Use Case

Transform Your Remote Access Solution

Challenge

Strategy implementation

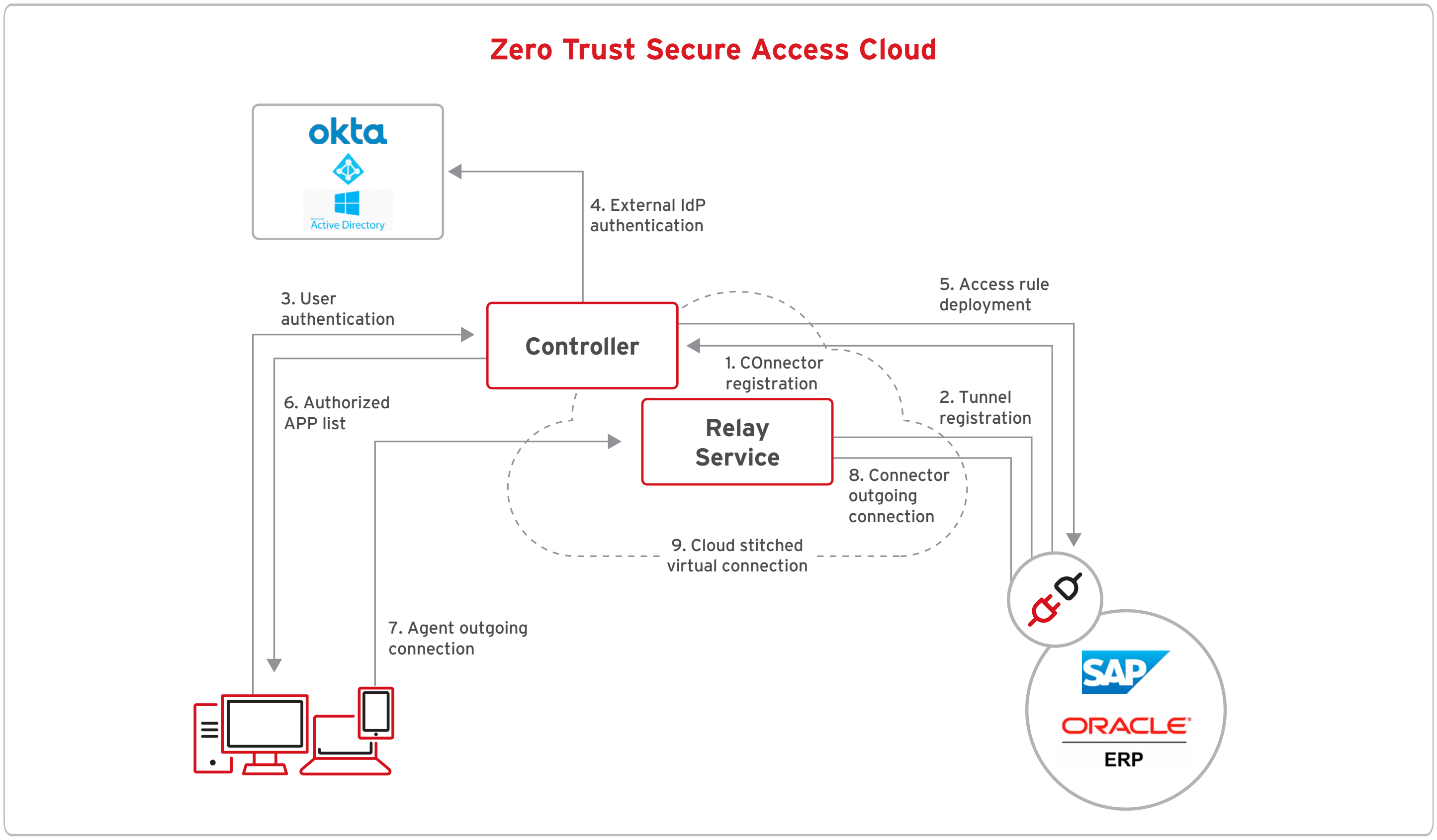
Organizational cybersecurity is a complicated task when viewed from the strategy level. Equally so is the day-to-day administration. As organizations look at new models of security, such as zero trust, it's easy for both strategic and tactical staff to be overwhelmed with the first steps.

