

eBook



Build Cloud to Edge Architectures with Docker Containers

www.trustgrid.io



The era of applications running in data centers and server closets may be past its peak, but it's far from over.

Despite what the bloggers or tech media may have you believe, many applications remain (and possibly will always remain) running on on-premise. While these applications may not be moving to the cloud, the push for innovation persists.

For applications requiring on-premise components, innovation is being achieved through advances in software-defined networking coupled with edge computing capabilities.

Legacy applications desiring more architectural flexibility are extending some services to the cloud, even when most of the application's services remain on-prem. In these distributed or hybrid scenarios, some application workloads will process at the edge for cost, security, or technical reasons; while other services run in the public cloud - with data moving freely (and securely) between both.

Because the cloud-delivered components are usually built as multi-tenant applications by the software vendor and extend into a remote environment running the on-premise components, there are unique challenges associated with the deployment, management and support of these architectures.

Contents

- 01 The Challenges
- 02 The Trustgrid Platform and Products
- 03 Trustgrid Connect
- 04 Trustgrid EdgeCompute
- 05 Trustgrid Remote Access
- 06 Building with the Trustgrid Platform

The Challenges

SaaS applications that require connectivity into legacy systems or on-premise customer environments will require a networking component.

Initially, a software vendor's understanding of the networking challenge is focused on the most important one or two issues preventing success. As development progresses and deployments scale, the extent of the challenges come into greater focus.

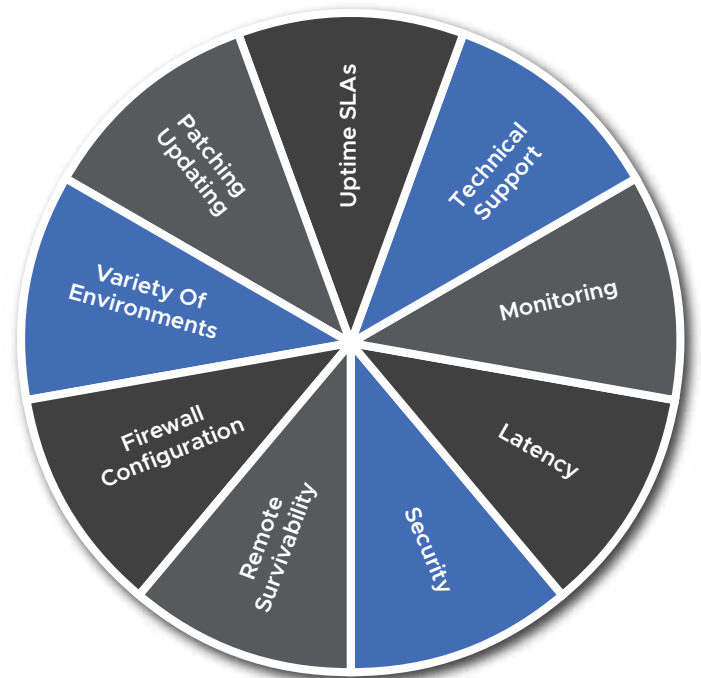
Deployment challenges are usually the first to cause pain. When cloud applications are dependent on a 3rd party-controlled environment the networking solution will require a change to on-prem firewall configurations, run into network address translation issues, and could even be impeded by their customer's available IT teams.

SaaS product and engineering leaders may initially seek to solve these challenges with tools like VPC peering and VPN gateways. But neither of these solve the scalability challenges of deploying and managing hundreds of connections and VPNs into customer environments.

Additionally, as a SaaS solution evolves, so do its architectural requirements. Often, connectivity solutions that were viewed as acceptable yesterday no longer work for the roadmap and profitability requirements of tomorrow.

Some vendors may want to run additional services at the edge, some may want a common way to access adjacent on-premise systems. Establishing a common way to manage and run workloads at the edge, through the use of containerized services, is usually one of these evolving requirements.

These types products or features may be prevented from future implementation due to ill-informed architectural choices early in the development of the product. SaaS vendors deploying cloud services like this need a more purpose-built connectivity solution that does not require the management of hundreds (or thousands) of unique VPN configurations.



