SandboxAQ is developing an end-to-end crypto-agile Security Suite that will provide you with (1) full visibility and monitoring of your cryptographic security posture, (2) cryptographic policy management, and (3) deployment and enforcement of quantum-resistant cryptography protocols to protect your sensitive data effectively. Selected by NIST as one of the technology collaborators for the National Cybersecurity Center of Excellence, SandboxAQ is helping the government to initiate the development of practices to ease migration from current public-key cryptography algorithms to replacement algorithms that are resistant to quantum computer-based attacks. To ultimately provide you a way to effectively implement cryptographic agility across your network, our Security Suite is developed with three foundational pillars in mind:

**CONTINUOUS INVENTORY**
Analyze your network, hosts and data, and catalog your cryptographic inventory across your entire IT infrastructure. Identify vulnerabilities and cryptographic algorithms that do not adhere to your policy (e.g. FIPS140-2).

**POLICY MANAGEMENT**
Transition your IT infrastructure to agile cryptography with automation to maximize impact and reduce risk. Integrate and operationalize the solution in your staging environment. Comply with different cryptographic requirements without extra development or maintenance.

**ENFORCEMENT**
Perform live remediation via cryptographic algorithms and/or protocol switching, to immediately respond to vulnerabilities and out-of-policy algorithms, without having to reboot your operating systems or applications, minimizing costs and time.

**What does SandboxAQ’s crypto-agile Security Suite do?**

- Examine the traffic, hosts, infrastructure and applications across your IT continuously
- Obtain a continuous cryptographic inventory specific to your organization
- Monitor the performance of your cryptography
- Identify targets that are not compliant with your defined policies
- Remediate and enforce off-policy algorithms
- Switch cryptographic algorithms and protocols with minimal efforts,
- Educate your team to become post-quantum crypto-agile, and implement security risk mitigation best practices across your organization

COMING SOON

**COMING SOON**

- Remediate and enforce off-policy algorithms
- Switch cryptographic algorithms and protocols with minimal efforts,
How does our crypto-agile Security Suite work?

The core of our product is the Observability and Cryptographic Control Center, which manages all cryptographic uses across all or a subset of your IT.

The Observability and Cryptographic Control Center retrieves information from our Cryptosense module with three types of scanners that run on hosts and network devices: the Application Scanner, the Filesystem Scanner and the Network Scanner. These tools examine the traffic, file systems, and applications across your IT infrastructure to identify where cryptographic materials and algorithms are stored and used.

All this information, visualized in the Observability and Cryptographic Control Center, will allow you to create a cryptographic inventory. This automated and continuous inventory will give you full visibility into the artifacts, libraries, algorithms, protocols, and their application across your IT systems. On top of full visibility, the Observability and Cryptographic Control Center provides you with benchmarking tools that will allow you to monitor the performance of your cryptography throughout your IT infrastructure.

In addition, the Observability and Cryptographic Control Center allows you to define your policies (both standardized such as FIPS 140, PCI DSS, or custom). Once such policies are set, you will be notified of any use of cryptography that does not adhere to your policies. Finally, you will be able to use our host or network deployed Cryptoservice instances to perform remediation and automated enforcement to respond to policy violations in your system.

Security Suite

Reach cryptographic agility

Our platform will ultimately deploy optimized cryptography across your entire organization in a continuous manner, using Cryptoservice. This module will allow you to transition your IT infrastructure to future cryptographic requirements seamlessly, minimizing time and costs for your organization. Our platform will allow you to quickly comply with different cryptographic policies with minimal maintenance, helping you to achieve sovereignty over your cryptography.

SandboxAQ can educate your personnel on the methodology and technology, and train your teams on crypto-agility to test scenarios and automation. This way you can be sure that your organization is able to perform all critical phases and activities during the security lifecycle.