SECURE YOUR ACCESS TO THE INTERNET

CHALLENGE

Strategy implementation

Organizational cybersecurity is a complicated task when viewed from the strategy level. Equally so is the day-to-day administration and affecting of the strategy. 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 apply corporate policy and secure access to the internet for all users”

A majority of organizations share the same concern: setting guard rails for corporate policy (restricting NSFW sites) and providing security protection to block threats without negatively impacting device performance and productivity. This is often solved using secure web gateway (SWG) solutions, often running independently of other products in the security tool stack.
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 – Internet Access provides the capabilities of a powerful SWG. By leveraging this proven technology through the lens of Trend Micro Vision One™, not only are the SWG capabilities present, but the wider ecosystem provides additional data. This allows for automated access decision making, rich telemetry, and reporting visible, along with simple and consistent policy control.

Moving beyond the boundaries

Along with existing solutions to the internet access control problem are limitations that often undermine the solution. These range from performance issues, false-positive blocking, uptime, and availability to agent and agentless coverage. Internet Access takes aim at these challenges and breaks down the boundaries that have traditionally restricted the overall effectiveness of an SWG.

Performance, uptime, and availability: Internet Access provides customers with options on how and where gateways are deployed. The leading deployment option includes Trend Micro hosted gateways within the public cloud. Accessibility is managed by the cloud service provider (CSP) while customers are connected to the nearest point of presence (PoP). Trend Micro-hosted gateways are elastic, so despite how much traffic is flowing, performance and availability won’t be restricted.

Security accuracy: Trend Micro leverages internal research teams to deliver global threat intelligence. This is implemented via several systems, including the Web Reputation Service (WRS) to provide up-to-the-minute data on website category and risk. This service collects data from billions of endpoints deployed worldwide and limits the potential impact of accessing a dangerous website—without blocking normal web activity.

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. 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 users the same advanced protection and policy enforcement inside or outside their network perimeter. Organizations can set up a connection with an Internet Protocol Security (IPsec) tunnel to the closest supported data center, or forward user traffic via a lightweight Client Connector or a proxy auto-config (PAC) file. Internet Access sits between the end users and the internet, inspecting traffic inline across multiple security techniques, including TLS/SSL.

End users access a website following this process:

1. Users authenticate with an identity provider (IdP) using their 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 or group
2. Select a URL or category
3. Specify the schedule and action

NEXT STEPS

A free trial of Zero Trust Secure Access – Internet Access is available through the Trend Micro Vision One solution. 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 60-day trial of Trend Micro Vision One.