Trustgrid Remote Access

Quick, Secure, Agentless Access to Applications

Trustgrid’s Remote Access is the easiest way to deliver Zero Trust network access to any application or device. It allows users to connect to private applications (hosted in the cloud or data center) from any location, without requiring expensive proprietary hardware and weeks of configuration.

This modern approach to user access changes the way that remote users connect to enterprise applications. Instead of creating tunnels to a corporate network and allowing all traffic and users to pass through, Trustgrid Remote Access instead uses an agentless approach that creates a software-defined perimeter around the user and application. These connections allow for every session to be established, secured and monitored without the use of device agents.

Once deployed, users connect to applications through a personalized web portal that authenticates and authorizes sessions based on a user’s identity and location. Deployments can be done in minutes and complex configurations are virtually eliminated.

As a cloud-delivered service, networking teams are able to easily deploy and manage secure access at scale.

How It Works

Trustgrid Remote Access is enabled by a distributed network of nodes. These nodes can be placed in front of cloud or data center applications to provide direct identity-authenticated connectivity between applications and end users.

Simplified Management

The Trustgrid management portal acts as the Identity Broker for all access. It gives administrators the ability to manage user identities, groups and access policies, and can be synced with a 3rd party identity provider to leverage existing identity repositories.

From the portal, applications can be quickly added by deploying a Trustgrid Node into an application environment. Once deployed, the portal manages node configurations and has the ability to set granular access controls according to users, groups, and locations.

These nodes can be deployed with minimal firewall changes for simple plug-and-play installation. Once installed, these network nodes establish a fabric of application connectivity who’s access is governed by the management portal.

From the management portal user sessions can be monitored in real-time, logged or have their metadata streamed to a 3rd party security solution. Should a threat or anomaly be detected, sessions can be manually terminated via the portal or triggered to automatically disconnect via the API controls built into each node. Access logs are easily accessible from the portal and create a single source of truth for reporting and compliance purposes.

Seamless User Experience

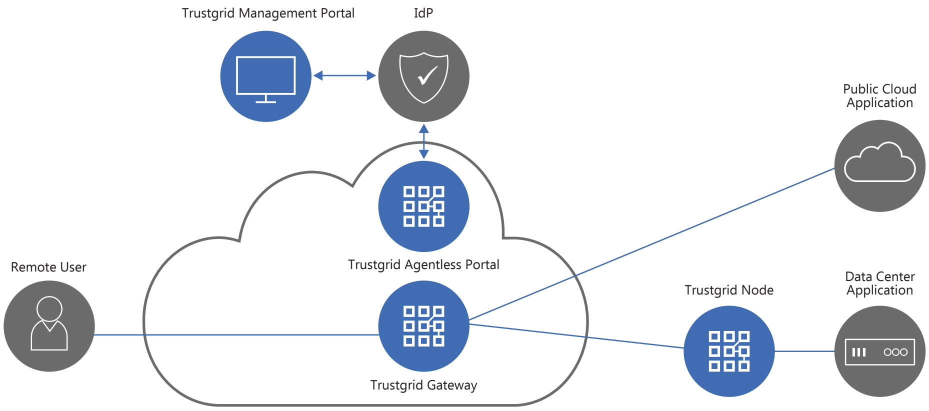
Users attempting to access an application, log in through the Trustgrid Remote Access web portal. Authentication is handled via a captive portal from an identity provider (IdP).

Once credentials are authenticated, the portal exposes authorized applications to the user. The Trustgrid Identity Broker manages the transaction between the IdP and the Trustgrid portal to ensure that access policies are properly applied to all sessions.

Identity-specific access policies dictate what applications are exposed to the user and what they are able to access within that application. Applications are hidden from the public internet, preventing malicious actors from discovering potential attack vectors and are only exposed (via a virtual network) to authorized users.

The user portal is accessed via web browser to ensure access across a wide variety of desktop and mobile devices.

Agentless Remote Access Architecture



Compatibility

Supported Application Environments	▪ **Public Cloud** ▪ **Private Cloud** ▪ **Data Center** ▪ **SaaS**
Supported Public Cloud Providers	▪ **AWS** ▪ **Azure** ▪ **Google** ▪ **Oracle**
Supported Identity Solutions	▪ **Azure** ▪ **AD** ▪ **Okta** ▪ **Google**

Features

- Secure application access without device agents
- Policy-based network segmentation
- SOC 2 Type II compliant connectivity
- Single access interface for all applications
- Centralized visibility and logging of access
- Single-tenant and multi-tenant data plane available
- Granular policy definition
- Mutual TLS encryption of all application traffic
- Cloud-like user and administrator experience
- Easily integrates with cloud security solutions

888.308.8995
info@trustgrid.io

For More Information Visit **www.trustgrid.io**