The most common cloud to on-premise networking challenges

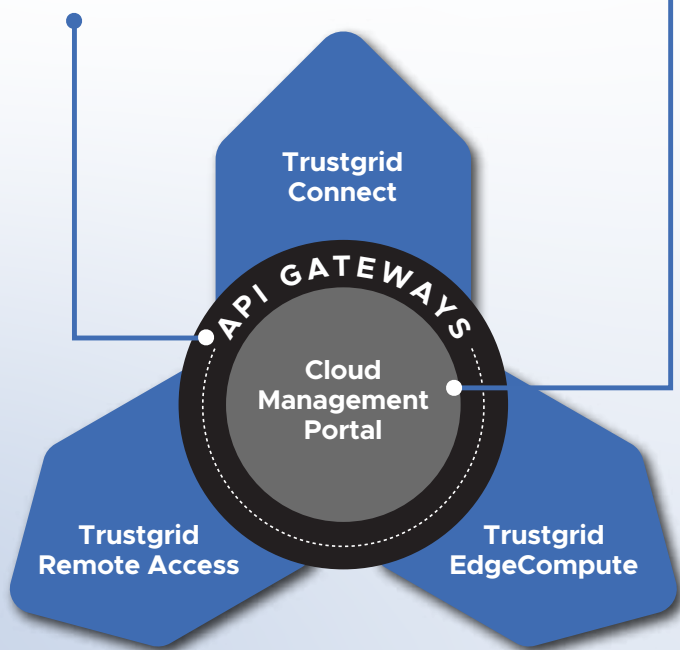
The Trustgrid platform is designed as an alternative to VPN and MPLS solutions and solves many of the issues encountered by SaaS application providers as they attempt to connect, deliver and scale applications from the cloud to the edge.

The Trustgrid Platform

Trustgrid gives software providers the ability to seamlessly build, connect, and deliver applications across any environment (owned or 3rd party) with the same levels of control and automation they experience in the cloud.

The Trustgrid platform enables this by supporting both networking and edge computing features on the same virtual appliances or hardware. Trustgrid nodes support software-defined networking as well as running proprietary scripts, ETL functions and Docker containers across any cloud or on-premise environment.

From within the platform, existing APIs can be secured with network protection and new APIs can be created from edge data sets.



At the center of this multi-tenant connectivity solution is the Trustgrid management portal.

The portal is used to configure and monitor networking functions and orchestrate the software running on nodes. From a single pane of glass admins can manage scripts and containers, push and track versions, and provide all troubleshooting tools for remotely deployed software components.

Trustgrid’s customers typically seek this type of a solution when they want to deploy code into 3rd party environments, but manage it as if it is a public cloud service.

This allows their software development and DevOps teams to remove themselves from the provisioning of networking and management of edge computing capabilities, and focus on delivering software to hundreds or thousands of locations with minimal support hassles.

The Trustgrid Products

Each of the products in the Trustgrid Platform work seamlessly together to build, manage and support cloud-to-edge architectures from a common management portal.

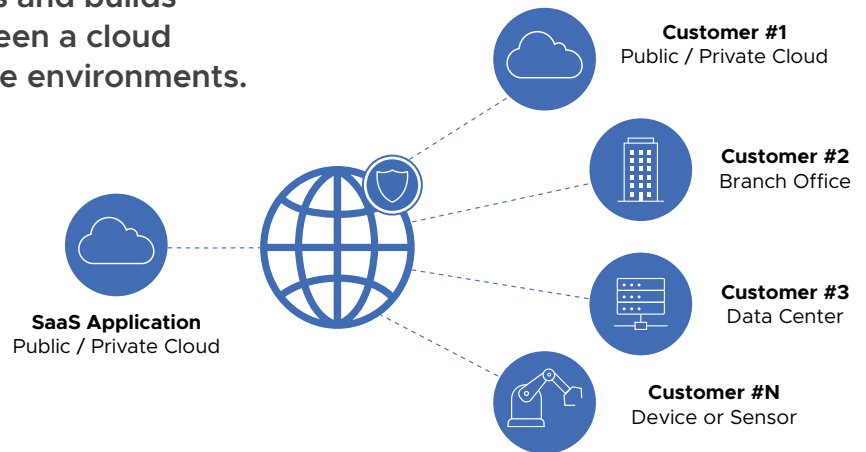
Trustgrid Connect	High throughput, secure networking to connect applications and data
Trustgrid EdgeCompute	Deploy, update, and monitor containers and VMs scripts at the edge
Trustgrid Remote Access	Zero Trust network access to manage and support remote applications

Trustgrid Connect

Trustgrid Connect is a network-as-a-service delivering next-gen SD-WAN capabilities. It is designed to meet the challenges of application providers who require cloud-to-on-premise and multi-cloud networking. The product runs in all public and private cloud environments with plug-and-play deployments that eliminate the need for on-site networking expertise.

Trustgrid Connect is critical to connecting distributed application components and builds a multi-tenant network fabric between a cloud application and any number of edge environments.

