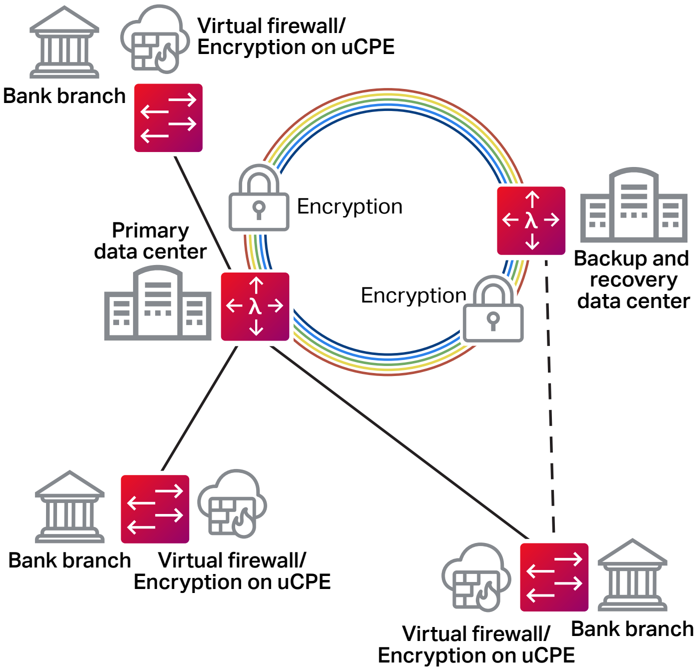
INFOBRIEF

Financial Services Industry Optical Network Use Cases

Network Encryption

As financial services remain a high-priority target for hacking, many banks are looking to strengthen their holistic security capabilities rather than relying purely on perimeter security. This includes ensuring all data is encrypted at rest (for example, when in an array of storage locations). Also, in-flight data protection is increasingly seen as a cost-effective method of enhancing the end-to-end security profile. Solutions must be capable of protecting high-capacity links between data centers or to cloud providers without impacting throughput and latency, as well as the lower-capacity links connecting branches, ATMs, regional offices, etc. What is needed is a solution based on a distributed virtual network function that can be deployed, managed, and updated easily without requiring extra footprint at the bank branch.


Bank branch
Virtual firewall/ Encryption on uCPE
Encryption
Primary data center
Encryption
Backup and recovery data center
Bank branch
Virtual firewall/ Encryption on uCPE
Virtual firewall/ Encryption on uCPE
Bank branch

Ciena provides hardware-based AES 256 encryption with Federal Information Processing Standard (FIPS) certification capable of supporting up to 200 Gb/s per card with minimal incremental latency for encryption between data centers and regional headquarters. This allows the best of virtual encryption and firewall to be deployed onto universal customer premises with equipment deployed at branches, regional offices, and ATM locations.

Ciena's encryption solutions provide a wide range of benefits to the financial services industry, including helping to comply with state, national, and international security and privacy regulations and minimizing impact on application performance and the ability to scale to 200 Gb/s throughput. Additionally, bifurcated management provides separate network and security management that allows the service provider or network team to manage the network while the security team manages the keys. Finally, FIPS-certified encryption can mitigate financial and reputational harm caused by data breaches.

? Was this content useful? Yes No