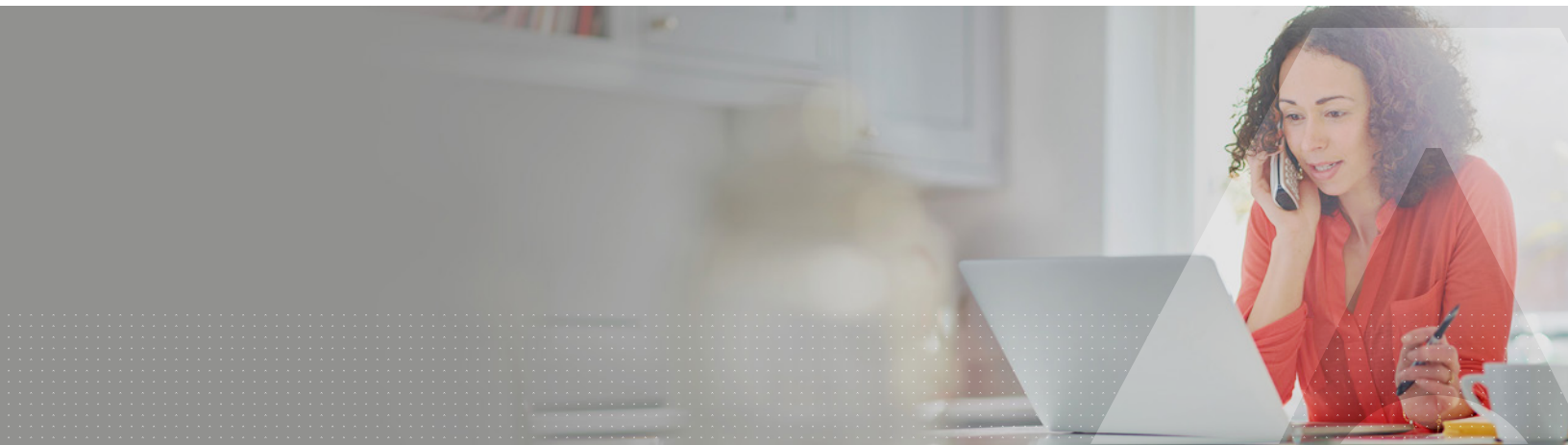


SafeNet Trusted Access and Zscaler Private Access Solution

Protecting and streamlining your IAM Environment



Securing your Zero Trust Access to Private Apps

Today's organizations are constantly under the threat of costly security breaches. The need for remote access to corporate resources has grown exponentially. Providing secure and simple access to internal resources, for both employees and third-party contractors, regardless of their physical location and device, requires support for a wide range of remote access requirements.

Access Management and Zero Trust Private Access: Better Together

Thales and Zscaler work together to achieve Zero Trust security, providing access to all apps securely, regardless of whether the apps are in the cloud or on-premises.

Thales SafeNet Trusted Access (STA) provides powerful protection by enforcing rigorous access policies at the access point with adaptive and multi-factor authentication, while Zscaler Private Access (ZPA) creates micro-segmented trusted zones to control which applications are available to authorized users.

STA ensures a single sign on experience to resources behind the Zscaler Service Edge by applying modern access management and authentication, including policy-based access and adaptive authentication at the Zscaler ZTNA console. STA ensures the right people have access to the right apps under the right conditions and enables users to access applications securely.

Highlights

Simplified Strong Authentication

Automated workflows provide flexible, context-based authentication and a broad range of strong authentication options to mitigate reliance on passwords.

