



CREDIT UNIONS & HYBRID CLOUD:

Leveraging Secure Member Services with Hybrid Cloud

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." – Warren Buffett

Challenges

- Cybersecurity
- Meeting NAFCU standards
- Member privacy
- Interoperability between branches
- Accessibility of data & financial tracking
- Legacy infrastructure maintenance
- Downtime from upgrades & patching
- Lack of skilled, in-house, IT teams
- Mobile banking vulnerabilities

Solutions

- Hybrid Cloud umbrella over multiple technical disciplines
- Role-based data and workflow access to limit exposure
- Integrated, responsive cybersecurity
- Data backups and recovery
- Remote workstations
- Vulnerability Assessments/Pen Testing

Benefits

- Deliver financial services securely
- Build digital trust and member confidence
- FFIEC audit compliance
- Enhance the member experience – reduce frustration
- Gain visibility into the network and systems
- Collaboration tools
- Protect digital identity
- Risk management tools

Credit unions are equally susceptible to digital disruptions as big banks. Technology is dominating the financial market, and credit unions must invest in continuous digital integration without losing sight of the responsibility they owe to their members.

Challenges

Credit union resources are stretched thin addressing multiple challenges posed by government compliance, digital bank competition, and membership demands. Underlying these stressors is the difficulty of securing long-term, in-house, skilled IT professionals. Most credit unions have either shared IT resources in a collaborative manner, or outsourced IT management and cybersecurity to a Managed Service Provider (MSP). The expertise required to solve configuration puzzles between systems/networks/environments and the downtime associated with upgrades, patching, and maintenance is usually more than a single branch can afford.

The ability to collect, analyze, store, and share data securely across branches is of primary importance. Data powers the business, but a data breach resulting in the loss of confidential information exposes more than PPI, it opens the door for continued attacks and the inability to recover customer confidence. Even a single cybersecurity event could result in lawsuits and financial losses that insurance policies do not cover. The long-term consequences are even worse if data backups and disaster recovery are not viable and can lead to an inability to recover data quickly to jump start stalled banking operations.

Solutions

Credit unions holding onto their legacy infrastructure should move to a hybrid cloud infrastructure that will provide integrated security and data protection. Customers expect secure and easy transactions, helpful resources, and to feel like valued members of the institution. Credit unions in turn, must protect their most valuable business commodities – customer data and customer relationships – and this is possible with Hybrid Cloud capabilities.

Data integrity is a central component of credit union operations. Regularly testing the security controls with a Risk Assessment/Penetration Test (testing access to data, breach detection, response to incidents, and monitoring the systems, networks, and environments), as recommended by the FFIEC, will ensure that reported security vulnerabilities have been remediated.

Benefits

Hybrid Cloud offers optimal flexibility to remain competitive in the financial industry. While controlling operational expenses is certainly a motivating factor to digitally transform, a key driver of cloud adoption is gaining visibility into, and control of, critical banking systems, networks, and data to achieve safe handling of highly sensitive membership data and banking operations.

Cloud adoption bridges the gap between disparate data sources and branch locations to allow for greater speed, communication, growth, and smart controls of access to members' financial data and banking service workflows. Many credit unions are turning to MSPs for IT advice, expertise, and ultimately, to engage a high-trust partner for cybersecurity and service delivery. Using the IT 'as a Service' model, an MSP can power the back-end technology needed to deliver financial services efficiently and professionally.

