TREND MICRO™

Deliver Fast and Secure Access to Cloud Apps

Challenge

Strategy implementation

Organizational cybersecurity is a complicated task when viewed from the strategy level. Equally so is the day-to-day administration. As your organization looks 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 your 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 your operations team 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 fast and secure access to cloud apps, while returning visibility and control?"

It has become more commonplace to find organizations relying on public cloud apps to power their business. This includes Microsoft 365, Google Workspace™, Salesforce, and SAP. As more of your business functions are moved to these public apps, visibility and control of access range from "challenging" to "non-existent". This increases risk to your data being processed within.
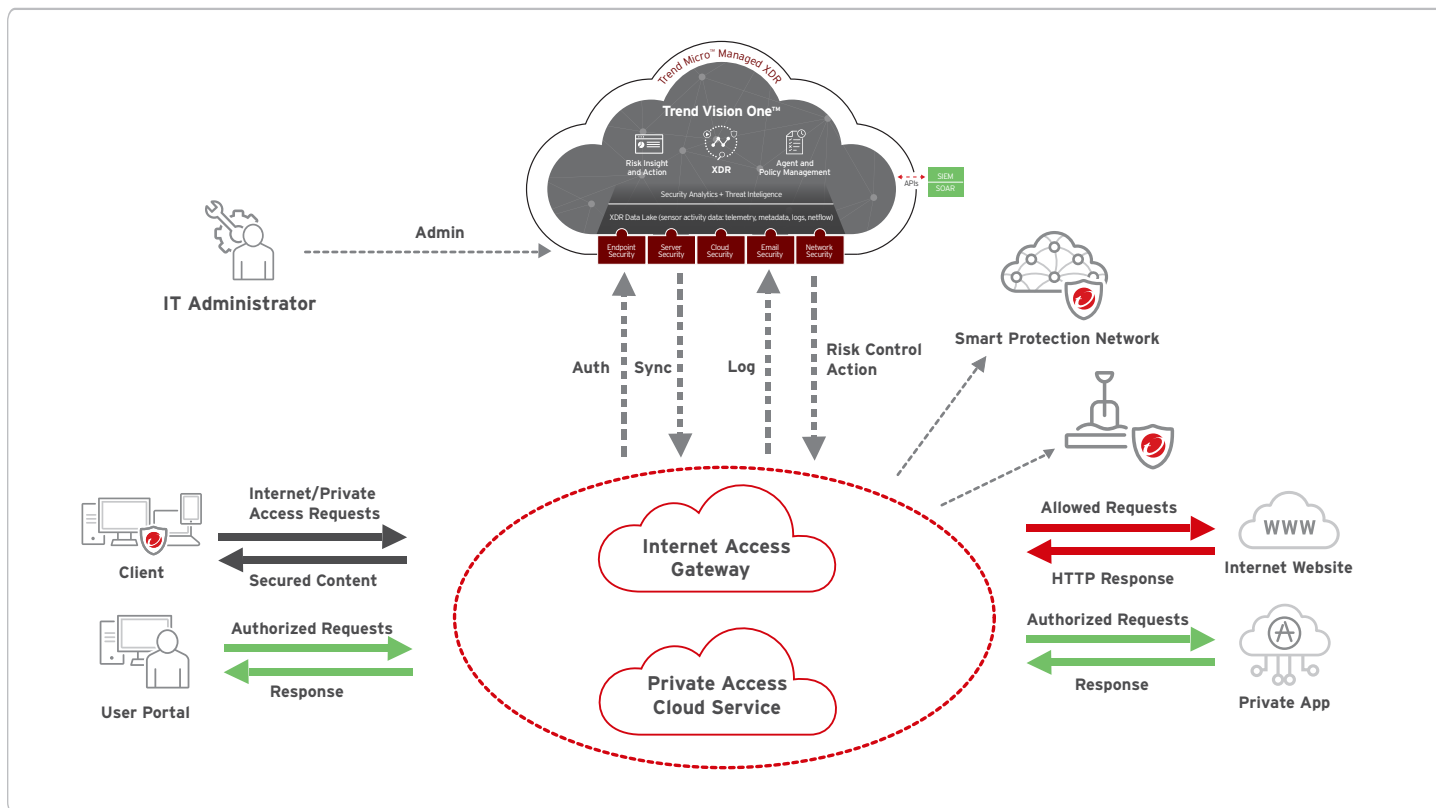
Bridging disparate technologies

