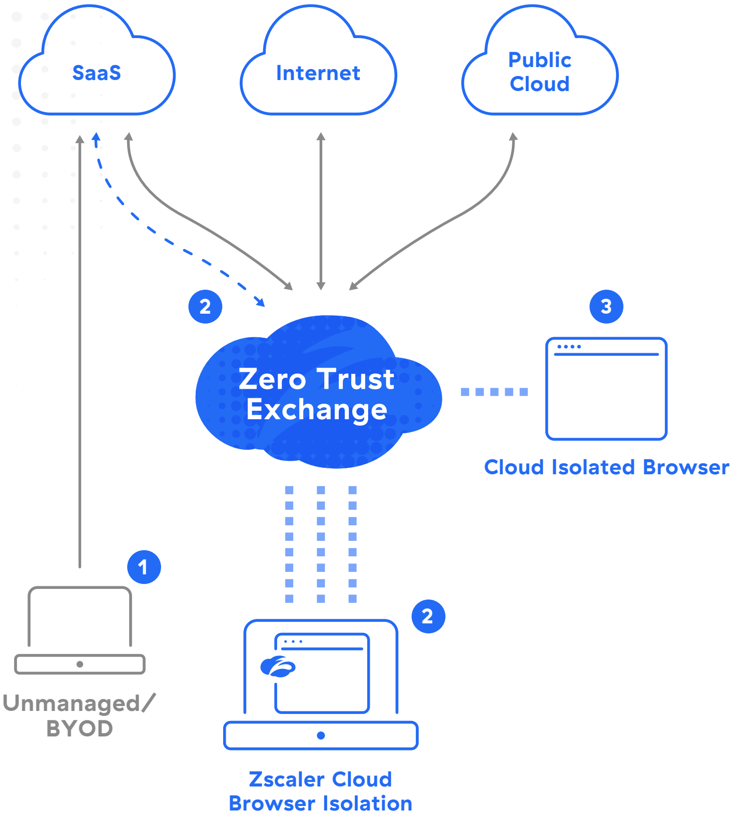
An Unmatched User Experience
Unique pixel streaming technology and Zscaler's direct-to-cloud proxy architecture ensure the lightning-fast connection to apps and websites users expect. Users are sent a high-performance stream of pixels via their browser over an HTML5 canvas to guarantee security without slowing down mission productivity.

Consistent Protection for Users Anywhere
Protect any user on any device in any location with a zero trust isolation policy that spans even your most highly targeted functions and missions.

Less Management Hassle
Deploy and manage in seconds with cloud agility as a natively integrated extension of the Zero Trust Exchange. Avoid end-user browser performance degradation by leveraging your existing Zscaler Client Connector (or an agentless option) to route traffic through the Zero Trust Exchange.

Universal Compatibility Built In

Cloud Browser Isolation works with all major browsers, including Chrome, Safari, Firefox, and Internet Explorer. Cookie persistence for isolated sessions ensures users' key settings, preferences, and sign-on information remain intact. Let users keep their preferred browser to stay productive.



How it works

1. User tries to access a potentially malicious webpage, a SaaS app, or a private app from a managed or unmanaged device
2. Request is evaluated against defined policies, and if there is a match, an isolated browser session is created
3. Zscaler connects to the webpage or app and loads the content onto the isolated browser
4. Web content is streamed to the user's browser as pixels over an HTML 5 canvas

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.