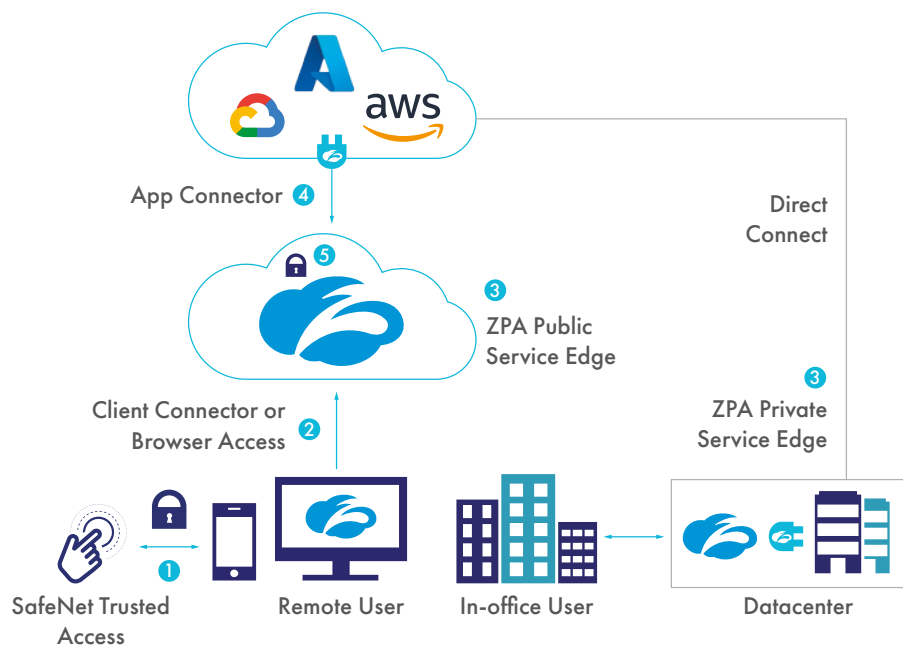
Convenient and Secure

Convenient yet secure access to business resources increases productivity and reduces workload at the helpdesk without compromising security or compliance. Supports BYOD and BYOPC initiatives.

Protect Everything

Apply a Zero Trust security model by extending policy-based access, single-sign-on, adaptive authentication, and multi-factor authentication to your Zscaler solution and other cloud applications.

Zscaler gives users the ability to access on-prem applications. Zscaler provides a scalable Software-Defined Perimeter (SDP) that enables an On-Demand Perimeter, providing administrators with the ability to dynamically create access rules for authenticated users to access on-prem applications and data in a fully-automated process.



How it works:

- 1 User authentication with IDP (first time only)
- 2 Authorized user attempts to access an app; Client Connector tunnel is created
- 3 The ZPA Service Edge enforces policy and sends dispatch to connectors
- 4 The App Connector closest to app sends inside-out tunnel to ZPA Service Edge
- 5 The ZPA Service Edge stitches together the connection between app and user

STA integrates easily with Zscaler ZPA to provide an elegant solution that balances security and usability to protect all corporate resources behind the ZPA Service Edge.

How the Joint Solution Works

STA integrates with Zscaler ZPA to allow businesses to securely scale up to support a remote workforce and suppliers, and access applications and data in the cloud and on premises.

Scale securely in the cloud

Access Management enables you to expand with the confidence you are secure. Protect all cloud apps with centralized policies and a range of authentication methods.

Security at the access point





STA enforces access policies and the appropriate level of authentication to assess users and applications accessing Zscaler ZPA, protecting businesses from unauthorized access and reducing the risk of a data breach.

Combining STA with ZPA, authorized users can access both cloud-based and on-prem applications.

Zscaler provides access to on-premises applications with an on-prem ZPA Private Service Edge, and to cloud-based applications with a cloud-based ZPA Public Service Edge. In both cases, Zscaler manages the Service Edges and no appliances are required.

Key Benefits

Together, STA and Zscaler let you control access to critical systems without hindering the work authorized users need to perform. STA authenticates and enables authorized users to access cloud-based apps—including Zscaler. Working with STA, Zscaler provides secure access to on-premises apps and data.

> cpl.thalesgroup.com <    

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

About Zscaler

Zscaler's flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100 percent cloud-delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances are unable to match.

One half of Zscaler's Cloud platform, Zscaler Private Access (ZPA) provides secure, software-defined access to internal applications running on public cloud and within hybrid environments without the need for VPN. ZPA decouples application access from network access, and delivers comprehensive visibility into user activity, enabling enterprises to embrace a zero trust strategy.

About Thales Access Management

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web, and cloud-based applications with a Zero Trust approach. Utilizing policy-based conditional access, rigorous SSO, and universal authentication methods, enterprises can effectively prevent breaches, migrate securely to the cloud and simplify regulatory compliance.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.