

# Secure Enterprise Connectivity

## Trustgrid enables secure connectivity to data with integrated compliance.

Trustgrid delivers a cloud-native SD-WAN to enable highly available and secure connectivity between public and private cloud applications and on-premises environments. That’s why fintech, health tech, retail, and other companies in highly regulated industries choose Trustgrid for their cloud-to-edge networks.

### Protect Your Enterprise Data

Trustgrid integrates state-of-the-art security with software-defined networking to deliver an industry-leading security posture. The Zero Trust model ensures policies and trust are enforced throughout the network environment and leverages an implicit denial on all traffic until authorized. By removing all pre-shared keys (PSKs) from the network and using certificate-based authentication, Trustgrid eliminates many possible attack vectors.

Date	IP	Event	Details	User Name	Item Type
2024-03-29 08:00	64.17.3.164	change	Node (uid=fac3db88-adc0-422b-8b79-964bdd4a6812, fqdn=aws-gw1.demo.trustgrid.io) changed config.snmp.engineId1NifLt1CZjpMGY69k0vpBUN to vBVkLKPNU2bvO5BdVZWVdxKe	demo@trustgrid.io	node
2024-03-29 08:00	64.17.3.164	change	Node (uid=fac3db88-adc0-422b-8b79-964bdd4a6812, fqdn=aws-gw1.demo.trustgrid.io) changed config.snmp.port 14562 to 4877	demo@trustgrid.io	node
2024-03-28 08:00	64.17.3.164	change	Node (uid=fac3db88-adc0-422b-8b79-964bdd4a6812, fqdn=aws-gw1.demo.trustgrid.io) changed config.snmp.engineId pRVi2WQmOX43CNrPmpOeDQm3 to 1NifLt1CZjpMGY69k0vpBUN	demo@trustgrid.io	node

Figure 1 Configuration audit logs in Trustgrid portal.

Trustgrid encrypts all connections using TLS 1.2\* in place of traditional IPsec tunnels. This delivers a higher level of encryption and future-proofs the connection.

\*TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 cipher

## Simplify Your Compliance

Designed to meet the increasing needs of highly regulated institutions, Trustgrid offers native features designed to simplify your compliance and audit processes.

Trustgrid is audited annually for compliance with SOC 2 Type II standards which includes a full penetration test of all systems. Centralized logs capture network flow, all configuration or system access changes, and the installation of patches/updates.

The Trustgrid cloud management portal natively requires multi-factor authentication and can be restricted to specific IP ranges. Support for many common SSO providers (Okta, Azure AD, etc) is also provided.

## Trustgrid Secure Architecture

The security and privacy of your enterprise data are enhanced with Trustgrid’s application architecture. Trustgrid utilizes a centralized, multi-tenant suite of applications deployed in Amazon Web Services (AWS) for the management of all Trustgrid Nodes including configuration, security policy, and monitoring. This is called the Control Plane.

A separate single-tenant, distributed application handles all data transmission, called the Data Plane. The Data Plane is a point-to-point connection from your data centers directly to an application provider’s environment. The Data Plane is dedicated to each data center and is unable to connect to anything other than the application provider.

The separation of the Control Plane from Data Plane enables complete privacy and security of all data transmitted between the data centers and the application provider.

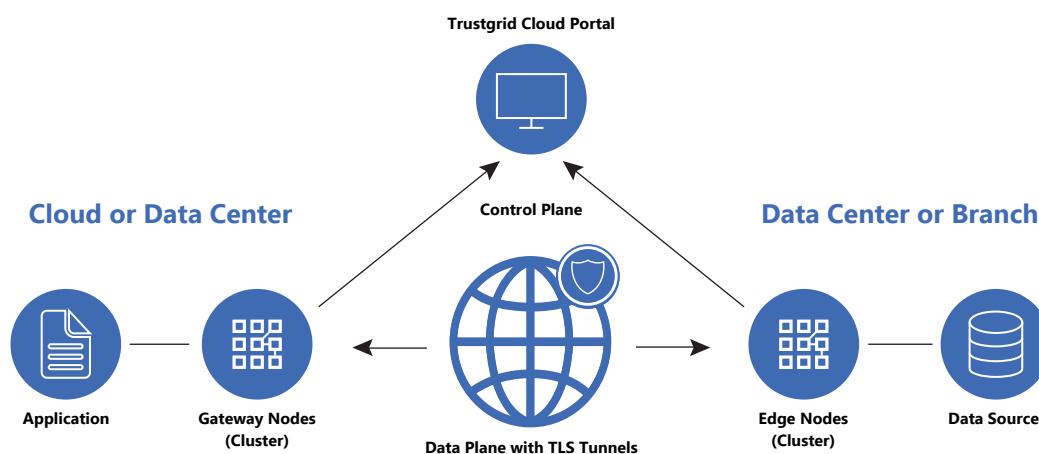


Figure 2 Trustgrid's application architecture

## Trustgrid Secure Operations

Trustgrid develops, deploys, and operates the software platform used for a data centers’ connectivity. Trustgrid provides Tier 2 and 3 support services as well as automated patches/updates. The SOC 2 Type II compliance audit ensures all necessary controls are in place to prevent access to data that is encrypted and transmitted in the Data Plane. These controls include role-based access controls for all support and development staff, no retention of any Data Plane traffic for any reason including testing, and a comprehensive IT Security Policy.

Trustgrid utilizes Amazon Web Services (AWS) for all Control Plane application functionality. AWS’ extensive security and compliance investments also protect access to critical Control Plane assets.