Quantum Secure and Banking Institutions

ABOUT OUR CLIENT

Our client is a U.S. regional banking corporation headquartered in the Midwest. The company’s main businesses include branch banking, commercial banking, consumer lending, payment processing, investment advising, and title insurance.

One of the top-performing banks in the United States, our client is a Top 15 super-regional U.S. bank with 1,400 branch offices, 110 operation centers and 23,000 employees in 14 states.

VISION AND REQUIREMENTS

The main goal of our client’s security team is to minimize the overall risk posture of the organization with regards to the physical and logical security of the organization. To ensure this, they needed a solution which could manage the lifecycle of the physical identities and ensure efficient policy-based physical access operations with sufficient internal governance and audit controls built-in. The bank had multiple disparate systems and devices which were operating independently of each other. Therefore, they had the following key requirements for its physical security infrastructure when it comes to managing physical identities and their access:

Interoperability of Authoritative and Security Systems

The bank’s security team lacked a consolidated view into the physical security infrastructure of the organization which prevented them from managing the growing safety and security infrastructure and impacted the facility access and operational needs of the organization’s employees, contractors and vendors. This was due to a lack of standardized policies, reporting, planning processes, documentation and tools to protect people, information and facilities across 110 operations centers in 14 states.

Managing Access Lifecycles for Multiple Stakeholders

The bank has multiple stakeholders (employees, visitors, contractors) with varying risk profiles and access requirements accessing the organization’s premises. The entire process of onboarding, performing background checks, provisioning access to off-boarding was done manually which led to a slow and error-ridden process.

Common Notification and Escalation Procedures

A complex relationship existed amongst the identities and their configuration rules for the multiple access zones/levels and the access approval/termination rules were all managed manually, resulting in human errors and making it extremely difficult to track and monitor access-related activities. For instance, if an approver was not available, the identity had to wait multiple days to be granted access.

To solve this problem, the bank needed standardized criteria for activation, communication and escalation including all tools to ensure compatibility.

Ability to Track Physical Assets Centrally

Beyond ensuring that every employee, contractor and vendor is authenticated at all times and their physical access needs are controlled and managed, the bank also wanted to ensure that the physical assets such as metal keys or credentials are linked to the respective identities and tracked by security practitioners using automated means to dramatically reduce human errors, ensuring that compliance needs are met and creating an overall higher level of security.

Common System Architecture and Design

The bank has multiple identity-based systems which store data for the same person but due to lack of proper integration, data exchange happens through manual interactions. These solutions also had limited or no integration with authoritative and logical security systems. As a result, there were huge operational inefficiencies, delays and a high state of risk to potential security exceptions.
THE QUANTUM SECURE SAFE SOLUTION

SAFE Software Suite offers automation of physical identities along with their related physical access enforcing complex policies and rules to streamline access operations.

The bank selected Quantum Secure’s SAFE Physical Identity and Access Management (PIAM) Solution to automate their existing manual processes associated with the access and identity lifecycle management resulting in faster processing times and better audit controls. Some of the key components of the SAFE Solution offered to the bank are:

Provide Integration and Interoperability of the Siloed Physical Security System
SAFE provides ready-to-use connectors (agents) which integrate with the external disparate PACS present at the bank (Picture Perfect) and authoritative system (ADP, HR SAP) to provide a common centralized security platform. With the ability to communicate across devices and systems, SAFE delivers the bank with a unified comprehensive view of the security and provides seamless processing of identity information from the PACS to SAFE.

Automate the Entire Physical Identity Lifecycle Management
At the bank SAFE automatically synchronizes person, card, and access rights information with building access systems. SAFE allows employees, contractors and vendors to gain role-based access to their facilities based on standardized on-boarding and off-boarding processes in SAFE. SAFE also enables the bank’s security managers to create and automate standard security processes and policies to grant, manage, revoke and provision physical security identities and access privileges across multiple sites.

Automate Physical Asset Management Needs
SAFE Asset Manager for the bank handles all physical asset management needs, such as attaching assets to identities, tracking those assets across the identity lifecycle and providing comprehensive reporting and resolution capabilities. SAFE Asset Manager allows the security and operations departments to manage all aspects of their physical assets — all tied to a single identity.

BENEFITS

The SAFE Solution has replaced the bank’s manual processes associated with personnel on/off-boarding, card issuance, access assignments and provisioning in PACS so that new personnel can be on-boarded and operational in minutes. SAFE ensures the access is revoked as soon as the employee, contractor or vendor leaves the organization and thus safeguards the facilities and critical infrastructure.

With SAFE, the staff can ensure that identities have access to authorized areas and facilities as per their role or contract, which is critical when managing a large financial organization system. Automating identity management has freed staff to work on more challenging projects, rather than routine task administration. In addition, the risks associated with human errors, inadvertent access grants and not terminating access on time were all eliminated.

To summarize, the overall benefits delivered to our client by utilization of Quantum Secure SAFE are:

> Centralized Security Administration and Operational Flexibility: SAFE’s policy-based physical security access management solution provided the bank with operational agility and created a “one-stop” management point for security managers and administrators to manage multiple identity types. This ensured that the “Who”, “Where” and “Why” of identity access was established at all times. This caused reduction in operational costs and improved the security posture across multiple facilities.

> Enhanced Operational Efficiencies: With SAFE providing automation of the otherwise manual tasks and system interoperability, physical access processes, such as access approvals, are completed within minutes without any delay, improving their operational efficiencies.

> Substantial Reduction in Operation Costs: SAFE reduced manual interventions such as paper-based request forms and additionally, automated reports for security and business units to analyze traffic and be able to make informed business decisions.

> Auditing and Compliance: SAFE delivered a 100% automated environment for Reporting and Assurance in accordance with government/industry compliance standards.

> Future-proofing Security Operations: With the dynamic and agile policy-based SAFE system, the system is now free to introduce workflow changes, new rules/policies across diverse set of identities, access management and compliance. The physical security computing environment is also flexible due to SAFE, as the integration challenges with newer systems and technologies are eliminated.