outsystems

Checklist: Security features to look for in cloud-native low-code platforms

How to evaluate cloud-native low-code platforms and modernize software delivery securely

You're ready to accelerate and modernize your organization's application development with a cloud-native low-code platform. But how can you be sure the solution you choose won't open the door to new risks?

While it's true that the dynamic and distributed nature of cloud-native architectures can create unique security challenges, they're not insurmountable. The key is to find low-code solutions that meet the most stringent compliance requirements while giving you complete transparency. You'll want to seek out a platform that uses the latest security practices and provides multiple tools to help you build secure apps, protect and anticipate cyber threats, and secure valuable data. Using this checklist as your guide, you'll learn the top emerging application development threats and get a comprehensive list of must-have cloud-native security features so you can choose a low-code platform with confidence.

Which risks keep you up at night?

Whichever cloud-native low-code platform you choose should give you peace of mind when it comes to protecting your data and preserving your organization's reputation and trust with customers, partners, and employees. Look for solutions that weave security into every aspect of their platform and application development. An ideal solution will be built to handle the most critical threats to low-code/no-code platforms and web applications—including the following identified by the Open Web Application Security Project (OWASP). The OWASP Top 10 is an industry-known awareness document for developers and web application security. It reflects a global consensus on the most pressing security risks that developers need to tackle to create safer, more resilient applications.

OWASP Top 10 Web Application Security Risks[1]	OWASP Top 10 Low-Code/No-Code Security Risks[2]
Broken access controls	Account impersonation
Cryptographic failures	Authorization misuse
Insecure design	Data leakage
Injection attacks (includes SQL injection and cross-site scripting [XSS])	Authentication and communication security
Security misconfigurations	Security misconfigurations
Vulnerable and outdated components	Injection handling failures
Identification and authentication failures	Vulnerable ready-made components
Software and data integrity failures	Data and secret handling
Security logging and monitoring failures	Asset management failures
Server-side request forgeries (SSRF)	Security logging and monitoring

[1] https://owasp.org/www-project-top-ten/

[2] https://owasp.org/www-project-top-10-low-code-no-code-security-risks/

5 core criteria for evaluating cloud-native low-code security

Once you know all your risks, you can start objectively comparing cloud-native low-code platforms. Organize your evaluation around these five core criteria, then check off each box so you know your vendor of choice will meet your security non-negotiables.

1. Assess a vendor's overall security posture

Each low-code platform vendor will offer different levels of security, compliance, and performance. The most secure platforms will have comprehensive and all-encompassing security policies. When fortified with a zero-trust architecture and the most stringent global and industry-specific compliance certificates, these platforms offer unparalleled security and reliability. The following features can help you avoid multiple OWASP risks, including vulnerable and outdated components, security misconfigurations, identification, authentication and communication issues, and data leakage.

- [ ] Shared responsibility model
- [ ] Zero-trust architecture
- [ ] Security policies and procedures
  - [ ] Risk management program and procedures
  - [ ] Data protection
  - [ ] Role or attribute-based access control with frequent and recurring access reviews
- [ ] Compliance
  - [ ] Global:
    - [ ] ISO 9001
    - [ ] ISO 27001
    - [ ] SOC 2
    - [ ] ISO 27017
    - [ ] ISO 22301
    - [ ] GDPR
    - [ ] ISO 27018
  - [ ] Industry-specific:
    - [ ] Trusted Information Security Assessment Exchange (TISAX)
    - [ ] Healthcare Insurance Portability and Accountability Act (HIPAA)
    - [ ] Payment Card Industry Data Security Standard (PCI DSS)
    - [ ] DORA (Digital Operational Resilience Act)
  - [ ] Administrative/regional:
    - [ ] Esquema Nacional de Seguridad (ENS)

2. Anticipate and prepare for any cyber event

Your IT team shouldn't have to tackle cyber threats alone. Top low-code platforms will help you detect and prevent unexpected activity and potential threats—with no impact on application performance. Look for the following features to reduce your risks for injection attacks (including SQL and XSS intrusions), vulnerable and outdated components, SSRFs, security logging and monitoring failures, and security misconfigurations.