Trend Micro™ Zero Trust Secure Access delivers centralized control and unified visibility to several previously disconnected technologies. Trend Micro™ Zero Trust Secure Access – Internet Access brings the capabilities of a powerful secure web gateway (SWG) and cloud app activity sensors together. Leveraging this proven technology through the lens of Trend Vision One™ delivers SWG and cloud access security broker- (CASB) style capabilities. In addition, the wider ecosystem provides supplementary data. This allows for automated access decision making, rich telemetry, and reporting visible, along with simple and consistent policy control.

Moving beyond the boundaries

As your organization moves forward in your digital transformation journey, visibility and control of software as a service (SaaS) apps can be left behind. This leads to the expansion of your organization's cyber risk surface, often resulting in issues like unauthorized access and loss of data. In addition, performance concerns arise as the possibility for business slowing down in the name of security enhancements increases.

- **Data and access control:** Internet Access manages entry to public SaaS apps through SWG technology. This applies continuous risk assessments for each connection, only permitting access to those authorized within set and dynamic policies. Cloud access security broker- (CASB) style techniques are also applied to provide data loss control, ensure privacy, and data access policy conformance.
- **Performance, uptime, and availability:** Internet Access provides you with options on how and where gateways are deployed. The leading deployment option includes Trend hosted gateways within the public cloud. Accessibility is managed by the cloud service provider (CSP) while you are connected to the nearest point of presence (PoP). Trend hosted gateways are elastic, so despite how much traffic is flowing, performance and availability won't be restricted.
- **Agent and agentless coverage:** Although it's not feasible to install an agent on each endpoint, you may be equipped to run an agent, or you've deployed an agent from a third party. In these cases, corporate and security policy must be applied no matter the agent status of your endpoints. Internet Access provides coverage to secure internet access, protecting gaps in coverage from exploitation.
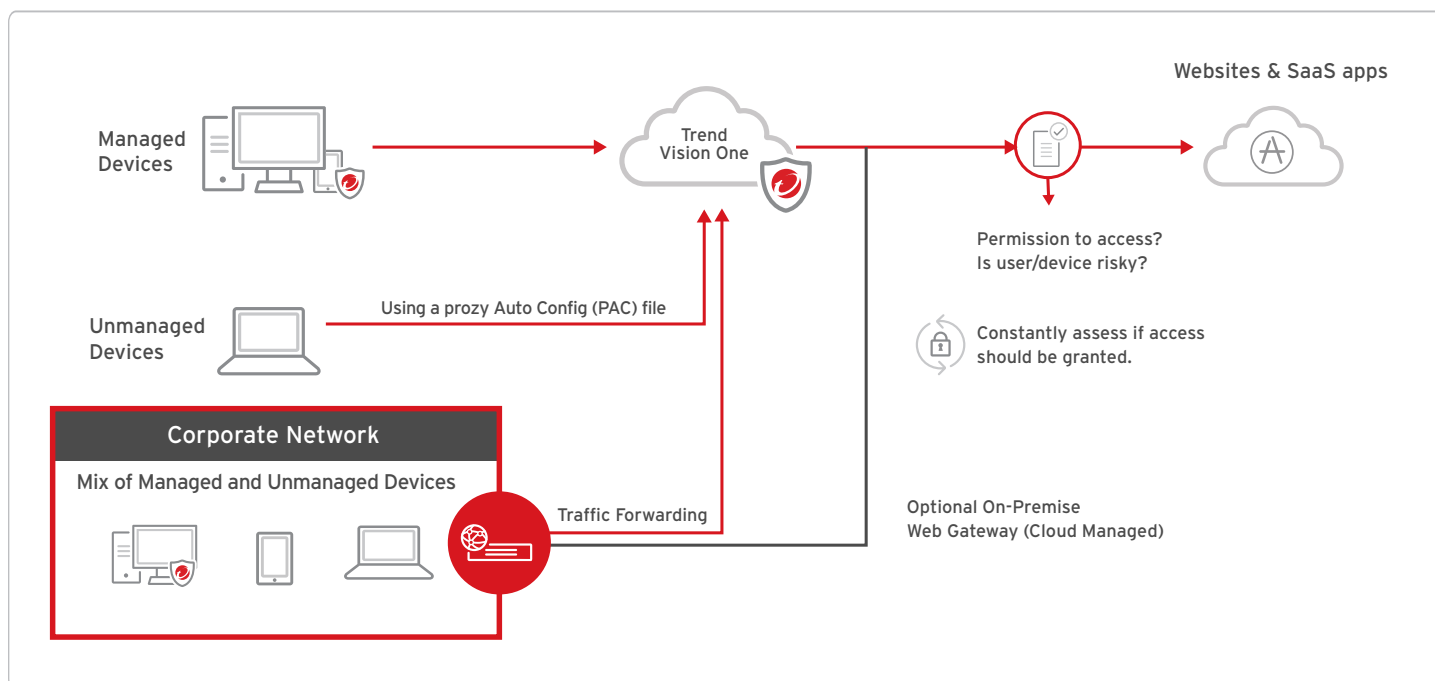
Implementation

