trustgrid

# Network Management for Hybrid Environments

Network management within hybrid environments presents configuration and management challenges. Network engineers often juggle a complicated web of technologies, consultants and application vendor provided solutions in an attempt to maintain order.

Public cloud, multi-cloud, distributed data centers and varying data owners complicate the deployment of new, and management of existing, connections. These challenges multiply at scale and can become an inhibitor to growth, as well as a drain on IT budgets.

Trustgrid's software-defined networking solutions simplify the deployment, management and support of hybrid network environments and allow engineers to simplify their infrastructure while taking advantage of advanced functions unavailable in even the most robust VPN and SD-WAN solutions.

**Configuration |** Trustgrid's software-defined nodes are hardware agnostic and can be deployed on a number of commercial off the shelf (COTS) devices. These nodes reside near the end points of the connection and can be placed in front of, or behind, a firewall to simplify deployments of any resource in any environment, including in the cloud. Trustgrid nodes can be set up to integrate with existing capabilities in AWS, AZURE or Google Cloud and establish integrations to data centers or on-premise resources. Leveraging Trustgrid's clustering technology these nodes can also be configured for failover protection, ensuring consistent uptime should a node ever drop connection.

**Visibility |** Trustgrid's cloud portal gives global visibility by allowing you to see the status of all connections from a single pane of glass. This view and control of all connections can be used as a single source of truth for current bandwidth usage statistics and historical network events. The portal also enables the browsing of Netflow-like traffic and delivery of logs to a SIEM or storage services like Amazon S3.

**Operations |** Trustgrid was designed to centralize the management of connectivity between disparate and remote resources at scale. Whether connected resources are owned by one organization or shared between two organizations, all connections leverage standard broadband internet and can be configured via the cloud portal to share visibility and management responsibilities. In addition, software patches and updates can be pushed to all nodes, but when needed, lay waiting in a queue until updates are approved by an owner on the other end of a connection.

**Security |** Security is Trustgrid's top priority. Once connected, network tunnels leverage mutual TLS authentication that can be managed by a customer-owned certificate or hardware-based authentication. All user authentication events are logged, and administrators can be alerted to failed or unauthorized authentication attempts. Additionally, all configuration changes are logged and can also trigger alerts.

**Support |** The Trustgrid cloud portal is equipped with a variety of support tools to enable less technical staff to extend Level 1 support into tasks previously reserved for Level 3 engineers. A management API enables the scripting of common management tasks including automated support and failover tasks. Trustgrid also provides advanced support to assist with any software issues.

Trustgrid automates many configuration, provisioning, and management tasks while drastically simplifying the management of connectivity across multiple environments. This allows fast, easy deployment of new connections, lower network management requirements and the ability to scale network management across hundreds to thousands of connections.


888.308.8995
info@trustgrid.io

**Learn More About Network Management for Hybrid Environments at www.trustgrid.io**