GUARDIAN PLATFORM BRIEF

Guardian DNS Protection

Managed DNS-layer security policy, blocking, visibility and follow-up.

INTENDED AUDIENCE	Business customers, participants, providers and security teams
PUBLICATION STATUS	Optional managed module - protected scope, deployment and policy require commercial confirmation

Protection before connection

Guardian DNS Protection applies managed filtering policy and presents blocked, allowed and monitored activity through participant, business and provider-safe views.

Included managed service

- Managed DNS security policy
- Malicious, phishing and command-and-control domain blocking
- Agreed category and policy controls
- Blocked, allowed and monitored event visibility
- Available user and device attribution
- Participant, business and provider-scoped views
- Investigation context and Guardian action follow-up
- Customer-safe reporting

Deployment and scope

Coverage applies where DNS traffic is routed through the approved service or a supported endpoint deployment is active. Protected users, devices, sites, policy categories, exclusions, identity mapping and retention are confirmed in the package schedule.

Complementary control

DNS Protection complements endpoint security, firewalling and Security Operations. It is not represented as a replacement for those controls or as a guarantee that every malicious domain or event will be detected.

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.