How Internet Access provides protection

Internet Access operates as a cloud-based security gateway, filtering web and internet traffic at the application level. Using a cloud-based solution gives you the same advanced protection and policy enforcement inside or outside your network perimeter. Your organization can set up a connection with an Internet Protocol Security (IPsec) tunnel to the closest supported data center. Or you can forward user traffic via a lightweight Client Connector or a proxy auto-config (PAC) file. Internet Access sits between your end users and the internet, inspecting traffic inline across multiple security techniques, including TLS/SSL.

Your end users access a website following this process:

1. **Authenticate with an identity provider (IdP) using existing SAML SSO credentials**
2. **User or user groups gateways/locations are verified by Access Gateway**
3. **Access is granted if control has been configured to be allowed or monitored in a rule. If a rule has been configured to block the URL or cloud app, the action will be blocked. Access Gateway will apply further threat protection or data loss prevention (DLP) profiles on traffic if configured**
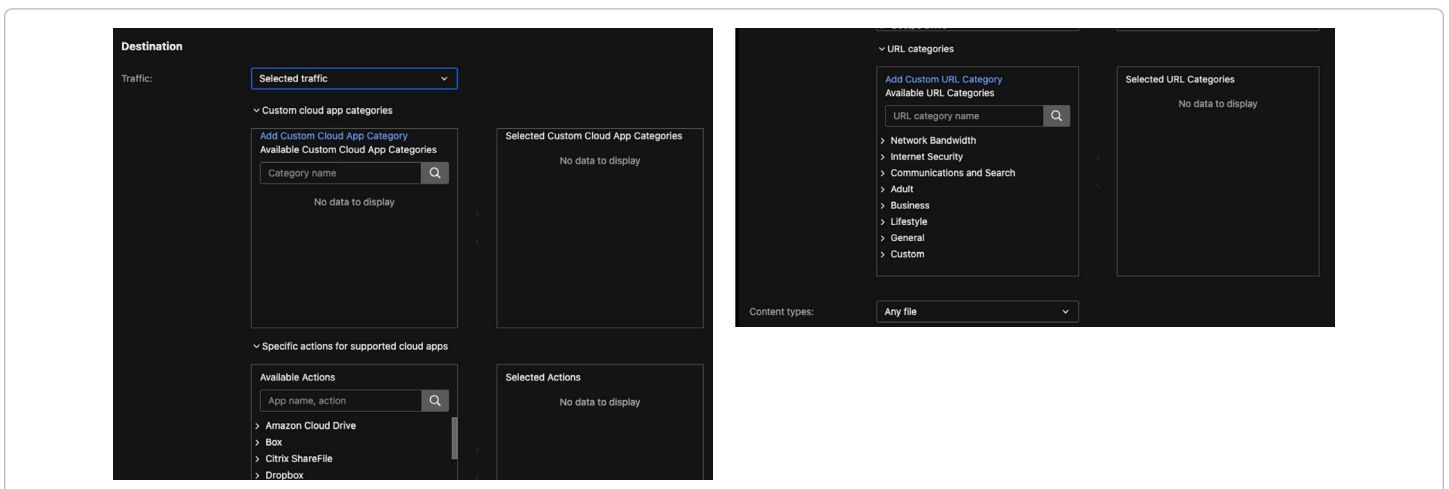
Simple Setup

