White Paper

trustgrid

Trustgrid enables and secures remote access to FI data with integrated compliance

Trustgrid delivers a cloud-native SD-WAN to enable highly available and secure connectivity between public and private cloud Fintech applications and the core banking systems that store secure data. Trustgrid is trusted by leading Fintech providers such as Apiture, eCU Technologies, and Q2eBanking.

More Protection for FI 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 deny 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.

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 as IPsec is deprecated by the Internet Engineering Task Force (IETF).

Configuration Changes

Export Config Changes

Search

Advanced Search | Clear Advanced Search

Date	IP	Event	Details	User Name
2019-08-07	12.244.52.246	change	Node (uid=8439d499-2fb9-4386-b5d2-1c8618d969a5, domain=demo,trustgrid.io, fqdn=aws-cluster-gw1.demo.trustgrid.io, name=aws-cluster-gw1, profile=aws-cluster.demo.trustgrid.io-1553631658010, state=ACTIVE) added config.alert={"enabled":false, "threshholds": [{"node": "edge1-cluster-1", "max": 150, "exceedWindow":30,	joe+demo@trustgrid.io
2019-08-07	12.244.52.246	change	Node (uid=8439d499-2fb9-4386-b5d2-1c8618d969a5, domain=demo,trustgrid.io, fqdn=aws-cluster-gw1.demo.trustgrid.io, name=aws-cluster-gw1, profile=aws-cluster.demo.trustgrid.io-1553631658010, state=ACTIVE) removed maintenance_schedule+{}	joe+demo@trustgrid.io

Showing Rows 1 to 2 of 2 10

Figure 1 Configuration audit logs in Trustgrid portal.

Learn more at www.trustgrid.io

Simplify Compliance for Banks and Credit Unions

Designed to meet the increasing needs of highly regulated institutions, Trustgrid offers native features designed to simplify compliance and audit for application providers and FIs. Trustgrid is audited annually for compliance with SOC 2 Type II standards which includes a full penetration test of all systems. Centralized logs capture netflow, all configuration or system access changes, patches/updates and are easily integrated into SIEM systems. 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 banking data is enhanced with Trustgrid's application architecture. Trustgrid utilizes a centralized, multi-tenant suite of applications deployed in Amazon Web Services (AWS) for 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 the financial institution data centers directly to the application provider's environment. The Data Plane is dedicated to each FI and is unable to connect to anything other than the application provider.

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

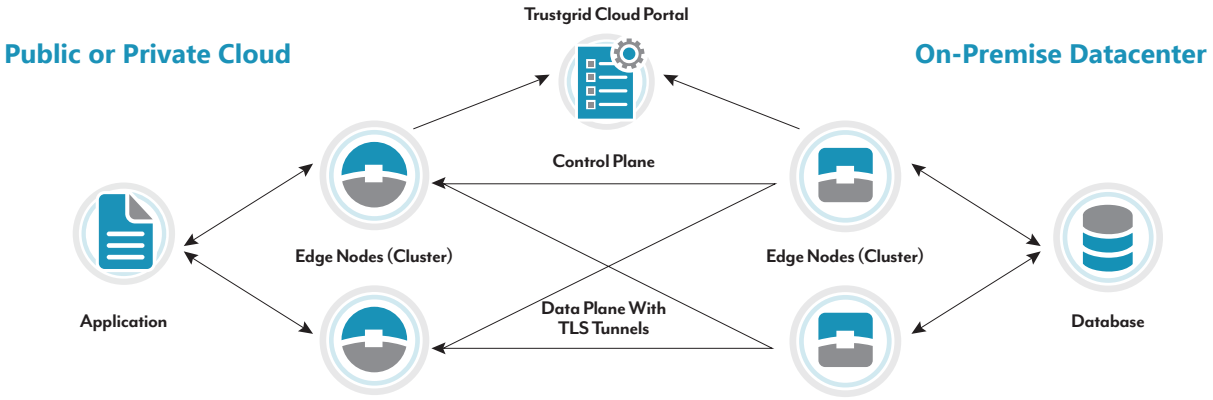

Figure 2 Trustgrid's application architecture

Trustgrid Secure Operations

Trustgrid develops, deploys and operates the software platform used for FI 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 FI 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.

888.308.8995
info@trustgrid.io

Learn more at www.trustgrid.io