



Connecting Cloud Applications to Community Banks and Credit Unions

FinTech applications, moving to the cloud, experience unique challenges.

The thousands of community banks and credit unions across the US are rapidly embracing cloud applications to deliver online/mobile banking and other services to their customers. But, software providers in this market are being held back from successful cloud migrations by their connectivity requirements to the core banking data within these banks and the core banking providers' data centers.

The technical limitations and complexity of legacy WAN solutions have become one of the biggest challenges for FinTech providers seeking to capitalize on the benefits of moving their applications to the cloud.

This white paper highlights the challenges that providers must take into consideration as they seek to connect FinTech applications to customer systems and data.

Cloud Migrations for FinTech Applications

Unlike branch-to-branch networks, connecting cloud-hosted banking applications to a financial institution's on-premise, core banking data (or a core banking provider's data center) presents challenges that are unique to the FinTech industry.

Compliance

In a compliance heavy industry such as banking, due diligence in selecting vendors should be thorough. The current infrastructure of banking has been built on a foundation of technology that has passed the rigor of previous compliance testing. But all of this must be re-evaluated with new compliance testing when moving to the cloud. Financial institutions (FIs) will want vendors to ensure that new solutions are both vetted and tested. New compliance standards have been established for the cloud to help both application providers and FIs navigate these waters. Product and service vendors supporting a cloud migration should be asked about their ability to meet standards such as SOC 2 Type II and PCI.

- Amazon Web Services and Microsoft Azure maintain compliance to most major security standards and publish their compliance reports, including SOC 2, for customers.
- Many SD-WAN and other network providers are not compliant with standards such as PCI and SOC 2 Type II. Some use partners for deployment and management that may also require compliance audits.

Security

The control and security of data is much easier when the application resides behind the same firewall as core banking data. Moving to the cloud forces a rethinking of some security functions such as reporting, access controls and the dynamic of how data is transported over the internet. A variety of pre-packaged security solutions are available (IDS, IPS, SIEM, IAM, etc) and allow for the easy implementation of security features that can strengthen an application's security posture far beyond what has been used historically. A cloud migration also presents a great time to begin thinking about the implementation of more advanced networking features like certificate-based authentication or Zero Trust networks.

- Encryption at rest is available in most major cloud providers, but is usually not configured by default. Support for encryption at rest can vary widely by the service in use at the cloud providers.
- The configuration of users and organizations within public clouds is complex and requires extensive research of best practices and planning. The complexity of this task is often underestimated.

Coexistence with Legacy Systems

Moving applications to the cloud reshuffles and optimizes an organization's IT infrastructure. Modern application architectures allow for storage and compute workloads to be separated across geographic and organizational boundaries. New systems will sit alongside legacy ones...and cloud resources will need communication with on-premise. As these hybrid cloud environments are being rearchitected, special consideration should be paid to where these resources will live, how they will be managed and how they will connect to each other. Reliable, highly available and secure connections will be required.

- Dedicated network connections from cloud providers, such as AWS Direct Connect and Azure ExpressRoute, deliver high bandwidth and low latency between legacy data centers and new public cloud environments. These solutions are priced by the hour and amount of data transferred.
- VPN connections, while more complex to configure, may be an effective alternative if Direct Connect or ExpressRoute are not options.
- Software-defined networking options have emerged as a more flexible and inexpensive way to manage the connection between cloud and on-premise environments. Attention should be paid to a vendor's ability to support your particular cloud environment and customer deployment needs.

Heterogeneity of Customer Environments

FinTech applications rely on the core banking data held by their FI customers. Current WAN connectivity solutions such as VPN and MPLS were not designed for cloud environments and present a number of challenges during both deployment and management phases. Variability in onsite technical expertise, network configurations and security policies can complicate new customer deployments. While scaling connectivity to these heterogeneous environments adds to the management complexity as application providers must manage dozens, hundreds or even thousands of connections at great time and expense.

Networking solutions should be flexible enough to connect from the cloud to any customer environment without the need of advanced skillsets on site.

- Many SD-WAN solutions offer limited public cloud support for mission critical applications (high availability and/or multi-region failover). Native networking solutions from the public cloud providers can offer high availability or multi-region failover, but frequently struggle with other networking challenges that would be considered basic features of routers.
- Overlapping RFC 1918 private subnets (e.g., 192.168.0.0, etc) are a serious challenge when connecting from an application provider's network to a variety of different customer networks. Managing the NAT translations can be tedious and cumbersome, if it's even supported. Software-defined networking solutions offer features to handle this problem and speed up initial deployments.

