Rocket® software

Securing Low-Code Development in a High-Risk Digital World

A strategic guide for C-level leaders to protect applications without sacrificing agility

Contents

← Back to contents

Executive Summary

Low-code development is accelerating digital transformation across industries. By empowering teams to build applications faster and more collaboratively, low-code platforms deliver unmatched agility, drive innovation, and reduce development costs.

But more speed can create more vulnerabilities, which is why rapid innovation comes greater responsibility. As cyber threats grow more sophisticated — and many now using AI to automate and target attacks — the need for built-in, scalable security has never been more urgent.

Today's CIOs, CTOs, and CISOs must lead with a new mindset: low-code is an opportunity to embed modern security into every stage of application development, faster and more effectively than ever before.

Equally important is recognizing that security is a shared responsibility across the organization. Everyone — from business leaders to developers to operations — plays a role in ensuring applications are built and deployed with integrity. Complacency at any level introduces risk. Today's threat landscape means that proactive vigilance is mission-critical, not optional.

← Back to contents

The Evolving Threat Landscape

Today's enterprise applications operate in a dynamic, hyper-connected environment. From cloud integrations and mobile interfaces to third-party APIs and distributed infrastructure, the surface area for potential threats has grown dramatically. As a result, application-level security has become a critical priority for modern organizations.

What's more, adversaries are evolving. State-sponsored groups and cybercriminals are leveraging AI and automation to launch highly targeted, scalable attacks at unprecedented speed. These tactics are more adaptive, harder to detect, and increasingly effective at exploiting even small missteps in the software supply chain. This is why security-by-default is essential.

Low-code platforms play a vital role in enabling secure digital transformation. Their declarative, modular design makes it easier to build, test, and deploy apps consistently. But consistency alone isn't enough. To withstand today's advanced threats, organizations must elevate their defenses with proactive, runtime-level protections.

Why Executives Must Act Now

Relying on perimeter defenses like firewalls or access controls is no longer enough. Effective security requires a layered approach that includes application-level protection. For C-level executives, this means:

- **Proactively addressing software integrity** as part of the development lifecycle.
- **Ensuring traceability and trust** in how apps are built, deployed, and maintained.
- **Reducing human error** through automation and integrated checks.
- **Prepare for AI-enhanced threats** by adopting AI-resilient strategies.
- **Meeting evolving compliance standards** across global markets.

Low-code platforms, when combined with robust application certification, offer a powerful advantage: the ability to harden software pipelines without sacrificing speed or innovation.

Real-World Breaches: Why Integrity Matters

Solar Winds Supply Chain Attack 2020)

Attackers inserted malicious code into Orion software updates, which were digitally signed and distributed to 18,000+ customers. This proved that even trusted deployment channels can be exploited.
Lesson: One-time code signing isn't enough. Without runtime certification, tampered apps go undetected.

3CX VoIP App Attack (2023)

A compromised software library infiltrated a legitimate update of the 3CX desktop app. Despite being signed, the update extracted data after distribution.
Lesson: Post-signing tampering happens. Only runtime validation can catch it.

Codecov Bash Uploader Hack (2021)

An altered CI tool silently sent secrets to an external server. It went unnoticed due to lack of integrity checks in deployment workflows.
Lesson: Tools within your pipeline can become attack vectors if application certification isn't enforced.

← Back to contents

Key Principles for Securing Low-Code Applications

To effectively secure low-code environments, organizations should adopt strategies that balance simplicity with rigor:

01

Built-in security, not bolt-on.

Security must be embedded into the platform and processes, not added after the fact.

02

Application integrity at every stage.

Use mechanisms like digital signing and verification to ensure that what is deployed is exactly what was built — and nothing else.

03

Minimal attack surface.

Limit access to underlying code, enforce least-privilege roles, and remove unused components.

04

Auditability and compliance readiness.

Ensure all application actions and changes are logged and traceable.

05

Performance without penalty.

Security measures must be efficient enough not to disrupt user experience or development velocity.

← Back to contents

Real-World Challenges and Misconceptions

Many businesses hesitate to implement stronger security controls in low-code environments due to perceived barriers:

“We trust our internal teams.”