Specifically designed for SaaS applications that must connect to hundreds or thousands of customer, partner, or other diverse IT environments, Trustgrid Connect is an alternative to site-to-site VPNs and MPLS and provides a cloud-delivered WAN, optimized for ease of management.



Trustgrid Connect provides all the tools to build both mesh and hub-and-spoke architectures to support multi-cloud, hybrid cloud (cloud to on-prem), and on-prem to on-prem use cases.

Trustgrid offers IP SLA to select the best path for traffic, as well as QoS at the end points to prioritize latency sensitive data.

Segmentation by customer is default behavior and can integrate to VRFs and VLANs in data centers and cloud environments.

Application providers gain global visibility, control and support capabilities from a single pane of glass that logically separates each network from each other.

This multi-tenant connectivity allows for an application provider to support the entire network as if it is another cloud delivered service.

Trustgrid Connect features include:

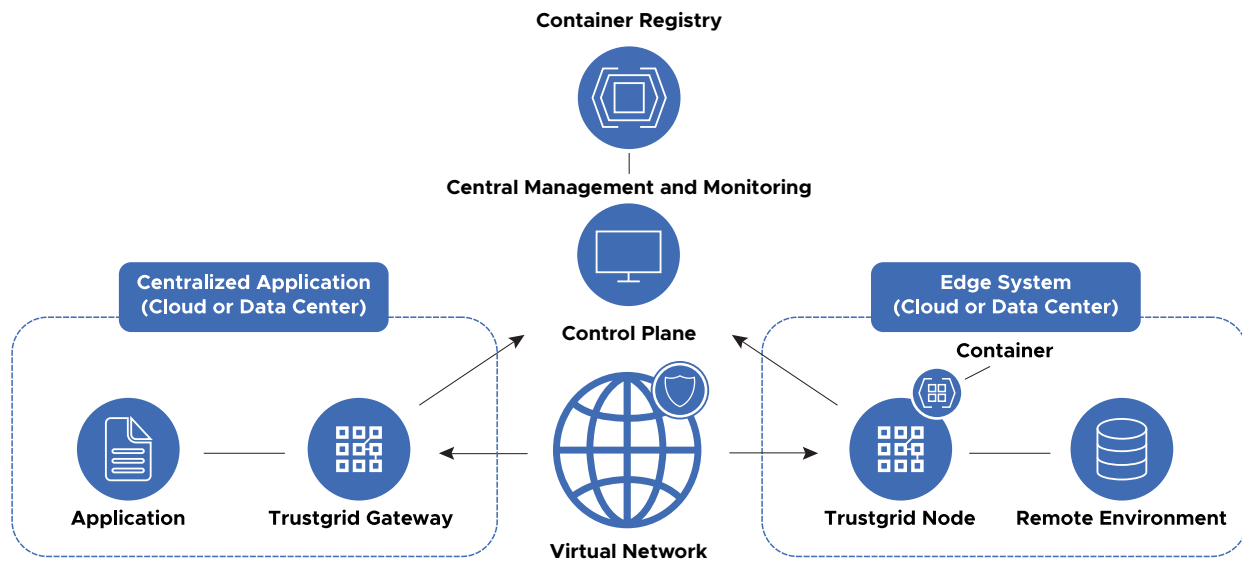
- Layer 3 / 4 networking
- Zero trust network architecture
- Separate control plane and data plane
- Certificate-based authentication
- Continuous patching and updating
- Automated failover and disaster recovery
- Supports all cloud and on-premise environments
- Simplified network address translation management
- 1-touch deployments with little to no firewall reconfiguration
- 99.99% uptime SLA

Trustgrid Connect works seamlessly with Trustgrid EdgeCompute or Trustgrid Remote Access.

Trustgrid EdgeCompute

Trustgrid EdgeCompute adds to the capabilities of Trustgrid Connect to provide a distributed computing platform for deploying and supporting distributed applications at the edge.

Integrating networking features with a containerized application platform, Trustgrid EdgeCompute overcomes the challenges of edge computing by delivering infrastructure, services, APIs and software lifecycle management tools to applications running in on-premise locations.



When connecting distributed applications, Trustgrid EdgeCompute allows for plug-and-play edge deployments that run advanced services on-premise while eliminating the need for on-site networking or container expertise.

For application providers building applications that require low latency, local data processing, or need to meet data residency requirements, EdgeCompute creates a seamless distributed application delivery environment that allows edge appliances and services to be managed in the same way as a cloud service.

