TENITTY

Security Blueprint

A practical picture of your security posture, the risks that matter, and what to do next.

Current state	Risk	Action
What is in place today?	What could matter most?	What should happen next?

For growing technology companies preparing to launch, scale, sell into enterprise, answer a customer security review, or simply understand where they stand.

01 / What this is

A security assessment built around useful questions.

The Blueprint gives a team a grounded view of its security posture without turning the engagement into a giant checklist exercise.

We look at the areas that shape real exposure:

Application & API	Authentication, authorization, sessions, business logic, input handling and exposed interfaces.
Cloud & infrastructure	IAM, network exposure, storage, secrets, configuration, logging and external attack surface.
Identity & access	Privileged access, service accounts, MFA, role boundaries and access lifecycle.
Data & security controls	Sensitive data flows, protection, retention, backups and operational controls.
Security operations	Logging, monitoring, vulnerability management and incident readiness.
Risk & requirements	Critical assets, threat context, control gaps and relevant customer or compliance requirements.

The exact depth and testing method are agreed during scoping. The Blueprint is not a substitute for a full penetration test where deeper exploitation is required.

02 / How it works

Five steps. No mystery.

01	**Discovery** Understand the product, business context, architecture and the question you need answered.
02	**Scope** Agree assets, access, testing windows, exclusions, authorization and deliverables.
03	**Assess** Review the agreed technical and security-control areas and validate important observations.
04	**Explain** Connect findings to evidence, realistic abuse scenarios and business impact.
05	**Roadmap** Prioritize the work and leave you with a sensible 30 / 60 / 90-day sequence.

A calm process, even when the findings are not.

Testing is performed only against assets and activities explicitly authorized in the agreed scope. If a critical issue appears during the engagement, it is communicated promptly rather than saved for the final report.

03 / What you receive

The output is meant to be used.

Executive summary	A short explanation of the important observations and what they mean.
Current-state assessment	The security areas reviewed, observations and relevant evidence.
Attack-surface view	Critical assets, exposures and trust boundaries identified during the engagement.
Prioritized risk register	Findings organized around severity, impact, treatment and ownership.
Remediation recommendations	Specific changes that can reduce the identified risk.
30 / 60 / 90-day roadmap	A practical sequence for moving from findings to action.

After the Blueprint

The Blueprint can stand alone, or become the starting point for deeper application testing, cloud review, remediation support, compliance readiness or a targeted retest.

Ready to start?
Tell Tenitty what you are building, what concerns you have and what you need to know. We will shape the scope around that.