Trust is important — but mistakes, misconfigurations, and insider threats happen.

“We’ve never had a breach.”

Past performance doesn’t guarantee future safety, especially as threat vectors evolve.

“Security is too complex for our teams.”

The right tools make security seamless, reducing reliance on specialized expertise.

“It will slow down our releases.”

Done right, security checks can be automated and optimized for performance.

"It won't happen to us."

Attackers use automation to scan for any vulnerability. Even low-profile businesses and tools are targeted. Application certification acts as a proactive safeguard against both external and internal threats.

← Back to contents

A Modern Approach: Application Certification as a Security Enabler

A practical example of prevention in action.

To illustrate how application-level protection can be implemented effectively, consider the concept of **Application Certification.** Application Certification is a powerful, native safeguard that ensures only trusted, verified applications run in your environment. It's especially important as attackers automate tampering efforts using AI.

What it does:

- Packages an application for deployment and digitally signs it.
- Validates the application at runtime against the signed version.
- Blocks execution of any tampered or unauthorized code.

Why it matters:

- Prevents accidental or malicious changes.
- Supports compliance and audit requirements.
- Reduces risk of data exposure and system compromise.
- Adds a "trust layer" to your applications without adding friction.

The business value:

- Ensures consistent, secure deployments.
- Instills confidence in software integrity.
- Enables secure innovation in fast-moving low-code environments.

By embedding certification into the development and deployment workflow, organizations strengthen their security posture without slowing down delivery.

Low-code platforms like Rocket® Uniface accelerates development and gives organizations a chance to build more securely, more consistently, and more confidently than ever before.

As the sophistication of attacks increases — driven by automation, AI, and supply chain targeting — security must move closer to the application itself. Application Certification, runtime validation, and embedded governance are the foundation of modern software resilience.

In low-code, security can be your differentiator. With the right approach, it already is.

← Back to contents

How Application Certification by Rocket® Uniface Can Help

For organizations using Rocket® Uniface as their low-code development platform, **Application Certification** offers a streamlined, enterprise-ready way to implement strong security without hindering the development process.

Built-In Integrity and Trust

Rocket Uniface's Application Certification acts as a **digital seal of authenticity** for your applications. When an application is packaged for deployment, it is digitally certified using a secure, private key. At runtime, Uniface automatically checks the application's integrity. If any part of the application — code or configuration — has been altered, it will not run.

This means:

- Tampered or unauthorized code is immediately blocked.
- Only verified applications can execute.
- You maintain strict control over what enters production.

Simplicity Meets Strength

One of the most powerful aspects of Application Certification is its simplicity. It is built directly into the Uniface platform. There's no need for cryptographic expertise, custom scripts, or complex configuration. From a development team's perspective, certification becomes a natural part of the deployment process.

This lets your team:

- Improve security without altering workflows.
- Avoid the overhead of managing external security tools.
- Deliver secure, trusted applications at speed.

← Back to contents

Compliance and Audit Readiness

Application Certification also helps you meet internal and external compliance standards. Whether your organization is governed by industry-specific regulations (e.g., HIPAA, PCI-DSS, SOX) or general best practices for IT governance, certification provides:

- Documentation that only approved versions have been deployed.
- A technical safeguard aligned with risk mitigation policies.

Performance Without Compromise

Worried about impact on performance? You shouldn't be. The runtime integrity check is lightweight and highly efficient. **There is no perceivable degradation in application speed or responsiveness**, ensuring a smooth user experience alongside robust protection.

← Back to contents

In Summary

If your organization is looking to enhance application security and maintain compliance in a fast-moving development environment, Rocket Uniface's Application Certification is a smart, scalable solution. It brings together trust, simplicity, and automation, right where you need it most. And best of all, Application Certification is included in version 10.4.03 at no additional cost for current customers who are active on Maintenance.

Want to see it in action or learn how it fits into your environment?
Check out this short, and visit learn.rocketsoftware.com to learn more.

About Rocket Software

Rocket Software is the global technology leader in modernization and partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,000 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located around the world. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and X.

Learn more

Modernization.
Without Disruption.™

Rocket software

Visit RocketSoftware.com ›

MAR-14626_WP_UnifaceSecurity_V3