SOLUTION BRIEF

Zscaler™ Private Access

Secure application- and user-specific access to private internal applications

Zscaler Private Access delivers policy-based, secure access to private applications and assets without the cost, hassle, or security risks of a VPN. Using the Zscaler App, users can now get all of the benefits of Zscaler's Cloud Security Platform for Internet traffic, as well as granular, policy-based access to internal resources from a single point.

BENEFITS

- **Optimal Security:** Users get application access without network access, and can only see the apps and resources they are authorized to access.
- **Better Value:** There's no need to buy, maintain, or upgrade VPN hardware, no need for redundant VPNs or additional user licenses in case of emergency, and no need to set up site-to-site VPNs to facilitate a move to the cloud.
- **Better User Experience:** There's no need to log in to a VPN client; if a user is authorized to access an application, it "just works."
- **Rapid Deployment:** Automatically discover application locations, then provision the specific policies that you want; there are no complex NAT/ACL/ firewall policies to configure or maintain.

Virtual Private Networks (VPNs) have been the standard method to provide remote access to private applications and assets since users began moving away from a central office with a direct connection to the data center.

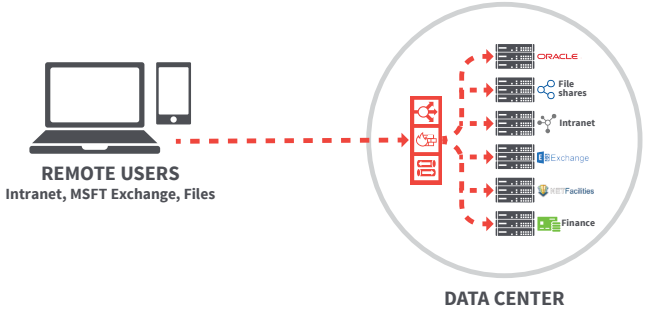
VPNs extend the enterprise network perimeter to "trusted" users, providing them with an "on-net" experience. As the network perimeter has evolved and use of the cloud becomes increasingly prevalent for business and personal applications, however, certain attributes of VPNs have become drawbacks.

An "on-net" user experience brings risk

VPNs were designed to deliver the user access to a network, not to an application. Once on a network, malware can propagate and users may be able to get access to adjacent applications from which they should be restricted. In addition, because VPN concentrators must listen for inbound connection attempts, they create an attack surface which may be exploited.

Virtual private networks are networks

As the enterprise network becomes increasingly mission-critical, it has become increasingly complex. The proliferation of VPNs adds exponentially to this complexity.



With VPNs, application access is really network access

This is partly because, like any other part of an enterprise network, the VPN must be highly available. This typically leads to multiple, regional data centers, each with load balancers and redundant configurations to ensure reliability. Enterprises often must further deploy global load balancers to ensure availability in case of regional disaster, as well as purchase additional user licenses for concurrent use.

VPNs are costly

The cost of installation, deployment, maintenance, and upgrades required by any network appliance can be daunting. VPNs also require client software to instigate connections and concentrators to terminate them, as well as helpdesk staff to direct users. These CAPEX/OPEX expenses are in addition to the possible costs that can be incurred by increasing security risk, network complexity, and business inflexibility.

VPNs don't work well with cloud deployments

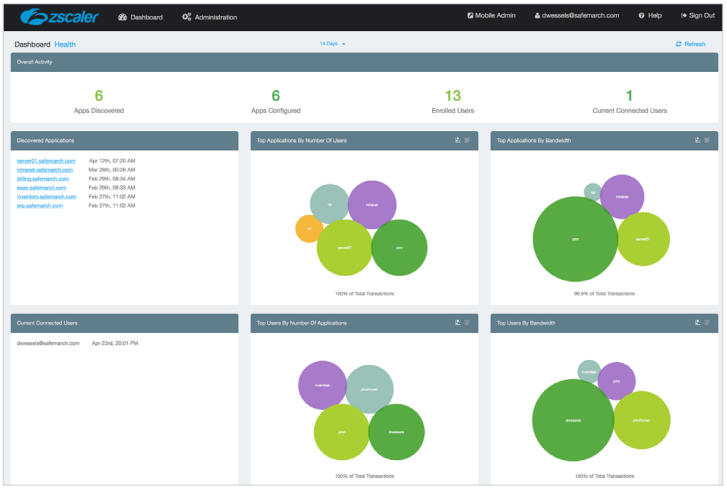
In this age of data center consolidation, most enterprises are looking to the cloud to address the need for flexible, elastic application hosting. Unfortunately, getting remote users to these deployments remains anchored firmly to the network by the VPN. Remote user traffic ends up traversing the Internet to get to the data center, in order to get to the cloud-based app via the site-to-site VPN between the data center and the cloud apps. It's terribly inefficient—like flying from San Francisco to London by way of Buenos Aires—and provides a similarly terrible experience for the user.