DevOps Transformation

Moving to the cloud means gaining the ability to centralize operations, automate tasks and move to a more agile form of product/service delivery. Initially, the network had not been part of that transformation. Recent developments have changed this. Advances in software-defined networking have allowed for IT and software development teams to take greater control of connectivity between applications and operate with DevOps like efficiency.

By abstracting the complexity, incorporating automation features and allowing for flexibility in deployments, a software-defined network can begin to evolve and operate as fluidly as the applications it is serving.

- Basic coding skills with languages such as Python can automate many common tasks in all public cloud environments and software-defined networks.
- Training up networking teams for new responsibilities often creates concern about the stability of their positions. Focusing on the new challenges of public cloud and opportunities for the automation of manual tasks can help overcome this concern.

Time to Transition

Cloud migrations present a significant shift for FinTech applications and their organizations. Not only are architectures and infrastructures being improved, but so are the workflows and staffing resources needed to get everything accomplished in both the short and long term. Considering the number of transformative changes occurring, it is not uncommon for timelines to take much longer than originally anticipated with many taking at least a year for an initial phase to be completed.

- Cloud environments can be configured to best practices from scratch in days or weeks. However, the steep learning curve and application compatibility issues will inevitably cause some schedules to slip.
- For FinTech application providers that connect to their customers, engaging each customer for new network connections, firewall rules, DNS, or other changes may present the greatest scheduling challenge.

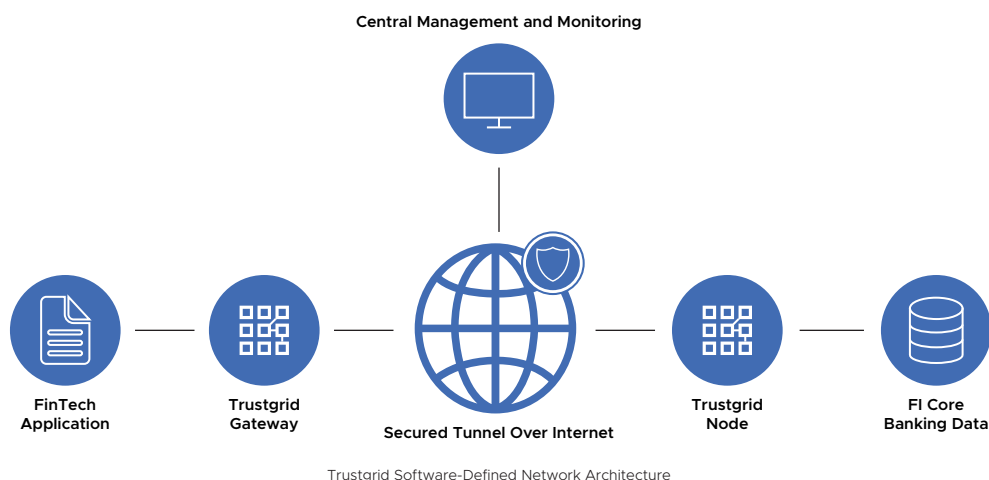
Often many of these cloud migration challenges are either not considered, or under-appreciated in the planning phase. By getting in front of these questions early in the planning process, organizations can minimize the time to success and improve business outcomes.

Trustgrid enables seamless transitions to the cloud for FinTech application providers that must integrate to core banking data

Trustgrid’s software-defined connectivity was designed for FinTech application providers connecting to customer environments. As an application-specific networking solution, it has been engineered to facilitate seamless cloud migrations by securely connecting cloud environments to on-premise networks.

Quickly Connect to Customer Core Banking Data

Deploy new customers in a fraction of the time by replacing legacy WAN infrastructure with a cloud-native solution that improves the visibility and control of hybrid environment resources.



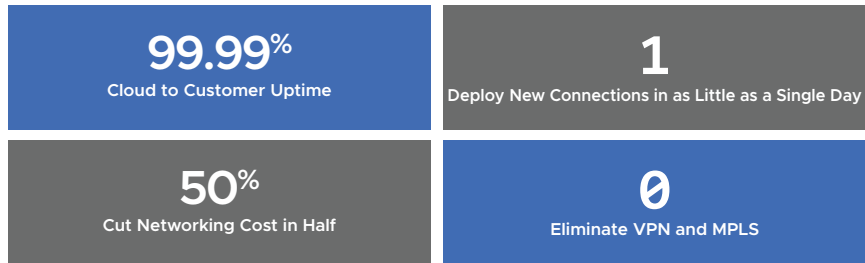
Lower the Cost of Connectivity

Eliminate costly VPN and MPLS connectivity, enable remote monitoring, and automate management functions to deliver both hard and soft cost savings that are realized immediately.

