avast business

DATA SHEET

Secure Private Access

Avast Secure Private Access (SPA) replaces the traditional VPN with a cloud-based zero trust network access (ZTNA) solution that lets users easily and securely access business applications from any device, anywhere, any time.

SPA is a cloud service that uses a distributed architecture to provide fast and secure access to private applications running on-prem or in the public cloud. The service provides access based on four key principles:

- The internet has become the enterprise's new transport network
- Application access is based on user permissions and will not require inside the network access
- Inside-out connections are used to make the network and applications invisible to hackers
- Application segmentation should connect users to a specific app and limit lateral movement

Benefits

78% of enterprises are looking to adopt a zero trust strategy. Here are some justifications for making zero trust network access (ZTNA) technology part of your digital transformation journey.

Simplified management:

100% cloud-based solution that is easy to manage from one platform and is consistent across all apps and devices.

Better user experience:

Eliminates the distinction between being on and off the corporate network. Users don't need to connect anymore since they have always-on access across all apps and devices. This results in increased end-user productivity.

Enhanced security:

With ZTNA, access to private apps no longer requires network access. Service-initiated ZTNA architectures use an inside-out connection to make apps invisible to the internet.

Unlimited scalability:

100% cloud-delivered, zero trust network access service that doesn't require appliances and improves flexibility and agility. This enables digital ecosystems to function without exposing services directly to the internet, thus reducing risks of distributed denial of service (DDoS) attacks.

Reduced complexity:

Straightforward deployment and implementation with no need to set up VPN gateways. This makes deployment simple and scalable, eliminating infrastructure overhead.

Reduced cost:

No need to upgrade or purchase VPN appliances and clients. Improves user productivity and scales simply by adding users.

Features

Secure Private Access Platform
Global data centers, high availability, SAML authentication, etc.

Global visibility for users and applications
Single pane of glass shows which users are accessing private, internal apps.

Secure private application access to internal apps with Zscaler App
Allows secure access to internal applications (whether public/private/hybrid cloud or data center environments) without exposing network or apps to the Internet.

Secure private application access to web apps
Allows secure access to all web-based applications while simultaneously making the company network and apps invisible to cybercriminals.

Includes SPA App Connectors for App Servers
Lightweight VM deployed in data center, cloud, and hybrid environments, enabling secure connectivity to applications through Secure Private Access.

Multiple identity provider support
Enables simultaneous support of Active Directory and multiple other IDP services.

Application and server discovery
Wildcard policy shows application and server locations as they are requested by users.

Enterprise DarkNet with DDoS protection for apps
Applications are only visible to users that are authorized to connect to them.

User Portal
A centralized portal that visually displays applications the user can access.

Microsegmentation by application
Granular access control by user or group for up to five specific application definitions, each of which may contain multiple hosts and/or ports.

Client Connector
A lightweight application for roaming devices to access Secure Internet Gateway and Secure Private Access. Available for Windows, Mac, iOS, and Android.

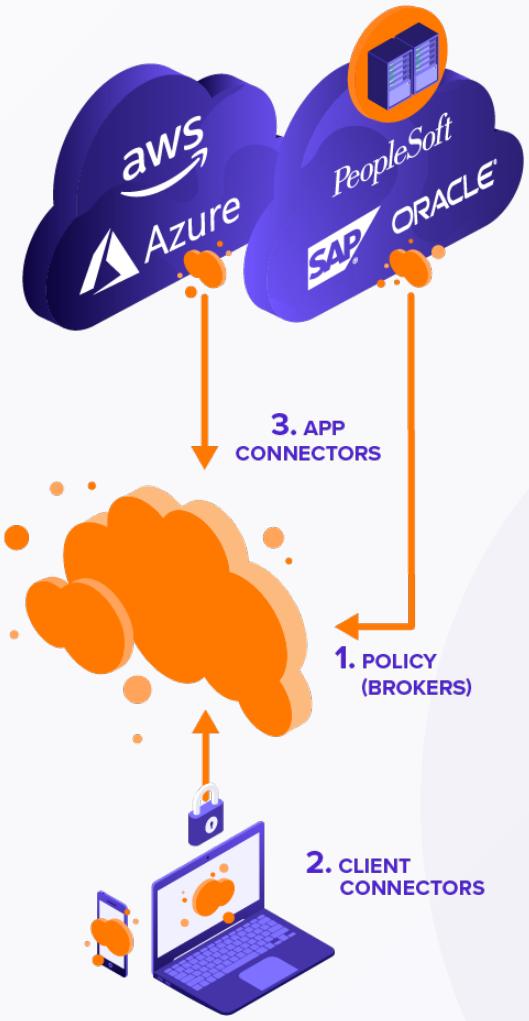
Device posture enforcement
Checks device fingerprint and certificate, as well as other postures.

Log Streaming Service
Automatically streams logs to SIEM provider.

Double Encryption with customer provided PKI
Allows for use of customer-provided certificates. Provides encryption to the microtunnel using the customer's Public Key Infrastructure (PKI).

Here is how SPA works:

1. A mobile user tries to access the company's internal applications. Instead of logging into their VPN client (and having to do so each time they start a session), the user simply opens up the Client Connector app on their laptop, mobile phone, or tablet.
2. The Client Connector app instantly routes traffic directly to the nearest Cloud Enforcement Node. The Enforcement Node servers are the "brokers" that are hosted within the global Zscaler cloud platform, supported from all locations and available at all times. The Enforcement Node first verifies the user, operating on a zero trust basis, and integrates with the enterprise's identity provider to authenticate the remote user. This is based on contextual access rather than relying on ACLs or IP addresses, which are tethered to individual devices. Before access is granted, the Enforcement Node applies all customized policies established by the IT admins, making only authorized applications visible. The Enforcement Node then sends a signal calling out to all private App Connectors.
3. The App Connector often deploys as a small VM that sits in front of all privately hosted applications, whether that be in the data center, public cloud, or private cloud. The App Connector closest to the requested application receives the call and responds with an inside-out connection down to the Enforcement Node. This inside-out connection is key to how SPA delivers zero trust. This creates a unique, secure segment between a user and application using encrypted micro-tunnels, avoiding the need to perform network segmentation and keeping applications invisible as IP locations and inbound firewall ports are never exposed. With hackers unable to scan your network, DDoS attacks become impossible.
4. The enforcement node then brokers a secure connection between the application and the user, granting application access instead of network access. The user receives the fast and easy application access they want, and the IT admins can implement zero trust security while gaining the complete visibility and control they need.



About Avast Business

Avast delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit www.avast.com/business.