Case Study

A Leading Global Bank Strengthens Its Cybersecurity Resilience in the Quantum Era

SANDBOXAQ

The global financial industry has become acutely aware of the threat of quantum computing to cryptographic security. It is within this context that a prominent global financial institution embarked on a mission to modernize their cryptography management, including their capabilities to observe, control, govern, and update cryptography. In doing so it set an example for similar institutions that will eventually embark on the same journey.

Cryptography on the Rise

At the very outset, bank leadership had two critical insights. Understanding the growing importance of cryptography, it created a dedicated team within the cybersecurity group. The bank's cryptography security team's main responsibility was to oversee the use and evolution of cryptographic standards within the bank, something that, until then, had remained a black box.

They also understood that cryptography was not just about algorithms and their use, but about attributing, correlating and enriching a cryptographic inventory with metadata, such as assets, teams, and owners.

The bank created a central platform that not only included the cryptographic inventory but also enabled the organization to flag security gaps, identify owners, correlate use of objects across different assets and manage a lifecycle of issues across the organization

Lack of Visibility and Inventory

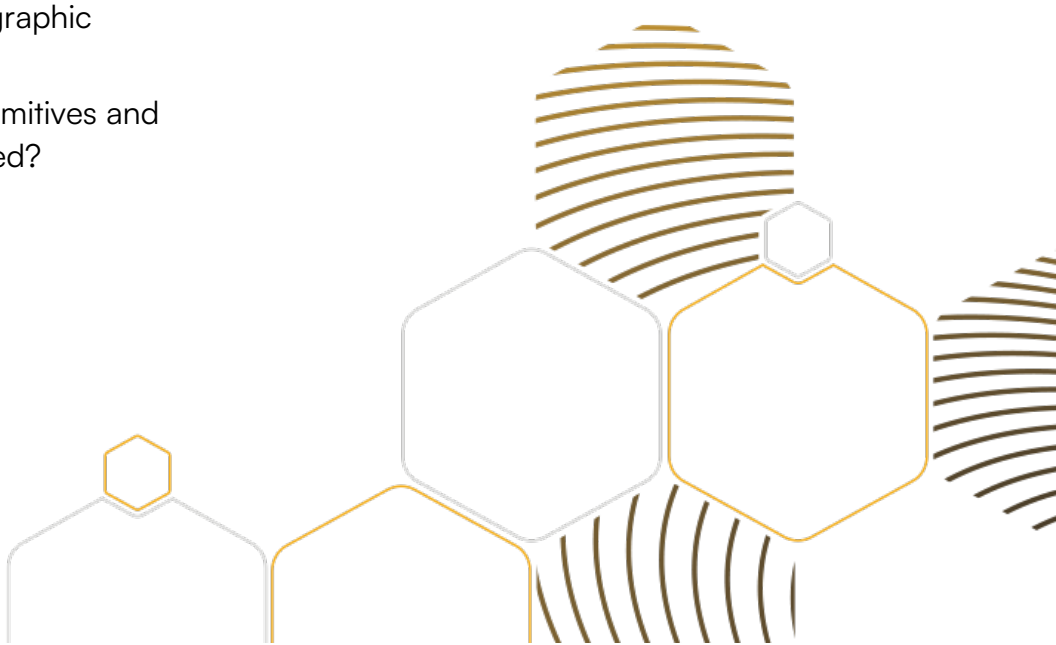
The organization faced its initial challenge in the form of insufficient visibility into their existing cryptography infrastructure. The team grappled with limited insights at every level of core infrastructure, including hosts, networks, and applications. This made it challenging to understand the state of cryptographic sprawl and potentially unidentified attack surface areas of their digital assets. In addition, despite having disparate cryptographic solutions in place in some lines of the business, the bank needed to ensure that their cryptographic standards were applied consistently across their extensive IT infrastructure.

Key questions for the cryptography security team were:

- Who are the owners of these assets, responsible for eventually fixing identified vulnerabilities?
- Which assets were associated with cryptography use, including assets using the same cryptographic objects?
- What cryptographic primitives and libraries were being used?

To address these questions and assess cybersecurity risk posture, the team set out in search of a solution that could offer comprehensive visibility into their cryptography. They were looking for enterprise software that would answer these questions while integrating seamlessly with their existing IT management systems and automation workflows.

