Transient

# PRODUCT DATA SHEET

TransientAccess 2.x

# TransientAccess – Zero-Trust Network Access (ZTNA)

## BENEFITS

**Software Defined Perimeter (SDP) Architecture:**

- **Stealth and transient access** to business-critical apps and resources using app-based networks. Apps and resources are never exposed to the Internet
- **Zero-Trust** application-level connectivity between authenticated users and apps
- **Private** and end-to-end DTLS encrypted data traffic belongs to the customer and does not pass through 3rd party cloud gateways

**App Segmentation and Full Visibility**

- Fine grained application access policies allow segmentation of apps, not networks thereby mitigating the risk of lateral movement
- Full audit trail of users activities are available real-time

  Mobile data protection e.g. transparent data-at-rest encryption enables data leak prevention even on unmanaged devices, without an MDM or MAM solution

**Frictionless Implementation**

- Integrates easily into existing security configuration of enterprises **and requires no ACL or inbound firewall rule changes**
- Supports on-prem or SaaS based deployment models and integrates with existing automation tools through REST APIs

**The New Perimeter: Applications**

Traditional perimeter-based architectures were suitable in the days when servers were hosting enterprise apps inside a corporate data center, accessed by corporate users, using corporate issued devices. Fixed device-centric networks made it easy to define what "outside" is and secure "inside".

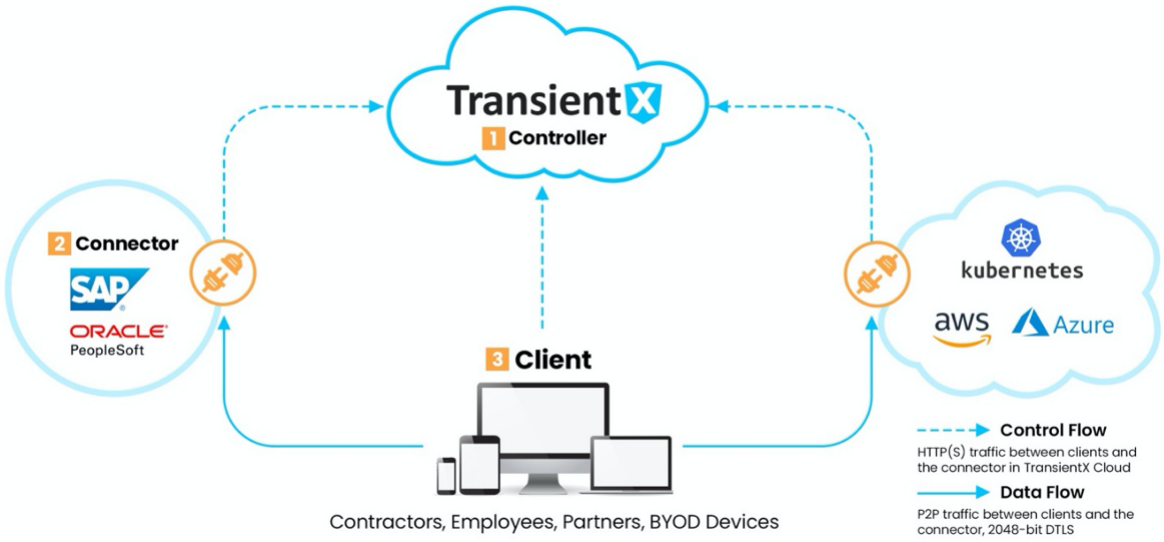
Enterprises today have distributed data centers. Applications are deployed on-premises or in a public cloud, accessed by SaaS apps, IOT devices, B2B partners, contractors, affiliates, remote workers, BYOD devices...

Increasing numbers of unmanaged devices accessing enterprise apps forced IT teams to utilize legacy technologies like VPNs despite the related management complexities and vulnerabilities. In this new world, traditional security and access models - network centric perimeters, VLANs, MPLS lines, NACs, VPNs or other all-or-nothing solutions - fail to keep up with the agility and speed requirements of a modern enterprise.

Today's dynamic business environments require a new paradigm that moves past old perimeter-based approaches and embraces the new software-defined perimeter for corporate applications, hosted anywhere, accessed from anywhere.

