trustgrid

The 5 Biggest Reasons Client Connectivity Requires Attention

Fintech Client Connections are NOT Like Ordinary Connections

Fintech applications rely on the core banking data held by their FI customers. To an outsider, this connection may seem to be a simple networking challenge... find one of the 100 vendors offering to secure a tunnel between the bank's data center and the application provider.

However, there are numerous reasons why this unique situation can produce some unexpected challenges.

- **Security and compliance are critical**
- **Deployments are more complicated**
- **Network is a bottleneck to modernization**

The nature of handling sensitive financial data changes everything. When you compound this with the challenge of connecting multiple organizations, and then introduce cloud operations into the equation, the status quo begins to show even more cracks.

Challenge #1 MPLS circuits are overpriced and provide limited value

Waiting months to turn on a connection, followed by paying hundreds or thousands of dollars a month for a simple network connection not only provides for a poor customer experience, but erodes margin.

Answer: Trustgrid's software-defined connectivity leverages widely available broadband internet to provide the same uptime and security benefits while enabling the ability to deploy new connections in just hours.

For More Information Visit **www.trustgrid.io**

Challenge #2 VPNs are difficult to deploy and manage

Using IPSec VPNs to connect centralized applications to remote core banking data creates configuration challenges due to the differences in host and client environments. This often requires onsite networking expertise and coordination with a customer's IT department. Once configured, managing a footprint of hundreds of VPN connections means patches and updates often happen on infrequent schedules, opening the possibility of security and compliance lapses.

Answer: Trustgrid gives application providers plug-and-play networking deployments into a customer's data center. Once connected, updates are simultaneously pushed to all connections, saving staff hundreds of hours a year and ensuring that the network is always up-to-date.

Challenge #3 Lack of visibility creates security gaps

Legacy connectivity options such as VPN and MPLS lack the ability for centralized visibility and monitoring of networks. Due to the importance of always-on connectivity between financial applications, security and availability of every connection is mission critical. Lack of visibility introduces security and down-time risk to the organization.

Answer: Trustgrid's centralized management portal allows fintech IT admins and DevOps to monitor status and receive alerts on all client network connections that need attention. This visibility allows for proactive health checks and lowers the time to remediation when problems do arise.

Challenge #4 Cloud delivery requires modernizing of the network

Connecting two data centers has been the bread and butter of networking solutions for decades. The process, equipment and needed skill sets have been long established. However, this well worn path must be re-evaluated when applications move to the cloud. Traditional networking solutions struggle with cloud connectivity and lack the integration and routing capabilities needed for public cloud environments.

Answer: The Trustgrid platform provides cloud-native connectivity that is managed like another cloud service. Its hardware-agnostic deployment options are compatible with virtually any system or device, allowing for connectivity to any environment. As an API-first platform it easily integrates into an organization's existing security and networking infrastructure.

Challenge #5 End-of-Life refresh cycles are wasting resources

The legacy networking providers are in the business of selling more hardware. They force this upon their customers through 'end-of-life' support for product lines. These vendor dictated refresh schedules force their customers to upgrade to new equipment despite the need or desire to do so.

Answer: Software-defined connectivity decouples the software from the hardware. Software updates are pushed over-the-air and ensure that the network is always up to date without updating expensive proprietary hardware. This separates the need to replace hardware before it is needed and gives the customer greater control over their networking expenses.

Struggling with the connections between your cloud applications and core banking data? Lets talk.