Case Study

A Global Financial Institution's Path to Cryptographic Leadership

SANDBOXAQ

In the face of increasing demands for data protection and security imposed by regulatory authorities and governments, financial institutions find themselves compelled to implement and enforce new cryptographic policies. Post-Quantum Cryptography (PQC), is a critical factor, particularly in light of NIST's efforts to standardize quantum-resistant algorithms that are expected to conclude by 2024.

Financial services organizations currently lack the necessary tools for fully automating and scaling their cryptography compliance processes, whether it involves adhering to standards like FIPS, PCI-DSS, or enforcing internal security policies. Neglecting to address this challenge can result in substantial fines and potential compromises to the security of sensitive data.

This case study covers the strategic initiatives of a leading global financial services organization leveraging SandboxAQ's AQtive Guard to enhance their cryptographic management operations, achieve compliance, become agile, and execute targeted remediation.

Achieving Cryptographic Agility and Compliance

A modern cryptographic management system can create and maintain a comprehensive cryptographic inventory, and can adjust the security posture of the infrastructure in response to evolving compliance requirements and threats, without requiring significant infrastructure changes to ensure business continuity.

The customer's executives understood the significance of modern cryptography management and crypto-agility, facing rapidly changing threats and the upcoming migration to PQC. The cybersecurity team was challenged to comply with stringent cryptographic regulations set forth by bodies, such as the SEC. To address these challenges, the bank aimed to transition from legacy cryptographic methods to compliant standards while staying ahead of regulatory requirements.

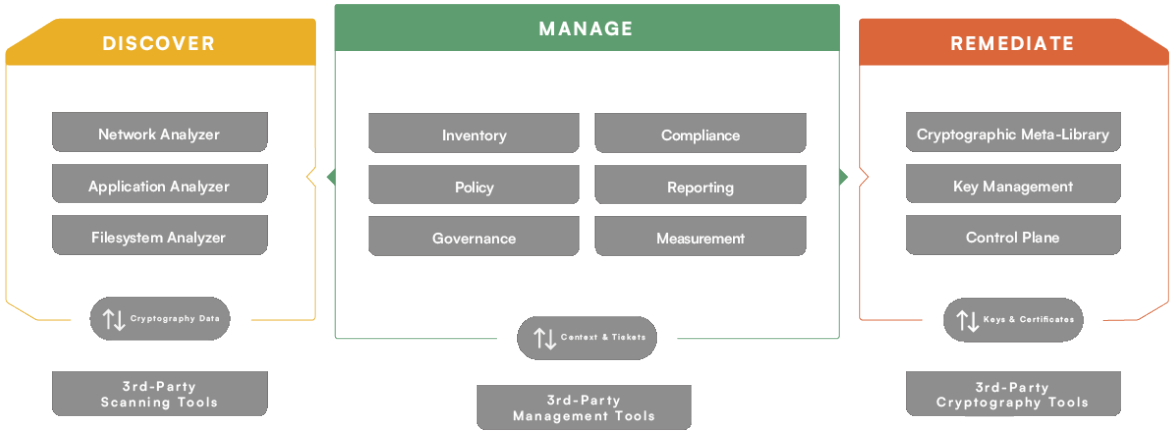
SandboxAQ's AQtive Guard

The looming threat of quantum computing and its potential to break existing cryptographic methods had been a growing concern for the company's leadership. They saw that an increasing segment of top financial institutions were actively investing in measures to safeguard their data from quantum attacks.

Following an exhaustive market benchmarking and Request for Proposal (RFP) process, the cybersecurity team chose SandboxAQ's AQtive Guard as the most mature product offering in the market, distinguished by the unmatched expertise of SandboxAQ's quantum security team.

The goal was to automate cryptography compliance for hundreds of thousands of endpoints, as well as databases, applications, perimeter components, and network elements.

SandboxAQ's AQtive Guard Architecture



Building A Comprehensive Cryptographic Inventory

To increase transparency and control over their cryptography, the team recognized the need to start building a comprehensive cryptographic inventory across their entire IT infrastructure.

By meticulously documenting their applied cryptography over two years the team gained deep insights into utilization patterns, leading to better decision-making.

Leveraging its robust cryptography discovery tools, and a versatile policy engine, designed to seamlessly align with top-tier IT management solutions, SandboxAQ's AQtive Guard was incorporated into the existing Endpoint Detection and Response systems and integrated into the Continuous Integration/Continuous Deployment (CI/CD) pipeline. AQtive Guard delivered substantial value to over a dozen internal teams, including DevOps, network security, risk management, and others, through a multi-phased rollout of functional and operational workstream enhancements.

The implementation began with the integration of Filesystem Analyzer with Tanium. Identified issues were exported to ServiceNow, and the resulting metrics were presented in comprehensive dashboards. In strict adherence to the organization's risk tolerance policy, the following risk mitigation measures are being implemented over the course of six quarters:

- **Implementing** comprehensive application tracers and scanners, spanning Binary, Container, and Cloud Scanning, ensuring full coverage.
- **Seamless integration** of additional certification management software, such as Venafi, to enhance cryptographic control.
- **Enabling** the generation of comprehensive dashboard reports that provide insights into the risk of network outages.
- **Developing**, refining, and piloting of governance strategies aimed at remediation and ensuring business continuity.

Cybersecurity Leadership

SandboxAQ's AQtive Guard met the unique needs of this financial services organization. The company strengthened its cryptographic posture, providing the cybersecurity team with enhanced visibility and control over cryptographic operations. AQtive Guard allows the cybersecurity team to smoothly transition away from deprecated cryptographic methods as required by new regulations or threats. They established a comprehensive cryptographic inventory that is automatically updated over time, providing the organization with valuable insights into their security risk posture. It enabled them to promptly identify and address misconfigurations, vulnerabilities and gaps. Improved compliance with policies and regulations was integrated into the company's DevOps toolchain and existing automated workflows.

The proactive measures against quantum threats provided peace of mind, ensuring the long-term security of their sensitive financial information.

SandboxAQ's AQtive Guard has helped this leading financial services organization bolster its cybersecurity resilience. It yielded a return on investment (ROI) within the initial six months of project implementation and enabled the cybersecurity team to stay ahead of evolving threats, uphold regulatory standards, and maintain the highest security benchmarks. SandboxAQ continues to support the organization in their journey towards cybersecurity leadership in the financial services industry.