Invest in Cloud-Ready WAN

Trustgrid's software-defined architecture is designed for today and tomorrow's hybrid cloud environments. This means your network is accessible, continuously improving and easily deployed in any environment.

Securely connect cloud-hosted banking applications to customer's core banking data.



The Trustgrid Difference

Networking

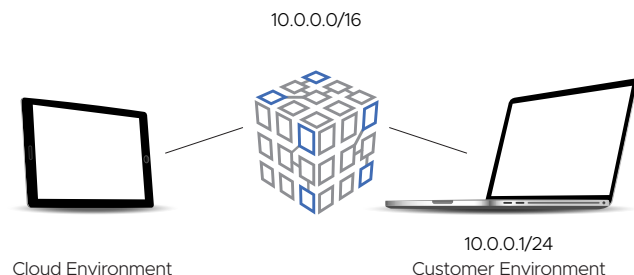
Eliminate dependence on VPN hardware and MPLS subscriptions with software-defined networking that meets or beats the performance of these legacy solutions. Advanced security, failover, and automated management features ensure greater security and reliability with less management overhead than traditional network solutions. Connections support high availability (99.99%) and are capable of ultra-high throughput for data intensive applications.

Additionally, when connecting a customer's network to a cloud application, challenges arise when the two networks use a common IP space. Trustgrid also handles the challenging task of overlapping private subnets (RFC 1918) with intuitive network address translation (NAT) features. By creating a virtual network overlay, application providers are able to configure and manage segmented networks as if they are all on the same virtual network. This virtual network streamlines the management of connected customer networks from deployment to support.

Security and Compliance

Trustgrid is a SOC 2 Type II certified organization built for compliance with FFIEC, PCI, as well as many other cloud and banking standards.

Advanced security features including certificate-based authentication, Zero Trust networking, and granular activity logging work to enhance security over legacy networking solutions.



And because it is software defined, updates are continuously and seamlessly pushed to all connections to enable effortless patching and network compliance. The logs of these activities are then made available as reports for auditors or can be pushed to other security applications for analysis.

Management

From a single pane of glass, the Trustgrid cloud-delivered management portal gives complete control and visibility over all connections to provide centralized troubleshooting and support. This portal allows operators to see the status of all connections, be alerted to anomalies and centrally support all connected customers in a DevOps-like fashion.

The portal also provides role-based access control features which enables the secure co-management of connections. This gives FinTech customers the ability to monitor network connections and produce reports on the activities of their connected IT resources.

Deployments

Difficulties in deployments cause frustration, loss of revenue, and poor customer experience. Trustgrid has streamlined and automated the way FinTech application providers establish initial connectivity between the cloud and their customer's core banking data.

Leveraging software deployed as virtual appliances or on off-the shelf hardware appliances, Trustgrid accelerates deployments to cloud or on-premise customer environments and eliminates the need for onsite specialists.

Step 1	■ An Amazon Machine Image (AMI) is deployed in the AWS environment using a Transit Gateway VPC.
Step 2	■ Trustgrid helps the application provider select a secure off-the-shelf hardware appliance and images it with Trustgrid software.
Step 3	■ A new FI customer is sent the imaged hardware device with instructions to simply provide power and a network connection.
Step 4	■ Once connected, the device is configured from the application provider's cloud management portal.
Step 5	■ Secure connection is established between the cloud and on-premise environments.

Hybrid Cloud Connectivity Consulting

Delivering on a cloud-first strategy brings a consistent stream of unforeseen questions, challenges and surprises. Trustgrid provides consultatory services to assist with the technical and operational aspects of network infrastructures that hybrid cloud environments require. Network analysis, connectivity roadmapping and implementation are all provided by a team of cloud networking experts.

The Answer is Trustgrid

From simplified deployments to automated management and support, Trustgrid has empowered some of the leading digital banking application providers to make the switch to the cloud. Get cloud migration ready and connect with software-defined networking from Trustgrid.