CREDIT UNIONS & HYBRID CLOUD: SOLUTIONS BRIEF

Leveraging Secure Member Services with Hybrid Cloud

Challenges:

- Cybersecurity
- Meeting NAFCU exam 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 frustrafion
- Gain visibility into your network and systems
- Collaboration tools
- Protect digital identity
- Risk management tools

Although smaller-scale financial enterprises, Credit Unions are equally susceptible to the
same digital problems plaguing big banks. As Credit Unions grow their membership base, they become an easy target for ransomware attacks through unaware employees, mobile banking, lackluster digital security protocols and a tendency to hang on to legacy infrastructure.
Credit Unions must respond to multiple challenges posed by government regulations, compliance reporting and membership demands, while simultaneously maintaining robust cybersecurity measures and keeping up with technology and industry trends.

With unrelenting pressure to digitally transform, many Credit Unions are turning to Managed Service Providers for IT advice, expertise, and ultimately, to engage a high trust partner to share the burden of responsible data ownership.

Hybrid Cloud offers optimal flexibility to remain competitive in the financial industry. The key value of cloud adoption is to bridge 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.

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.

Challenges

Data is the lifeblood of any business, but within the Credit Union industry, 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 and jump start stalled banking operations.

Data Integrity is a central component of Credit Union operations. Regularly tesfing the security controls (the access to data, breach detection, response to incidents, and monitoring the systems, networks, and environments) will determine if Risk Assessment recommendations have been successfully implemented. Even when security risks are identified in the Risk Assessments/ Penetration Test report recommended by the FFIEC, many Credit Unions fail to properly rectify each and every security insufficiency found.

Due to the difficulty in 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. The expertise required to solve configuration puzzles between systems/networks/environments and limit the downtime associated with upgrades, patching, and maintenance is usually more than a single branch can afford.

Solutions Expertise for a Disciplined Approach to Secure Member Data and Cybersecurity Management

1. Assessment and Recommendations for existing security, systems, and network controls. (**Security Posture Assessment**)
2. 24/7/365 Security Monitoring – Defend Against and Respond To any potential infiltration of environment. (**Security Monitoring**)
3. Reduce the turmoil of running disparate systems with asset identificafion and uniform policy controls during mergers or acquisitions of additional branches. (**Endpoint Management/Systems Total Care**)
4. Balance Cloud environments based on sensitivity of data and workloads and use vendor-agnostic/best-option integration of tools and hardware into Hybrid Cloud environments. (**Hybrid Cloud journey**)
5. Secure data backups and data recovery with multiple locations and redundancy. (**Backup as a Service and Disaster Recovery as a Service**)
6. Remote work capabilities with contact centers and centrally managed workstations. (**Unified Communications and Desktop as a Service)**
7. Fulfill FFIEC compliance recommendations. (**Pen Testing/Risk Assessment/Vulnerability Assessment**)

About Us

With almost 25 years in the IT industry, TBC offers broad business management expertise as well as main SOC2 certifications. With our
"As a Service" models, customized to the unique needs of the financial industry, organizations can rely on support through the rapidly changing demands of delivering financial services securely, efficiently, and professionally.

TBC manages technical intricacies of credit unions with the rigorous standards demanded by their members. Our IT teams are highly qualified to manage and support technical and security operations so you can focus on growing your business.

You can expect white glove service and a true partnership with TBC to power the back-end technology needed to ensure robust cybersecurity and service delivery with confidence.