

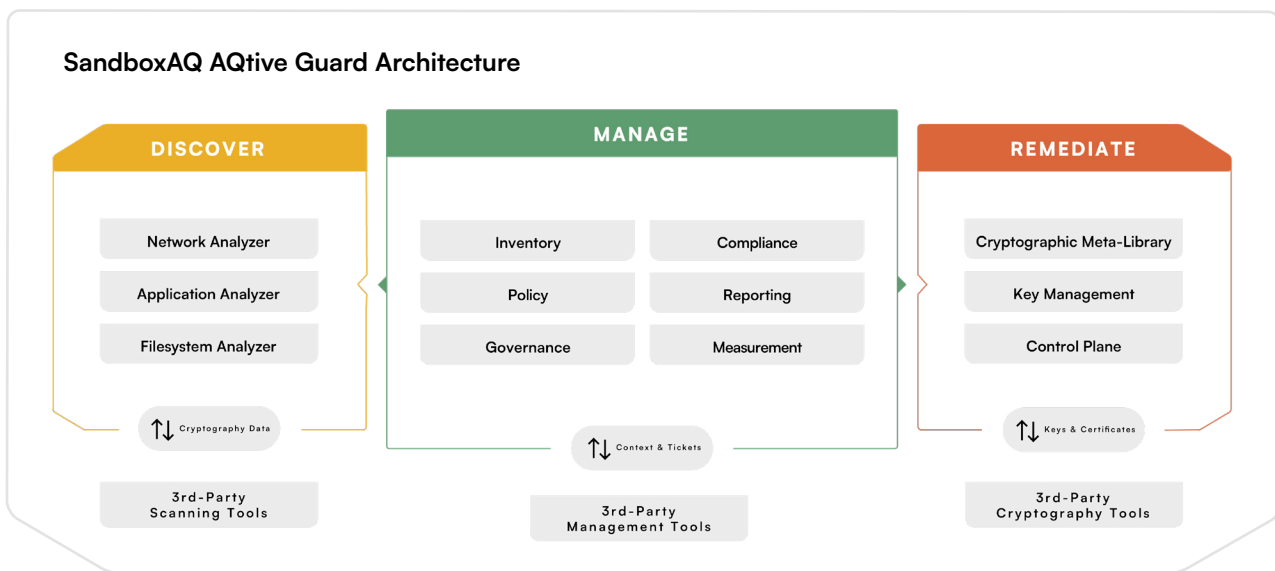


SANDBOXAQ | AQTIVE GUARD

SandboxAQ AQtive Guard is a unified cryptographic management software platform that provides a full range of services to achieve cryptographic agility.

AQtive Guard automatically analyzes and reports on your cryptographic security posture and policy management and enables your team to deploy and enforce new protocols, including quantum-resistant cryptography, without re-writing code or modifying your IT infrastructure.

By bringing cryptographic management into the agile and IT automation era, AQtive Guard will help your organization reduce risk and remain compliant with changing regulations, allowing you to seamlessly enhance your cryptography against current and future threats.



Discover

AQtive Guard provides valuable insights into your cryptography usage. Our analyzers capture snapshots of your cryptography triggered by your automated workflows, ensuring real-time visibility of your cryptographic inventory at intervals of your choice. By compiling information from three types of analyzers, AQtive Guard delivers comprehensive 360-degree visibility into your organization’s cryptographic inventory:

NETWORK ANALYZER

Captures network traffic and identifies cryptography used to protect data in transit.

APPLICATION ANALYZER

Detects all calls to cryptographic libraries made by an application at run time, identifying vulnerabilities and policy breaches.

FILESYSTEM ANALYZER


Scans files to find and parse cryptographic artifacts in data at rest.




Manage


AQtive Guard provides a dashboard view of your cryptographic inventory and includes benchmarking tools to monitor the performance of your cryptography.

 **Analyze** your comprehensive cryptographic inventory.

 **Cross-reference** cryptographic use in your network, applications, and filesystems.

 **Enable** remediation by integrating with JIRA, GitHub, IDE, and other DevOps issue tracking tools.

 **Monitor** cryptographic performance.

 **Identify** vulnerabilities and algorithms that do not adhere to policies such as FIPS 140-2, PCI DSS, or quantum-resistant cryptography. Integrate cryptographic inventory, analysis, and alerting into your CI/CD and DevOps toolchains for application tracing and monitoring.

Remediate

AQtive Guard enables remediation and supervised enforcement to respond to policy violations. Swiftly address vulnerabilities and out-of-policy algorithms through live remediation via cryptographic algorithms and/or protocol switching, avoiding the need for costly and time-consuming re-architecting or re-writing of operating systems or applications.

AQtive Guard is designed to be integrated into the CI/CD cycle. All scans and traces flow into a centralized database allowing insights to enhance triage and prioritization. The results can be seamlessly integrated into your custom dashboards and queried via our GraphQL API.

Reduce your organization's risk by transitioning your IT infrastructure to agile and automated cryptography management.

Adhere to new cryptographic requirements and switch among them without requiring additional development or maintenance.

Integrate and operationalize cryptography for deployment.

Remediate off-policy algorithms and enforce standards adapted, including post-quantum cryptography.

Achieve full sovereignty over your cryptography.

Future-Proof Your Security

Protect your organization's sensitive data from both current and future cyber threats. Developed by a global team of cryptography experts and enterprise software engineers, SandboxAQ AQtive Guard provides full visibility of your cryptographic security posture, policy management,

and deployment and enforcement of quantum-resistant protocols. With SandboxAQ you can achieve a high level of security, comply with standards, and prepare for the future of cybersecurity.