- [ ] Web Application Firewall (WAF)
- [ ] Protection against DDoS attacks
- [ ] Endpoint detection and response solution
- [ ] Real-time antivirus
- [ ] Continuous automated intrusion detection
- [ ] Runtime integrity monitoring
- [ ] Vulnerability management
  - [ ] No downtime/no impact on UX
- [ ] Secure configurations, including CIS hardening (K8s, VM, etc.) and other cloud-level security configurations
- [ ] Logging across all components
- [ ] Security and capacity testing
- [ ] Secure secrets management
- [ ] Continuous platform hardening
- [ ] Mobile app hardening
- [ ] Network
  - [ ] End-to-end encryption
  - [ ] Access control on all interconnects
  - [ ] Network inspection and protection
- [ ] Disaster recovery
  - [ ] RTO 30 minutes, RPO 15 minutes
  - [ ] Test backup/restoration and report metrics
  - [ ] Multiple availability zones (AZs) with built-in redundancy

3. Build secure applications

Your organization must ensure that any applications it builds with a cloud-native low-code platform are secure by design and follow established security best practices. The right platform will help you mitigate broken access controls, cryptographic failures, insecure design, security misconfigurations, vulnerable and outdated components, identification and authentication failures, software and data integrity failures, account impersonation and security logging and monitoring failures. Seek solutions with:

- [ ] Intuitive, visual integrated development environment (IDE)
- [ ] Automated software development lifecycle (SDLC)
- [ ] Containers technology
- [ ] Isolated production, development, and QA stages
- [ ] Comprehensive Identity and Access Management (IAM)
  - [ ] Ability to incorporate SSO
  - [ ] Ability to assign users Least Privilege
  - [ ] Authorized device configuration options
  - [ ] Ability to separate administrators and developers
  - [ ] Token technology and mutual TLS (mTLS)
  - [ ] Bring your own identity provider (BYOIP)
- [ ] AI-powered security guidance on the go
- [ ] Mobile-specific security controls
- [ ] Full monitoring and observability

---

4. Protect your data

The low-code platform you choose must be ready to protect personally identifiable information (PII) and other highly sensitive data at all costs. Seek solutions with features that will mitigate the most common cloud-native risks, including data leakage, data and secret handling, cryptographic failures, software and data integrity failures, and authorization misuse.

- [ ] End-to-end data encryption
  - [ ] In transit
  - [ ] At rest
- [ ] Data protection controls
- [ ] Data protection tests
- [ ] Comprehensive access control to customer data
- [ ] Continuous incremental data backup
- [ ] Minimum 30 days backup
- [ ] Automatic database failover and recovery across multiple AZs
- [ ] Dedicated databases for each development stage
- [ ] Secure connections

5. Monitor and respond quickly

In a shared responsibility model, your vendor should be responsible for platform monitoring and security—while you retain security oversight for your applications. The best low-code vendors will continuously monitor their platforms and respond immediately in the event of a platform security breach. Features to look for include:

- [ ] Security Operations Center team
- [ ] 24/7 platform monitoring and response
- [ ] Access to 24/7 global support
- [ ] Alerts and notifications
- [ ] Security dashboard/reporting
- [ ] Iron-clad service-level agreements (SLAs)

Which cloud-native low-code platform checks all the boxes?

Embracing cloud-native application development can feel daunting, especially with the rapid growth of cybersecurity challenges in distributed environments. But don't let these concerns hold you back from modernizing your app development! By choosing a vendor with robust security practices tailored to your organization's needs, you can confidently elevate your development process and stay ahead in today's fast-paced digital landscape.

OutSystems is a cloud-native low-code platform that gives you enterprise-grade protection that exceeds modern security standards so you can build business-critical applications faster with total confidence.

Learn more about how the OutSystems low-code platform compares to other cloud-native solutions.

Learn more

outsystems