A large-scale transformation to an organization's security operations can't be completed overnight. Trend Micro's view is to begin with a solution path for an achievable problem directly at hand. This allows operations teams to move beyond this first issue, meaningfully increasing security along the way through subsequent problems towards overall security goals.

The problem in front of the administrator

"How can I provide secure and scalable access to apps and resources for my remote and hybrid workforce?"

For years, organizations relied on VPNs for remote access of on-premises resources, either as a part of a firewall or as a standalone appliance. As employees began to migrate away from the office, expanding organizations' digital attack surfaces, many remote networks lack the same on-premises security features.


Zero Trust Secure Access Cloud
okta
Active Directory
4. External IdP authentication
3. User authentication
Controller
5. Access rule deployment
1. COnnector registration
6. Authorized APP list
Relay Service
2. Tunnel registration
8. Connector outgoing connection
9. Cloud stitched virtual connection
7. Agent outgoing connection
SAP
ORACLE
ERP

Capability

Bridging disparate technologies

Trend Micro™ Zero Trust Secure Access aims to deliver centralized control and unified visibility to several previously disconnected technologies. Trend Micro™ Zero Trust Secure Access – Private Access provides the capabilities of zero trust network access (ZTNA) gateways. In addition to delivering a trusted augmentation or alternative to VPN, this technology's wider ecosystem provides additional data. This allows for risk-based access decision making, rich telemetry, and reporting visible, along with simple and consistent policy control.

Moving beyond the boundaries

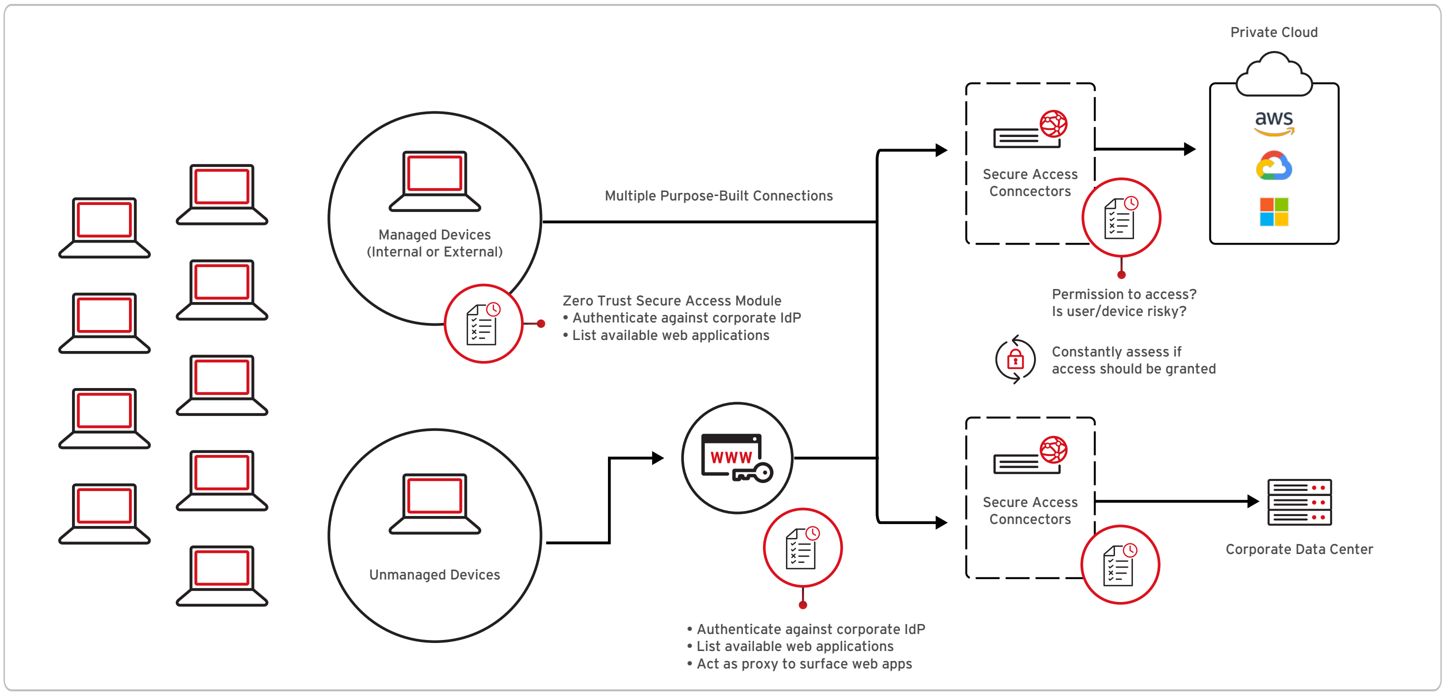
As organizations move forward in their digital transformation journey, many will retain on-premises apps and resources, while hosting others in private clouds. For organizations utilizing hybrid and remote workforces, it is vital to access these apps and resources in a fast, scalable, and secure way.

