GUARDIAN PLATFORM BRIEF

Guardian Katana Website and API Security Testing

Deeper active website and API assessment, evidence and tracked remediation for approved targets.

INTENDED AUDIENCE	Application owners, security teams, providers and digital businesses
PUBLICATION STATUS	Optional add-on - entitlement, target scope, assessment profiles and cadence apply

Beyond Core website monitoring

Guardian Core includes the approved baseline website vulnerability monitoring allowance. Katana is selected when deeper active website and API security testing is required.

Katana capabilities

- Approved website and API target management
- Scheduled and on-demand assessment workflows subject to entitlement policy
- Authenticated or custom assessment profiles where approved
- Normalised findings and customer-safe evidence
- High and critical remediation-action linkage
- Included rescans and rolling rescan allowances
- Provider and customer operational views

Commercial basis

- Approved websites and API targets
- Automatic assessment cadence
- Assessment profile and authentication requirements
- Manual-scan cooldowns
- Included rescans and rolling rescan allowances
- Separately scoped manual penetration testing where required

Governed boundaries

- Targets must be explicitly approved and tenant scoped.
- Assessment frequency and target limits are entitlement controlled.
- Credentials and raw request or result payloads are never exposed publicly.
- Availability depends on the approved deployment and service configuration.

Discuss Guardian with Damocles Security **damocles.com.au/contact**

This document is a controlled marketing foundation. Exact service coverage, commercial availability, data residency, response commitments and legal terms must be confirmed in the applicable proposal and agreement.