Despite their drawbacks, however, VPNs in some form have remained the only viable solution for secure remote access for over a decade. Until now.

ZSCALER PRIVATE ACCESS

The first major breakthrough in secure remote access since the VPN

Zscaler is a leader in securing Internet traffic for enterprises around the globe, with a cloud-based security platform designed to protect enterprise Internet traffic with Secure Web Gateway, Cloud Application Visibility and Control, Cloud Sandboxing, Data Loss Prevention, and more. Zscaler Private Access builds from the same cloud-based, elastically scalable infrastructure to deliver seamless connectivity to private internal applications and assets.



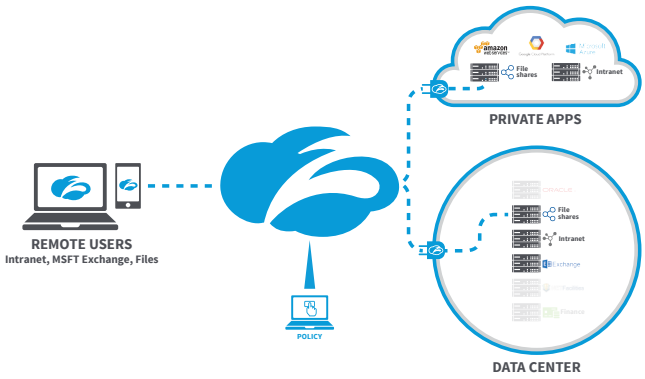
Zscaler App

Zscaler Private Access solves the challenges posed by a traditional VPN infrastructure by decoupling your internal assets and applications from the limitations, cost, and complexity of direct IP network connections.

Zscaler Private Access delivers seamless connectivity to private internal applications and assets whether they are in the cloud, the data center, or both. Policy-driven access adjusts dynamically to network changes, enabling enterprise agility while improving user experience.

With Zscaler Private Access, there is no need to provision VPN termination hardware, or to ensure that such a deployment is globally distributed and redundant. Users no longer need to go through a termination appliance in the data center to get to apps in the cloud. In fact, there is no hardware to buy at all, because Zscaler Private Access, like our Cloud Security Platform, functions as a service.

Zscaler maintains all hardware and software, freeing both your IT team and your budget even as we reduce latency and boost scalability. Zscaler Private Access is tied directly to your existing authentication infrastructure, leveraging single sign-on to further reduce complexity. The result is that unlike traditional, network-based remote access solutions, Zscaler Private Access can be deployed in a matter of hours instead of taking weeks or months.



Users are automatically routed to the best performing app.

Improve your security posture even as you provide seamless access

The reductions in overall cost and complexity are compelling on their own, but the paramount feature of the Zscaler Private Access solution is security. Once a connection is established between the asset and the client, the traffic traversing the solution remains completely isolated; because Zscaler Private Access is built on the premise of zero trust for your private applications, the traffic is isolated from us, as well. And because Zscaler Private Access abstracts the asset from the network, it not only ensures seamless access regardless of physical location, it dramatically increases your overall security posture by effectively making your most sensitive material invisible. Any attempt to route back to the application/asset meets a dead end.

Connect by application, not by IP address

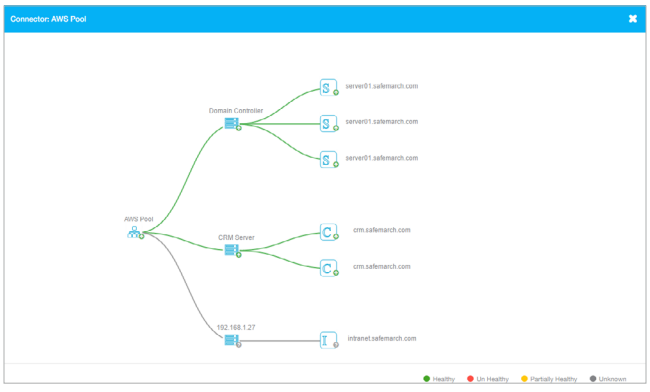
VPNs have been designed to deliver access to a network, not to an application. Once on a network, malware can propagate and users may be able to get access to adjacent applications from which they should be restricted. In addition, because VPN concentrators must listen for inbound connection attempts, they present an attack surface which may be exploited by such things as Distributed Denial of Service attacks.