Performance: Private Access is offered in several formats, as a Trend-hosted platform, self-hosted in a private cloud, or self-hosted on-premises. This allows administrators to choose how they can access apps and resources. Cloud-based apps can connect without routing on-premises and employees don't have to deal with performance issues stemming from overloaded VPN terminators.

Scalability and accessibility: Private Access delivers specific access across private clouds and on-premises data centers following an elastic format. In the cloud, new gateways are automatically deployed and load- balanced as required to provide access. On-premises access is supported by self-hosted gateways that can be deployed in advance of expected demand. Trend Vision One™ delivers a cloud-stitched dedicated connection that balances across deployed gateways.

Secure access: A limitation of VPN deployments is the wide network access that is given to organizations' endpoints. This extends the corporate network to the untrusted and vulnerable home network of the user. Private Access mitigates these risks by providing access only to specific apps and resources through a gateway. This disconnects the home and corporate networks, only allowing traffic to pass if identity, authorization, and device posture meets policy. In addition, continuous risk assessments revoke access in real- time to stop threats from entering the network.

Agent and agentless coverage: Whether it's not feasible to install an agent on each endpoint, you're not equipped to run an agent, or you've deployed an agent from a third party, corporate and security policy must be applied no matter the agent status of your endpoints. Private Access provides an authentication portal for agentless endpoint access requests. This delivers strong identity and continuous risk assessment security no matter the asset status.


Private Cloud
aws
Secure Access Conncectors
Multiple Purpose-Built Connections
Managed Devices (Internal or External)
Zero Trust Secure Access Module
• Authenticate against corporate IdP
• List available web applications
Permission to access?
Is user/device risky?
Constantly assess if access should be granted
WWW
Secure Access Conncectors
Corporate Data Center
Unmanaged Devices
• Authenticate against corporate IdP
• List available web applications
• Act as proxy to surface web apps

Implementation

How Internet Access provides protection

Private Access works with your existing identity provider (IdP) to leverage single source multi-factor authentication.

A complete picture of the requesting user is built with hardware and OS identifiers, file system information, certificate data, and geolocation for endpoints and applications. Private Access enables access to apps hosted in cloud providers like AWS or Microsoft Azure using a service-initiated zero trust network access (ZTNA) gateway. This uses inside-out connections to make apps invisible to the internet, allowing organizations to mitigate attacks without limiting legitimate use.

Private Access enables adaptive, context-aware access to private apps from any location and device. The context for app access includes identity, device type, user location, and device security posture. Granular security controls can be implemented to prevent data exfiltration. This is done by regulating user operations delivering a least-privilege access solution.

End users can access an on-premises or private app following this process:

1. **Users authenticate with IdP using their existing SAML SSO credentials**
2. **The device posture is verified by Private Access, and checked continuously during the signed-in session**
3. **The controller gives the authorized application list to the Private Access endpoint module**
4. **An outbound connection from the Private Access endpoint module to the relay service is created**
5. **An additional outbound connection from gateway connector to relay service is created, these two connections are then stitched together to establish a secure connection between the user's device and connector**

Next Steps

A free trial of Zero Trust Secure Access – Internet Access is available through the Trend Vision One platform. Leverage **Trend Micro™ Attack Surface Risk Management** or contact your account team for more information.

Begin securing access to the internet immediately by signing up for a **free 30-day trial of Trend Vision One**.

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy