A Next Generation Centralized Edge Compute Platform

Steven Stites, CTO
Joe Gleinser, CPO
www.trustgrid.io

Abstract

The edge is exploding with the most exciting technologies being developed today - blockchain, IoT gateways, self-driving vehicles, and machine learning. Applications deployed in the edge, at enterprise scale, encounter significant challenges such as connectivity, availability, latency, security, compliance, and lifecycle management. Trustgrid solves these challenges with our Edge Compute Platform that combines software defined networking (SDN), advanced security features, compliance with rapidly evolving regulatory environments, and application lifecycle management including deploying and managing serverless applications in the edge.

Today the edge has two predominant technology architectures defined by maturity and prospects for growth. There is a “born in the edge” contingent built on feature expectations created by AWS but with the typical maturity of any rapidly advancing technology. When building is the only option many necessary features are deprioritized. IoT gateways, self driving vehicles, and edge data centers are struggling with new challenges and high expectations. Legacy on-premise infrastructure is the second common architecture at the edge. It operates much the way it has since the mid 1990s. Its expensive hardware-centric approach, advanced skill-set requirements, and decentralized UI/CLI driven management excessively consumes IT resources and budgets.

Trustgrid’s Edge Compute platform provides serverless application architecture in the edge by combining an enterprise-class software defined network, automated management, state-of-the-art security, and tools to enable compliance with rapidly changing regulatory environments, including GDPR. The platform dramatically reduces the costs of edge deployments to create opportunities that were not possible with legacy deployment methods.

The core challenges of edge deployments are:

1. Security
2. Availability
3. Connectivity
4. Compliance
5. Management
6. Cost

Trustgrid mitigates these challenges with a hardware agnostic approach, a robust API for management and data acquisition, and a flexible architecture that manages the lifecycle of edge applications.

Trustgrid is built to power the advanced, evolving edge use cases such as low latency data distribution (e.g., CDNs and Netflix Open Connect), large data storage requirements (e.g., Dropbox), 5G networking, and distributed machine learning. Trustgrid can replace legacy edge infrastructure with an advanced Edge Compute Platform.

Architecture

Nodes

A Trustgrid Node is edge software deployed on hardware or virtual appliances leveraging open source components to create a lightweight, flexible platform for edge application execution and data acquisition. Nodes can be installed anywhere, on nearly any platform, including public and private cloud infrastructures. The primary purpose of a Trustgrid Node is to host edge applications and/or expose hosts, services, or data between or among other authorized nodes.

Cloud Management

All Trustgrid Nodes are managed from a cloud portal that provides a powerful UI and REST API for managing Nodes in real-time. The cloud management infrastructure includes a Public Key Infrastructure for authentication, secure software repositories to manage application and OS updates, and cloud policy manager that tracks the security context of the distributed environment and applies authorization policies to enable or restrict communication between Nodes and services.

Domain Security Model

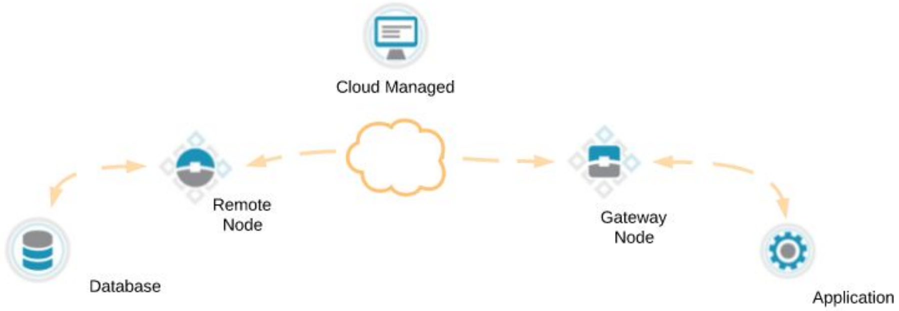
Trustgrid Nodes are grouped into domains and subdomains for automated configuration (profile inheritance) and group security policies. Domains provide an intuitive way to organize nodes in a way that can easily be reflected in DNS, as well a mechanism for quickly creating or revoking authorization policies between specific groups of nodes.

Software Defined Network

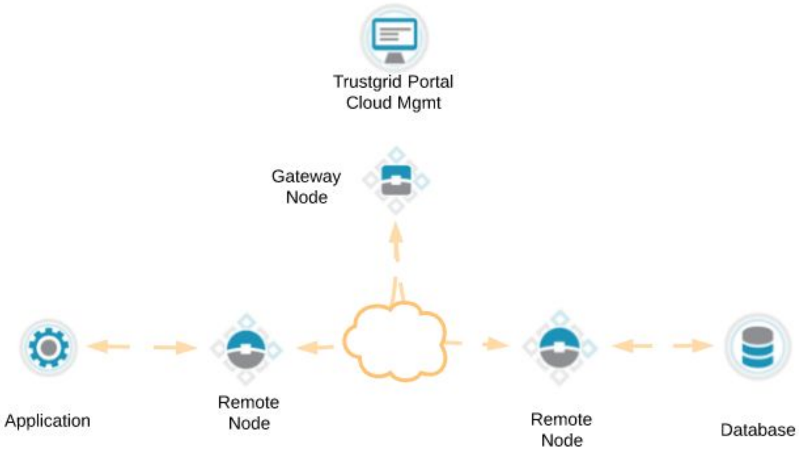
Trustgrid allows the user to define distributed virtual L3 or L4 networks that can span any number of nodes and locations. Applications can then forward L3 traffic or proxy L4 traffic across this network according to the network security policy. The underlying data plane that implements the network consists of a dynamic and encrypted mesh network that is constructed between relevant nodes.

Nodes connect to each other using TLS tunnels to form a software defined mesh network. The resulting SDN leverages TLS 1.2 to traverse firewalls easily and provide advanced encryption of data in transit, and can be used to route L3, L4 or L7 application traffic. Because this encrypted data plane is completely separate from the cloud management plane, sensitive data does not need to ever pass through infrastructure that is not owned or controlled by the customer or user.

Gateways are nodes that designated to receive incoming TLS connections from other Nodes in order to route traffic. Gateway Nodes can be deployed in a two-node or three-node architecture.



Two Node Architecture



Three Node Architecture

Three-node architectures allow for cloud hosting of nodes that can optimize performance across the network. Trustgrid testing shows substantial performance increases even when compared to unencrypted traffic through intelligent placement of cloud Gateway Nodes.

Nodes may be deployed as clusters which enables both load balancing and failover between nodes in the cluster. Clusters may encompass any number of nodes within a single datacenter/cloud, among multiple edge locations, or any combination thereof. These features combined with basic API scripting enables robust Disaster Recovery configurations to meet a variety of network and application requirements.

Public Key Infrastructure

Trustgrid built a proprietary Public Key Infrastructure (PKI) based on decades of cryptographic experience in enterprise software engineering. Trustgrid hosts a cloud-based Certificate Authority (CA) that enrolls certificates for newly registered nodes which are subsequently used for TLS mutual authentication. In addition to each node having their own unique and secure certificate, all node communication to the cloud is locked down to only trust servers that have been signed by Trustgrid. When forwarding traffic between nodes, no traffic is permitted without the remote node(s) presenting a valid certificate that can be verified by the Trustgrid CA.

Zero Trust Security

Derived from Google’s BeyondCorp initiative, Trustgrid incorporates a zero trust security model into all policy definition. By eliminating any implicit trust assignment this model can dramatically reduce the risk of breach. As zero trust is a drastically different model than most networks used today, Trustgrid also gives a set of L3 forwarding capability to allow an easy transition to a zero trust model by first identifying the L3 traffic flowing across the network, and then creating L4/L7 policies to lock down the network traffic to only the traffic that is needed and expected.

Edge Applications (Serverless)

Applications operating in the edge benefit from Trustgrid’s CI/CD pipeline which enable cloud deployment methodologies to extend to edge applications. Trustgrid unique application enablement platform allows the application developer to define what application operations are accessible to which callers, and transparently handles the complex networking that may be between the caller and the application. Supporting both traditional and serverless edge application architectures across a wide variety of languages, Trustgrid provides the most flexible edge compute platform on the market.

Edge API

The edge hosts diverse data sets that are consumed by cloud applications in financial technology, IoT, and healthcare. Often these datasets are closer to end users than the cloud applications, but it can be difficult to securely offer this data to the consumer where it most makes sense. To solve this problem, Trustgrid provides a robust and secure API toolkit to provide access their data at the edge via well defined REST APIs, or streaming web 2.0 technologies . By exposing the diverse datasets in a single API, executed on the edge Node, and geo-locating users, Trustgrid can improve application performance by reducing latency.

Hardware Agnostic

The price and performance of edge compute, driven by low cost and highly capable IoT hardware, enables Trustgrid to support a variety of low cost devices.Trustgrid is deploying on sub-$100 devices up to traditional multi-U servers. The market is flush with sub-$500 options that meet the needs of most edge deployment scenarios in IoT, fintech, and healthcare.

Use Cases

Trustgrid technology enables advanced solutions in the following use cases.

Multi-Cloud Compute and Cross Connectivity

Applications and data distributed among multiple public and private clouds present unique challenges to connect, secure, and manage. Connectivity must leverage software defined networking features to offer universal support for all cloud technologies. Security models must support trusted and untrusted connectivity. Management should be centralized and automated.

Trustgrid delivers robust connectivity, high security, and automated management to enable distributed applications and datasets across leading public and private cloud environments.

Fintech and Healthcare SaaS

Financial technology and healthcare industries require extensive integration to thousands of edge data sets to power SaaS and centralized applications. Fintech consumes core banking software and associated data to deliver digital banking applications. Electronic Medical Records integrates to practice management and associated systems to provide an integrated environment to healthcare users.

Trustgrid enables fintech and healthcare SaaS providers to securely, compliantly, and efficiently integrate edge data sets and architect applications to deploy to the edge.

Industrial IoT Gateways

With more than 700 gateway providers to market, the rapidly expanding field of Industrial IoT (IIoT) Gateways is one of the hottest spaces in tech. As with most markets early development has focused exclusively on minimum requirements for customers still more interested in proof-of-concepts than large scale deployments.

Trustgrid provides "magic quadrant" features for existing IoT gateway solutions with an Edge Compute platform that delivers advanced security, application lifecycle management, network and configuration automation, and centralized management.

Edge Data centers

Cloud providers are likely to describe the edge in the scope of dozens of datacenters. CDN providers will talk about the edge in hundreds of datacenters. New players are rapidly emerging that describe the edge in an order of magnitude more locations. Edge datacenter players like Vapor.io and Dartpoints are scoping the edge at tens of thousands of data centers localized to within a few miles or less of the end user.

Trustgrid is the perfect platform to take the ping-pipe-power approach of edge data centers into application development teams around the world.

Dynamic CDN

With the announcement of Cloudflare Workers, the first dynamic CDN feature set is loose in the market. CDNs traditionally supported only static content that must be replicated across hundreds of geographically distributed nodes.

Trustgrid enables serverless applications to be distributed across the same network for dynamic content distribution.

Local CDN

Edge datasets live adjacent to users and devices that create and consume the data. Cloud and, more generally, application centralization, has forced users and devices to suffer substantial latency on round-trips between the centralized applications and edge datasets.

Trustgrid enables users and devices to consume centralized applications with geolocated API access to local datasets. This eliminates as much as 50% of latency to dramatically improve application performance and responsiveness.

Blockchain

Blockchain represents one of the largest, decentralized edge applications deployed today. Blockchain requires a mesh topology for decentralized replication. Use cases outside of crypto-currency are exploring the centralized vs decentralized management infrastructures. Development of blockchain technology is currently a ground-up undertaking unless developers leverage a crypto-currency platform such as Ethereum.

Trustgrid's platform accelerates blockchain development by leveraging the security, networking, and management features inherent our Edge Compute platform without the need for cryptocurrency integration.

Edge PaaS / Serverless Applications

A platform-as-service (PaaS) approach to edge application development will enable edge applications to achieve the agility of cloud PaaS and Serverless applications. Azure IoT and AWS Greengrass are early players, as are dozens of IoT Application Enablement Platforms that deploy applications to bridge Information Technology (IT) and Operational Technology (OT).

Trustgrid is a next-level Edge Compute platform that delivers PaaS and serverless features to edge applications.

Self-Driving Vehicles and Drones

"Data centers on wheels and wings" are a quickly evolving space for edge compute. These devices generate huge amounts of bandwidth while requiring extremely low latency application responses (swerve or brake). As with IIoT Gateways the focus today is on basic functionality and safety. As these technologies mature enterprise-scale deployments will shift the focus to deployment, management, security, and regulatory compliance.

Trustgrid will be the platform of choice for large-scale deployments of applications across winged-or-wheeled devices.

Conclusion

The edge presents a serious challenge to incumbent technology architectures and the next evolution of platform-as-a-service capabilities. Trustgrid will enable developers worldwide to seize this opportunity without the drag of platform hardware, management, networking, and security.