



Arxan Application Protection for Desktop & Server

Comprehensive Application Protection for Desktop & Server

Traditionally, software has either not been protected, or is only protected by passive techniques such as encryption. These techniques fall short of providing the security needed to prevent software piracy and tampering since they only provide a static one-time hurdle that hackers can quickly master and breach. The application has no further recourse when that single defense layer fails or is breached.

Desktop applications come in many forms on many platforms. They are susceptible to piracy and counterfeiting. While servers are typically considered safe behind a firewall, a growing number of server products require protection from both piracy and targeted malware. Examples of server products that are licensed and sold to customers include critical infrastructure servers that manage everything from financial payments, telecoms, utilities, and online video to automobile assistance systems, software license management servers, CRM systems and gaming servers. The applications on these servers are susceptible to piracy and counterfeiting, in the same way that desktop applications are vulnerable to compromise; especially as they become widely distributed in untrusted environments.

Arxan Protects

- Brand
- Revenue
- Data
- Code Integrity
- Intellectual Property

Arxan Prevents

- Malware Injection
- Tampering with Security Controls / Sensitive Functions
- Reverse- Engineering
- Unauthorize Access and Fraud
- IP Theft and Piracy

Comprehensive Code, Cryptographic Key & Data Protection

Arxan Application Protection for Desktop and Server features automated, comprehensive, yet customizable protection for high-end software. It actively defends, detects and deters application attacks, providing durable and resilient security to today's threat profiles, which can easily bypass license management security protocols. Many software-driven Global 500 companies are using Arxan Application Protection to successfully safeguard their software assets and preserve revenues.

It is flexible, easy to use and tailored to individual application requirements to offer precise control over the implementation of security protocols; scalable, supporting the ability to increase the level and complexity of protection; and, virtually impenetrable, with its thousands of multi-layered dynamic Guards at work 24/7. Arxan Protection for Desktop/Server is a proven commercial software protection solution for managed, interpreted and native code. It also interoperates with license management solutions like Flexera and others to fully protect applications against piracy.



DEFEND Against reverse engineering, tampering and any manner of theft



DETECT An attempted attack on the application code, or on another Guard



DETER Attacks with self-repair, custom responses, and alerts or by responding to runtime attacks with customizable actions

Arxan Code Protection

Arxan hardens the application with its patented guarding technology. It enables runtime application self-protection (RASP) tamper resistance and self-healing measures inside the applications using its unique Defend-Detect-Deter methodology. This not only protects against known types of threats but also detects if a critical asset is being compromised – regardless of the attack vector. This is done by inserting a set of interdependent units of code called Guards® into the application, without requiring any source code changes. These guards will:

Without RASP, external malicious apps can intercept the execution of genuine applications at runtime and modify them for nefarious activities.

Arxan's Code Protection enabled with RASP addresses today's sophisticated attacks. Arxan's Code Protection for Desktop and Server is the only durable binary-based application hardening solution across Windows, Mac OS X, .NET, Java, Android and Linux Desktop and Server platforms for x86/x64 architectures.

Arxan Cryptographic Key and Data Protection

Arxan Cryptographic Key & Data Protection uses a robust implementation of white-box cryptography. It combines mathematical algorithm with data and code obfuscation techniques to transform the cryptographic keys and related operations so keys cannot be discovered. The keys are never present either in either the static form or in runtime memory. Arxan Cryptographic Key and Data Protection protects:



- Static keys – Embedded in an application when it ships
- Dynamic keys – Generated on the fly at runtime
- Sensitive user-data

Arxan's Code, Cryptographic Key, and Data Protection work together, to provide comprehensive application protection for Desktop and Server apps.

Core Features & Benefits of Arxan Application Protection for Desktop & Server

- Granularity of protection and performance-tuning
- Layered network of protections, with no single point of failure
- Compatible with third party license management such as FlexNet, SafeNet, Reprise and others
- Point-click breach management
- RASP (Runtime Application Self-protection) measures
- Fast, automated diversification to prevent BORE exploits
- Probabilistic execution for additional security
- Authorized debugging of protected application
- Ability to directly edit and optimize Guards
- Command line interface for build integration
- Ability to automatically discover the functional hierarchy of an application
- Algorithmically strong
- Simple APIs for easy integration