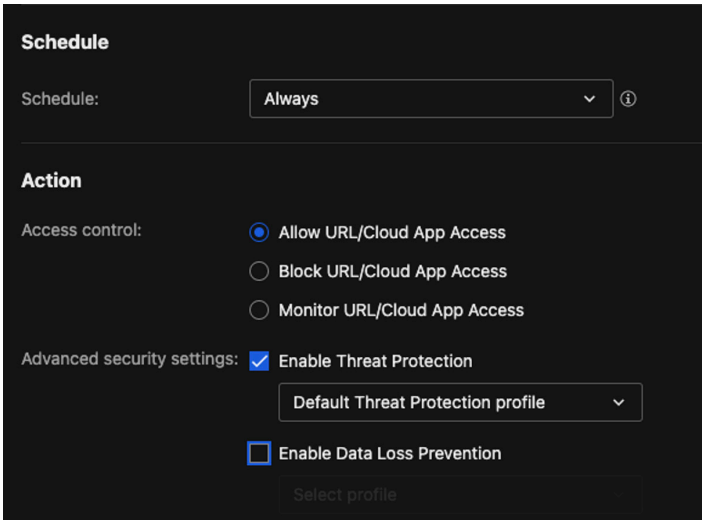The setup for allowing or restricting sites requires only a few steps to add or remove access:

1. Select user groups and/or locations
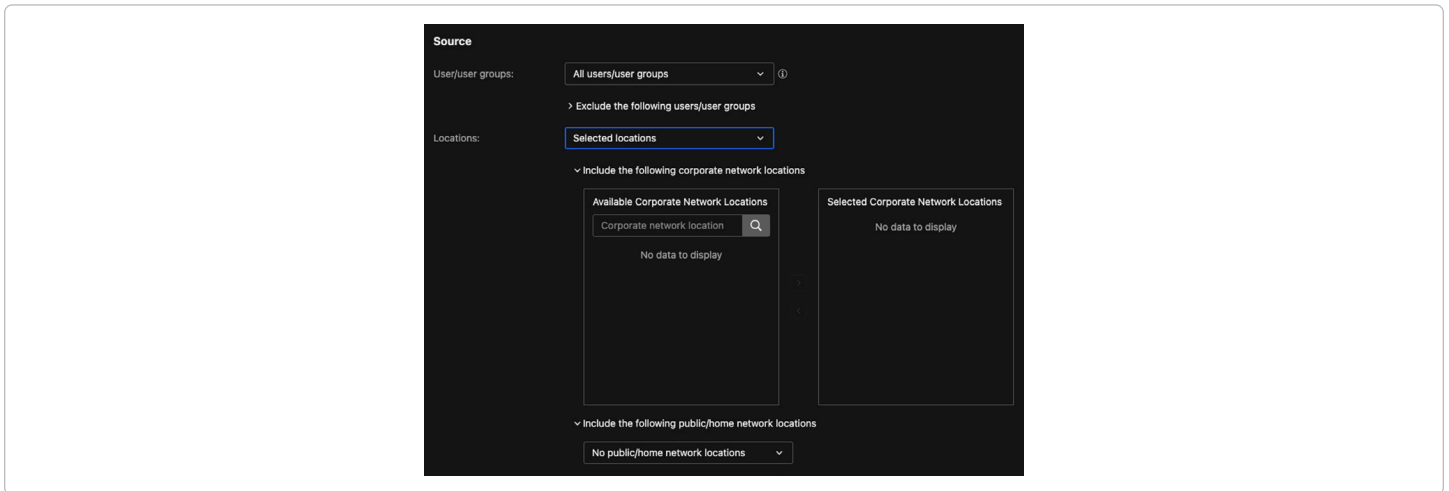
2. Select "traffic" or "content" type, which are designed to identify destination of traffic

2. Select "traffic" or "content" type, which are designed to identify destination of traffic

Next Steps

A free trial of Zero Trust Secure Access – Internet Access is available through Trend Vision One. Leverage our **Trend Micro Zero Trust Risk Insights** 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**.