Using Zscaler™ to Secure BYOD Access

Many organizations have enacted bring-your-own-device (BYOD) policies as a way to support the unexpected rise in remote work. BYOD gives users a seamless work experience while keeping productivity high, but it also introduces risk to organizations.

With BYOD, remote users are often connecting over untrusted Wi-Fi networks, which makes visibility into user activity a must for IT. Since IT does not have the benefit of installing an agent on these devices, such visibility isn't possible, and it's difficult to enforce policies, block threats, and prevent the spread of malware. Furthermore, IT teams are unable to check for the presence of endpoint security or antivirus software, or even ensure that operating systems are up to date. And each user may have more than one device, making it difficult to track user activity with each additional device the user may own.

Device

Posture of the device

Unsupported device

Lack of device control

User

Data retrieval

Establishing identity of user with all their devices

Application Access

Inherent trust

To enable work-from-anywhere, users must have access to apps and data in spite of using unmanaged devices and unverified networks. As a result, remote users are inherently trusted, which is contrary to the zero trust model.

Enable zero trust access for BYOD

Zscaler Private Access™ (ZPA™) is a cloud-based service that provides users with zero trust access to applications based on authentication and authorization. Whether your applications are on the public cloud, private cloud, or your data centers, the ZPA Public Service Edge is able to seamlessly connect the users to applications regardless of where they're connecting—all with zero trust at the center of it.

PAYCHEX

"With ZPA, users get access to what they need without being hijacked, and this becomes manageable from a security perspective and a common user experience regardless of where they are working from."

–Randy Longhenry, Network Engineering Manager, Paychex

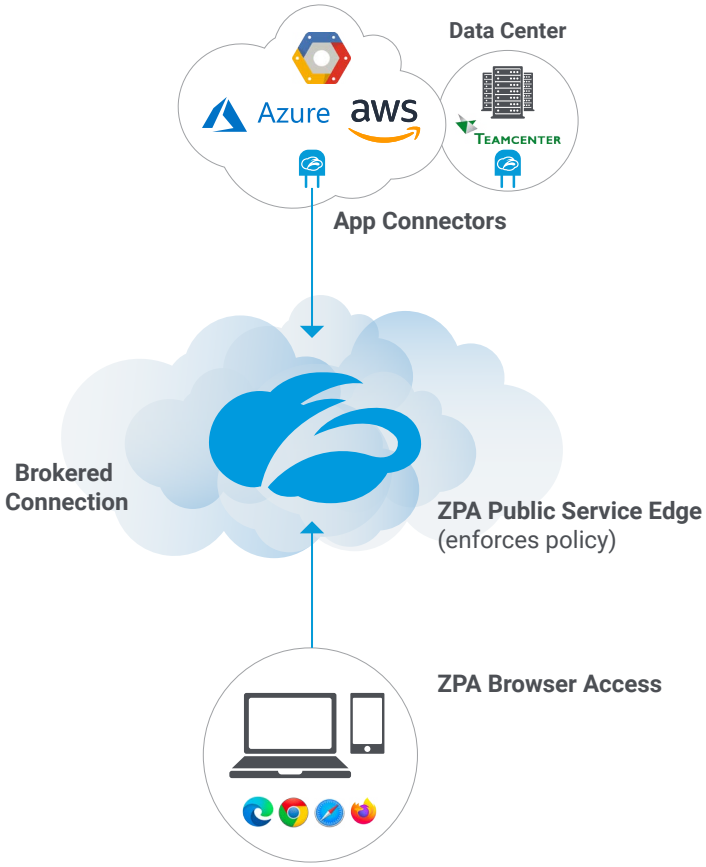
ZPA Browser Access provides application access without the need for an endpoint agent.

Device support is not an impediment due to no dependency on device type.

APIs for IDP allow for **SAML integration and support SCIM.**

Single location via the **Client Connector Portal** displays all apps a user is authorized to access.

Zscaler Cloud Browser Isolation prevents data from flowing down to unsecured devices.



Request a Demo >

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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

zscaler™

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com