

Founders Pre-Launch Security Overview

Application Security

Raghunath Gopinath

September 25, 2026

1	Research References	2
1.1	UK Cyber Security Breaches Survey	2
1.2	Software Finder 2026 SaaS Security Report	2
1.3	IBM Cost of a Data Breach Report 2025	2
1.4	SaaSFort Enterprise Buyer Evaluation Data	2
1.5	Canadian Cyber 2026 SaaS Security Assessment Checklist	2
1.6	Lorikeet Security Enterprise Readiness Data	2
1.7	SaaS Buyer Guide 2026	2
2	The 12-Item pre-launch checklist for engineering teams	3
3	Why standard scanners are not enough?	5

1 Research References

1.1 UK Cyber Security Breaches Survey

Only 30% of businesses conducted a cyber risk assessment. 43% experienced a breach. Only 25% have a formal incident response plan. 14% hold personal data without protection.

1.2 Software Finder 2026 SaaS Security Report

52% of buyers choose vendors for certifications and data privacy posture. 57% replaced a SaaS provider over unresolved security issues. Trust centers cut conversion time by 32%; missing security packets add 26% to sales cycles. 68% of RFPs require MFA/SSO in base plans. 93% of CISOs call SaaS security a top priority.

1.3 IBM Cost of a Data Breach Report 2025

Average SaaS breach cost: \$3.9M. Cloud/SaaS breaches: \$5.17M. Average time to identify and contain: 277 days. AI-powered security tools reduce breach costs by \$2.22M on average.

1.4 SaaSFort Enterprise Buyer Evaluation Data

Vendors providing complete security evidence within 72 hours close deals 3–4 weeks faster. Five dimensions buyers check: external security posture, compliance framework mapping, evidence response speed, continuous monitoring proof, and remediation velocity.

1.5 Canadian Cyber 2026 SaaS Security Assessment Checklist

~70% of SOC 2 material findings relate to access control weaknesses. 15 areas enterprise buyers assess before signing. Missing or unverifiable credentials caused vendor disqualification in nearly half of competitive evaluations.

1.6 Lorikeet Security Enterprise Readiness Data

Enterprise security review typically takes 2–6 weeks. Penetration test reports produce the fastest sales impact (2–3 weeks vs 9–14 months for SOC 2). A \$10,000 pentest can deliver 15x ROI through revenue acceleration alone.

1.7 SaaS Buyer Guide 2026

67% of enterprises require SOC 2 Type II before approving SaaS. 94% of Fortune 500 mandate specific security protocols. 79% require SSO (increases ACV by \$4,200). 91% require MFA. 87% expect end-to-end encryption in regulated industries.

2 The 12-Item pre-launch checklist for engineering teams

1. Authentication and access control

- Enforce MFA where possible.
- Implement RBAC with least privilege.
- Require re-authentication for sensitive administrative actions.

2. Authorization on every data endpoint

- Verify ownership checks on every data retrieval path.
- Never trust client-side filtering.
- Test with multiple user accounts.

3. Input validation and injection protection

- Use whitelist validation on all inputs.
- Use parameterized queries.
- Sanitize output rendered in HTML contexts.

4. Encryption at rest and in transit

- Use AES-256 for data at rest.
- Use TLS 1.2 or higher for data in transit.
- Store secrets in key management services, never in code.

5. Session management security

- Use secure, httpOnly cookies.
- Set a reasonable timeout, such as 30 minutes.
- Properly invalidate sessions server-side upon logout.

6. Secure file upload handling

- Validate content type, not just the file extension.
- Enforce file size limits.
- Store uploaded files outside the web root.
- Scan files for malware when feasible.

7. Error handling

- Display generic user-facing error messages.
- Store detailed logs server-side only.
- Do not expose stack traces or system paths in responses.

8. Dependency audit

- Use tools such as `npm audit`, `pip-audit`, OWASP Dependency-Check, or Snyk.
- Track both direct and transitive dependencies.

9. Logging

- Log login and logout events.
- Log permission changes, data exports, and administrative actions.
- Use a structured logging format.
- Store logs in tamper-resistant storage.

10. Default credentials removed

- Change all default passwords.
- Remove test accounts.
- Disable debug endpoints.
- Review cloud service defaults.

11. Infrastructure hardening

- Restrict security groups and firewalls to required ports only.
- Separate development, testing, and production environments.
- Do not use public S3 buckets or equivalent publicly accessible storage.

12. Incident response preparation

- Maintain a documented contact list.
- Define a scope assessment procedure.
- Prepare a customer notification template.
- Test the incident response workflow.

3 Why standard scanners are not enough?

Most automated scanners (SAST, DAST) catch syntax-level vulnerabilities like SQL injection and XSS but miss authorization logic flaws - the category that accounted for **36% of vulnerabilities in deployed vite-coded applications** and is the most common source of cross-customer data exposure. The 2026 IOActive study found that industry-standard tools missed **97.8% of formally proven vulnerabilities** in AI-generated authentication and memory allocation code. For pre-launch verification, combine automated scanning with manual review of authorization logic and business-critical flows.