To address these questions and assess their cybersecurity risk posture, the team set out in search of a solution that could offer comprehensive visibility into their cryptography. They were looking for enterprise software that would answer these questions while integrating seamlessly with their existing IT management systems and automation workflows.



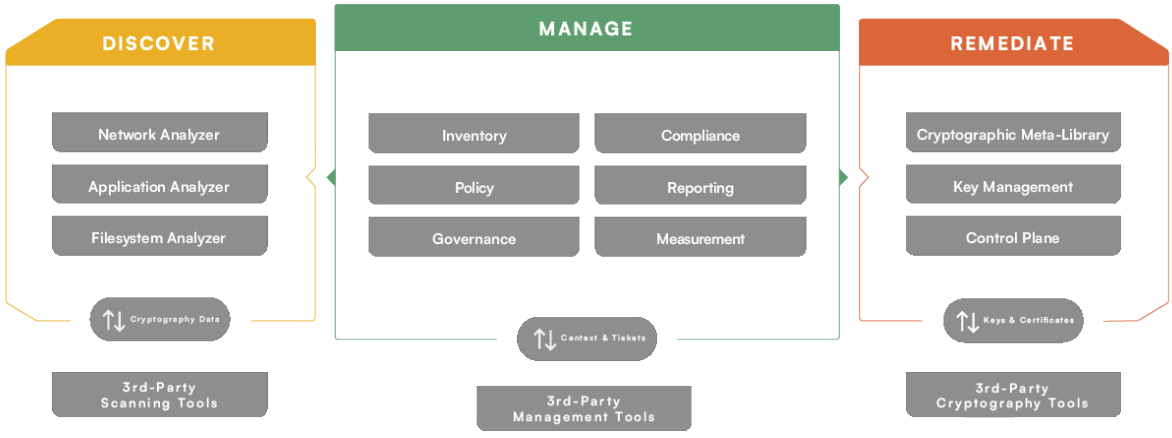
Leveraging SandboxAQ's AQtive Guard

The bank chose SandboxAQ to tackle their cryptographic challenges. The primary emphasis was on building a comprehensive inventory of their existing cryptographic infrastructure, a critical foundation for the adoption of post-quantum cryptography and the assurance of the highest level of data security.

The cryptography security team designed a scalable cryptography inventory platform architecture revolving around SandboxAQ's AQtive Guard. The goal was to create a cryptography data fabric, which aggregated cryptographic data from across the organization using different scanners, such as Filesystem, Network, and Application scanners. It enriched them with organization-specific metadata to make them actionable. One of the primary focuses while designing the solution was to ensure its scalability as the reach of the platform expanded throughout the organization.

During the deployment phase, SandboxAQ solutions and engineering teams provided invaluable support to the bank, enabling them to validate assumptions, and test automations. SandboxAQ's AQtive Guard empowered the organization's cybersecurity team to build a thorough and exhaustive cryptographic inventory that shed light on the details of their cryptographic sprawl, exposing vulnerabilities and gaps that demanded immediate attention. AQtive Guard's planned coverage will span all facets of the institution's IT infrastructure, including applications, file systems, and network protocols.

SandboxAQ's AQtive Guard Architecture



Unparalleled Cybersecurity Excellence

SandboxAQ's AQtive Guard facilitated the enforcement of cryptographic regulations, ensuring alignment with industry standards. In doing so, it not only underscored the organization's commitment to data security but also highlighted its dedication to regulatory best practices. Through their collaboration with SandboxAQ, the cryptography security team accomplished several significant milestones. They developed a profound insight into their cryptography, allowing them to formulate strategies for enhancing their cybersecurity stance.

These achievements included:

- Developing a scalable central cryptographic inventory platform.
- The ability to correlate assets that are using vulnerable cryptography.
- Identifying owners who need to take swift action when an issue is flagged.

This initiative was aligned with the interests of both the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), as it concurrently reduced risks and vulnerabilities while optimizing and automating operations. The proactive measures positioned the organization on the path to implementing post-quantum cryptography. As the global financial industry continues to confront new and evolving challenges, the bank is firmly committed to the pursuit of cybersecurity excellence.