

GUARDIAN PLATFORM BRIEF

Guardian Platform Overview

One platform to see, prioritise and reduce cyber risk.

INTENDED AUDIENCE	Business leaders, security teams, MSPs and MSSPs
PUBLICATION STATUS	Public foundation - capability wording governed by the availability matrix

Security built around action

Guardian brings customer-safe security information, findings, risks, remediation actions, assessments, learning, dark web exposure monitoring, website vulnerability monitoring and reporting into one governed platform. It is designed to help organisations move from disconnected alerts to accountable security outcomes.

Guardian Core

- Guardian customer workspace and Security Dashboard
- Risk Register and All Actions
- Guardian University and Human Risk
- Guardian Dark Web Monitoring
- Guardian Website Vulnerability Monitoring
- Standard evidence and reporting
- Capability and integration status for licensed modules

Expand when required

- Guardian Assurance adds broader Vulnerability and Remediation.
- Guardian Managed Defence adds Security Operations and Aegis managed threat detection and response.
- Endpoint Protection includes managed operating-system and supported application patching for covered devices.
- DNS Protection adds managed DNS-layer policy, blocking and activity visibility.
- Katana adds deeper active website and API security testing beyond the Core website-vulnerability monitoring allowance.
- Infrastructure Assessment and Guardian Intelligence are controlled optional add-ons.
- Advanced or bespoke reporting may be separately priced.

Operating principles

- Real data only - no fabricated counts or trends.
- Customer-safe presentation with no raw scanner payloads or internal identifiers.
- Server-derived tenant and provider scope.
- Clear empty, unavailable and controlled-availability states.
- Traceable metrics and governed capability publication.

Discuss Guardian with Damocles Security

**[damocles.com.au/
contact](https://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.