Eliminate the cost of VPNs and associated equipment

As part of our global, cloud-based security platform, Zscaler maintains all hardware and software, which frees both your IT staff and your budget and enables deployment in a matter of hours. Even better, Zscaler Private Access is deployed via the same Zscaler App you use to access our cloud security platform, which greatly reduces your "client sprawl" by delivering a single app that provisions Zscaler Remote Access, Secure Web Gateway, Data Loss Prevention, Cloud Sandboxing, Cloud Firewall, and more.

Take your applications from "on-net" to "dark-net," at the same time YOU get complete visibility

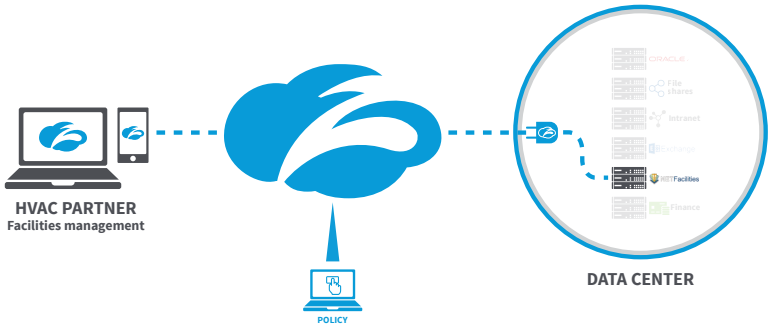
Zscaler Private Access renders your applications invisible to all but authorized users, and unroutable to anyone. But because the solution works at the application layer, we also deliver a level of visibility to you that has never before been possible. Once you provision a Connector in front of a bank of assets, you can use a wildcard attribute to discover exactly what applications are actually running there. Some customers have found almost ten times as many applications in use as they had expected! And once you know what applications are running, you can easily create granular access rules for them.



App Discovery makes deployment easy

Give contractors, partners, or other companies exactly the access they should have

Providing internal application access to third parties has always been risky—as proven by several recent security breaches. With Zscaler Private Access, there is no need to worry. You can provision granular application access without opening up your entire network to anyone. Now contractors can see the single app that they require and nothing else. In the case of a merger or acquisition, you can provision app access without worrying about overlapping private IP space, complicated NAT rules, or endless access control lists.



Extend application-specific access to contractors or partners.

The Zscaler Cloud Security Platform has long been declared a market leader by analysts like Gartner and Forrester in protecting enterprises' web traffic. Zscaler Private Access extends our platform's capabilities to enable simple, secure access to your vitally important private enterprise applications as well. Because Zscaler Private Access decouples the network and the application, the application IP address(es) become irrelevant, whether the asset is housed in a physical data center, a cloud data center, or any combination of locations.

FEATURE	PROFESSIONAL	BUSINESS	ENTERPRISE
Global visibility for users and application — Single pane of glass shows which users are accessing private, internal apps	✓	✓	✓
Secure Private Application access — Access to unlimited private internal applications (whether public/private/hybrid cloud or legacy datacenters) without exposing the network to users or applications to the Internet	✓	✓	✓
App and server discovery — Wildcard policy shows application and server locations as they are requested by users	✓	✓	✓
Enterprise DarkNet with DDoS protection for applications — Applications are only visible to users that are authorized to connect to them	✓	✓	✓
Single console for policy definition and management — All policy for global deployment via a single pane of glass	✓	✓	✓
Passive health monitoring — Application health is monitored when access is requested	✓	✓	✓
Zscaler App — Lightweight application used to provide access to Zscaler Internet Access and Zscaler Private Access	✓	✓	✓
Microsegmentation by application (up to 5 defined applications) — Granular access control by user or group for up to five specific application definitions, each of which may contain multiple hosts and/or ports.	✓		
Microsegmentation by application (up to 10,000 defined applications) — Granular access control by user or group for up to 10,000 specific application definitions, each of which may contain multiple hosts and/or ports.		✓	✓
Continuous health monitoring — Application health is continuously monitored to ensure that ports are available and users can connect to the app		✓	✓
Device posture enforcement — Checks device fingerprint and certificate, as well as other postures		✓	✓
Customer-provided PKI — Customer-provided certificates ensure complete privacy			✓
Double encryption — Provides encryption to microtunnel using customer's PKI			✓
Real-time user transaction view — Instantaneous logs for end-user support			✓

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/groups/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com