NOKOD
SECURITY

Govern and Secure your Low-code/No-code Apps & RPA

Gain control and build security into your low-code/no-code application and automation lifecycle.

Easy Adoption | Multi-Platform Support | Uniform Controls

Many enterprises struggle to manage and control the security of their low-code/no-code application and RPA development process. Amidst digital transformation and pursuing productivity and growth, their apps' vulnerabilities, compliance violations, and malicious activities often stay uncovered.

With Nokod Security's platform, you can now confidently and securely run your citizen developer programs and automation initiatives. Nokod seamlessly connects to low-code/no-code platforms like Microsoft Power Apps & Automate, UiPath, ServiceNow, OutSystems, and others to analyze your apps and automations for security issues during development and throughout their entire lifecycle.
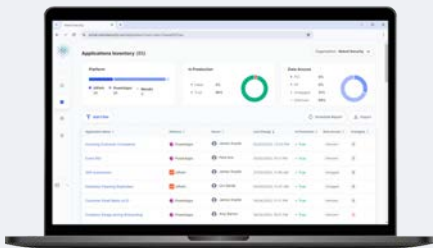
CONTROL AND GOVERN ALL YOUR LOW-CODE/NO-CODE APPLICATIONS

Maintain and track an up-to-date inventory of all your LCNC apps and RPA automations across all teams and development platforms.

Place all apps and automations under a uniform policy, within a single dashboard, for comprehensive visibility and control.

ENSURE YOUR APPS AND AUTOMATIONS ARE BUILT SECURELY

Detect security vulnerabilities and compliance issues in apps being developed and deployed.

Discover issues and risks such as hardcoded secrets, data leakage, injection vulnerabilities, and unpatched applications and components.
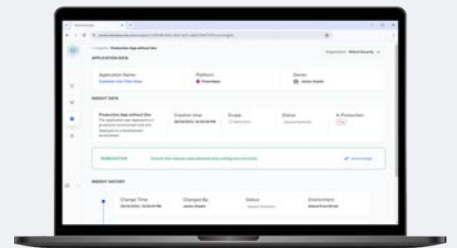
REMEDIATE AND MITIGATE ISSUES WITH EASE

When an application or automation violates of your organizational policies, your citizen developers receive clear remediation instructions.

If needed, your security team receives mitigation steps to put compensating controls in place.

"Before Nokod, we didn't know whether our teams were also using other low-code platforms. Nokod is now standard in our citizen development program, giving us full visibility and security over all our automations."

Automation Group Leader at Global Online Payment Provider

The Nokod Security Difference

Secure and accelerate your digital transformation journey and automation initiatives with Nokod Security's non-intrusive and agentless governance and security platform:

Secure, Stable, and Fast Discovery
Nokod's agentless platform uses simple API key registration processes and stable, compliant APIs from Low Code Application Platforms (LCAPs) to analyze their structure and find the right data about the applications, users, environments, and data connectors.

Nokod considers the most accurate and relevant information and, when possible, uses incremental updates to enable faster and more frequent data extraction and analysis.

Data Mapping and Application Inventory
The Nokod platform maps the extracted raw data to its own universal and platform-agnostic representation, allowing for a uniform set of rules and easy management across multiple LCAPs.

With this, you receive visibility into all your LCNC and RPA assets and environments in one platform.

Continuous Governance, Compliance, and Security Assessment
The platform continuously analyzes your apps and automations using different compliance, governance, and security engines, each processing the data to identify specific issues.

> **For example, the platform inspects the application logic to detect injection attacks, retrieves data access information to uncover compliance violations, integrates Nokod's proprietary threat intelligence to spot vulnerable third-party components, and inspects environments to discover user-defined misconfiguration.**

Policy Enforcement & Remediation
The Nokod platform continuously evaluates its findings according to the compliance, governance, and security policies created by its research arm. Detected violations and issues are shown as Insights in the platform.

Each Insight explains the findings and the policy that triggered it and offers remediation instruction for the business developer for straightforward fixing. The platform automatically updates Insights when fixes are applied.

Initiate Follow-Up Action
Define your preferred follow-up actions upon violations, such as sending information to a SIEM platform, ticketing system, or audit reports.

KEY BENEFITS & CAPABILITIES

» Maintain dedicated compliance, governance, and security policies for LCNC apps and RPA automations:
- Leverage Nokod Security's suggested policies
- Or customize for your company standards

» Monitor application ownership, history, and user permissions

» Map your data flows, sources, and types

» Control your data and prevent data loss with alerts of policy violations

» Automatically discover vulnerabilities and issues

» Detect and prevent:
- Application abuse
- Malicious apps
- Third-party attacks
- Injection attacks, and more.

» Generate reports to prove security control effectiveness

» Constant improvement through visibility into remediation and fixing trends

Nokod Security delivers expert and up-to-date threat intelligence to enable your organization to automatically detect, proactively prevent, and quickly respond to emerging cyber threats and vulnerabilities in the low-code/no-code application and automation era.