SANDBOXAQ

Post-Quantum Cryptography for the Public Sector

Quantum computing will disrupt major industries sooner than you think. Organizations across the globe are currently stepping up their investment in this technology to remain competitive and to ensure their survival in a post-quantum world. One critical factor that will affect every government agency is the impact of quantum computing on cryptography and data security.

Why You Need Quantum-Resistant Security Now

Quantum computers threaten the foundation of data architectures that rely on public-key cryptography, considered impossible for classical computers to break. In 2022, the White House issued National Security Memorandums-8 and -10, mandating federal agencies comply with quantum-resistant encryption algorithms and protocols approved by the National Institute for Standards and Technology.

Store Now, Decrypt Later

Store Now, Decrypt Later attacks pose an immediate threat to any sensitive data that is protected using public-key encryption. Data not secured with quantum-resistant protocols can be harvested, stored indefinitely, and then decrypted once an adversary has access to a large, fault-tolerant quantum computer. Everything from private constituent data to medical records and highly-classified national security information is vulnerable. It's not a question if this will happen, but simply, when.

SandboxAQ Protects Your Data Today

SandboxAQ employs the world's leading experts in post-quantum cryptography (PQC) software and hardware. Our proprietary AQtive Guard enables you to deploy quantum-resistant cryptography across your IT infrastructure, tailored to the specific needs of your organization. Our channel partners Accenture, Deloitte, EY and Carahsoft can support you at scale with the integration and operation of our PQC applications with a phased approach, according to your organization's size and mission needs. SandboxAQ AQtive Guard helps you maintain compliance, secure your networks, and protect sensitive data today and into the future.

SandboxAQ Deploys Across Your Entire Network

Encryption and Authentication of Endpoint Devices

Network Infrastructure Encryption

Big Data & ML DB SQL Security

Cloud Storage & Computing

Supervisory Control & Data Acquisition Systems

Your Roadmap For Quantum Protection

Public sector organizations need to begin planning PQC migrations right away. Our proprietary, crypto-agile framework enables you to replace public-key encryption algorithms with quantum-resistant algorithms. It also enables full sovereignty over the replacement process, so you can remain compliant as standards and protocols continue to evolve. Here is our recommended, phased approach:

01 DISCOVER

Analyze your IT infrastructure, catalog your cryptographic inventory, and perform a quantum-readiness evaluation to generate a risk-based PQC migration plan.

02 MANAGE

Identify and migrate selected encrypted objects from your IT infrastructure to quantum-resistant algorithms to demonstrate functional success and ensure performance. Catalog mitigation patterns that will become the standard for the full implementation.

03 REMEDIATE

Complete prioritized and phased transition of your IT infrastructure to a crypto-agile PQC framework to maximize the impact while focusing on reducing risk.

Partners

SandboxAQ is partnered with Accenture, Deloitte, and EY, three of the world's leading professional services organizations, who help us guide public sector customers through implementing transformative AQ solutions at scale.

accenture

Deloitte. EY

About SandboxAQ

SandboxAQ is an enterprise SaaS company combining AI and Quantum (AQ) technology to address some of the most challenging problems impacting society. Our products include quantum-resistant cybersecurity modules that migrate enterprises to higher levels of security. While our core team and inspiration formed at Alphabet Inc., we are now an independent, venture-backed company that delivers commercialized AQ solutions for organizations in the public sector, financial services, healthcare, life sciences, telecommunications, and other critical industries.

sandboxaq.com

publicsector@sandboxaq.com