Trustgrid EdgeCompute features include:

- Edge computing with seamless networking
- Cloud managed container repository
- Support for Docker containers and KVM virtual appliances at the edge
- CI/CD integration for automated patching and updating of remote systems
- Ability to build and maintain APIs for any data source
- Supports 1000s of remote services from single pane of glass
- Run 3rd party security solutions on at any edge location

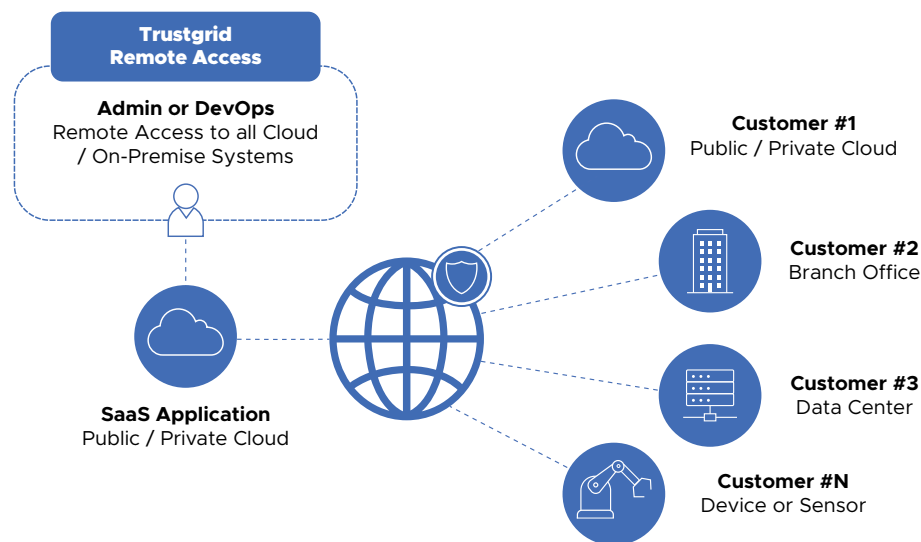
Trustgrid EdgeCompute works seamlessly with Trustgrid Connect or Trustgrid Remote Access.

Trustgrid Remote Access

Building distributed applications is the initial challenge, but supporting them at scale is another. Trustgrid Remote Access provides zero trust network access (ZTNA) for software administrators and DevOps teams supporting distributed application deployments.

Trustgrid Remote Access is designed to provide secure, granular access to remote application components for patching, troubleshooting and support.

Legacy VPNs or remote desktop support tools lack the granular access management controls needed for sensitive application components and can be easily exploited via stolen credentials and session hijacking. Extending remote access to 3rd parties or vendors for support can introduce even more risk.



Trustgrid Remote Access supports applications running in any cloud and on-premise environment by using an agentless web interface to grant access across a range of applications and devices.

Access policies can be custom configured within the tool utilizing existing roles, groups and permissions from 3rd party identity providers. If an agentless approach is not desired, open-source agents such as OpenVPN or Wireguard are also supported.

Trustgrid Remote Access features include:

- Agentless zero trust network access
- Supports access to apps on all popular operating systems
- Integrates with your existing IdP (Azure AD, Okta, Google, and more)
- Maintains auditable logs of all application access
- Provides secure access to remote container deployments
- Remotely supports systems behind firewalls you don't control

Trustgrid Remote Access works seamlessly with Trustgrid Connect or Trustgrid EdgeCompute.

Building with the Trustgrid Platform

Trustgrid is one of the only solutions on the market combining cloud networking, edge computing, and zero trust support tools for application providers.

How it all comes together.

Combining the elements of the platform, developers build and run services across any cloud, data center or on-premise environment.

The architecture starts with networking from Trustgrid Connect. Extending secure multi-tenant connectivity from the cloud, tunnels are configured, managed, and monitored from the Trustgrid management portal.

At the edge, full software lifecycle features manage the application components running on the Trustgrid nodes - allowing for containerized services to be deployed, version controlled, and supported centrally.

Trustgrid Remote Access then provides the zero trust network access used to support all of these elements.

Delivering multi-tenant SaaS applications requires automation and optimization in every layer in the stack. When integration with on-premise environments is needed, these requirements are complicated by the variety of systems, complexity of configurations, and lack of control over 3rd party infrastructure.

Tackling these challenges with Trustgrid enables software providers to build seamless cloud-to-edge architectures utilizing cutting edge networking and edge computing features specifically designed for these use cases. Functioning as a managed platform, developers and DevOps teams can focus on their product instead of maintaining the infrastructure that it is running on.

Trustgrid combines the power of connectivity and compute
in service of application developers and DevOps teams.