**TransientX's application networking technology builds a secure perimeter around enterprise applications and authenticated users.**

TransientAccess provides secure remote access to internal applications deployed in corporate networks, private clouds or data centers. It allows IT teams to build highly granular access policies and connects authorized users with resources without exposing them to the Internet. This zero-trust system avoids management complexities and does not extend corporate networks to users like legacy VPNs do. Instead, it ensures that authenticated users and enterprises apps are connected in a cloaked ephemeral network, invisible to attackers.




## KEY SCENARIOS

### Secure 3rd Party User Access and BYOD

Today's dynamic business environments require supporting a mobile workforce and business partners alike with access to enterprise resources. TransientAccess provides zero-trust access to these resources without providing network access or Internet exposure. No MDM or MAM is required.

### Secure XaaS Access

IT teams need a simple way for allowing access to applications hosted in public clouds like Azure and AWS, without management and setup complexities of existing tools. With TransientAccess, DevOps teams can access production workloads hosted in these environments using their favorite tools such as RDP or SSH anywhere in the world, securely.

### Secure Access to SCADA Systems

Enterprises with critical infrastructure have unique security and compliance challenges for governing access to SCADA systems. When contractors or employees need to access such systems in various sites such as power plants in different cities, they are often need to travel. TransientAccess provides a secure and compliant alternative, in that such systems can be accessed by authorized users, without exposing them to the internet through virtually air-gapped app networks.

### How it Works

TransientAccess has 3 components involved:

- **1. Controller:** The component which authenticates and authorizes users and orchestrates connections. This is normally deployed in the TransientX cloud as a service (SaaS).
- **2. Connector:** Connectors are deployed in front of applications which will be accessed, usually in a private cloud or on-prem data center.
- **3. Clients:** Users install TransientAccess clients on their devices in order to access enterprise resources.

When an authenticated user requests access to a remote resource, a temporary network of apps on users' device and the resource (e.g. enterprise apps, servers) is created, as needed.

With this patent-pending app networking technology, users can access only the apps and resources they are authorized, through a temporary application-based network.

Connectors are never exposed to the Internet, have no incoming connections and are deployed behind firewalls and other existing security components. A peer-to-peer tunnel is established between the user's application and the connector in the corporate network, with no data passing through 3rd party cloud gateways. The end-to-end traffic is based on DTLS protocol with 2048-bit keys.

TransientAccess couples zero-trust architecture with granular access control policies, application segmentation and full visibility into applications' and users' activities.

# Components and Technical Requirements

## CLIENTS

TransientAccess users run a lightweight application on their devices.

These clients are publicly available for downloading or IT teams can distribute them using their own distribution channels.

GET IT ON Google Play

Download on the App Store

Azure

## CONNECTOR

Connectors enable inside-out connectivity and peer-to-peer transient tunnels with clients outside the network.

It is available in multiple form factors for seamless deployment in any environment.

Download on the App Store

Azure

## TransientAccess Client

Connects ***apps to apps and resources in the enterprise network*** in order to provide a seamless user experience and broader application support.

| Supported Platforms | Major Features |
|---|---|
| • IOS 7.0 or later<br>• Android 5.0 or later<br>• Windows 7 or later<br>• Mac OSX 10.10 or later | • Zero Trust Network Access - Builds a peer-to-peer DTLS tunnel with connectors using 2048-bit keys<br>• Device Security Posture – Enforces a device's security state before allowing connections for: rooted or jailbroken devices, VMs, anti-debugging, anti-cracking protection<br>• Portable: No admin or root rights are required |

## TransientAccess Connector

Connects ***and bridges applications and resources in the enterprise network*** with users using TransientAccess clients.

| Deployment | Capacity Calculation |
|---|---|
| • Linux Virtual Appliance<br>• Azure or AWS Appliance<br>• Docker Container<br>• Package for Windows Server 2008 or later | Capacity requirements rely heavily on operational scenarios. The following is a guideline for calculating a general-purpose application access scenario:<br><br>For 10 connectors, a server with:<br>• CPU: 4 Core/vCore<br>• Memory: 8 GB<br>can be used to handle 1000-5000 concurrent connections. |