

TECHNICAL PRODUCT BRIEF

Mobile application penetration testing

Test how the mobile app protects identities, data and trusted actions.

Why customers use this service

Test the application package, device behaviour and supporting API interactions to expose weaknesses in storage, transport, platform integration and business workflows.

What we assess

Application package	Build settings, embedded material and exposed components.
Local data	Sensitive information in storage, logs, backups and caches.
Authentication and sessions	Login, token storage, lifecycle and device-binding controls.
Platform interaction	Permissions, deep links, inter-process communication and web views.
Transport security	Certificate validation and protection of data in transit.
API authorisation	Object, function and role controls behind the mobile client.
Client trust	Resistance to tampering and unsafe reliance on client decisions.
Business workflows	Replay, sequence bypass and misuse of legitimate functions.

Engagement outcome

A prioritised mobile report with device and API evidence, affected data or functions, remediation guidance and retest results.

How the engagement works

How we test or review

Damocles inspects the supplied build on agreed devices, observes local and network behaviour, and correlates findings with architecture and supporting-API evidence. Static review and runtime validation are reported separately; device, build and root or jailbreak constraints bound conclusions.

Testing and review perspectives

Black-box mobile application user

Installs and uses the supplied build as an ordinary user while observing storage, permissions, links and network behaviour.

Included when: Used for behaviour available without instrumentation or source evidence.

Access: The exact package, test account, representative data and supported device or emulator.

Limitations: Conclusions apply to the supplied build, platform version and user path.

Instrumented test-device reviewer

Examines files, logs, IPC, runtime state and protection behaviour on an authorised instrumented or rooted test device.

Included when: Used where deeper device-side validation is included and technically possible.

Access: A dedicated test device, instrumentation authority, package and agreed root or jailbreak state.

Limitations: Instrumentation can change behaviour and does not prove resistance on every device or OS release.

Mobile architecture and supporting-API reviewer

Correlates device observations with mobile design, cryptographic decisions and approved supporting API behaviour.

Included when: Used where architecture or supporting interfaces are included.

Access: Data-flow diagrams, platform configuration, API endpoints and scoped client credentials.

Limitations: Document and API review are reported separately from behaviour observed in the app build.

Customer access or evidence typically required

The exact package, test account, representative data and supported device or emulator.; A dedicated test device, instrumentation authority, package and agreed root or jailbreak state.; Data-flow diagrams, platform configuration, API endpoints and scoped client credentials.

What you receive

A prioritised mobile report with device and API evidence, affected data or functions, remediation guidance and retest results.

Detailed technical coverage

Application package and build provenance

What is assessed	Damocles records package identifier, version, signing information, source channel and build hash for the exact application artefact tested.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for application package and build provenance.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to application package and build provenance.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Application package and build provenance when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled application package and build provenance; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Local storage

What is assessed	Damocles inspects application files, databases, preferences, caches and platform-protected storage for sensitive data and access controls.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for local storage.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to local storage.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Local storage when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled local storage; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Logs and backups

What is assessed	Damocles reviews application logs, screenshots, task snapshots and backup or restore behaviour on the supplied device.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for logs and backups.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to logs and backups.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Logs and backups when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled logs and backups; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Tokens and credentials

What is assessed	Damocles follows token and credential creation, device storage, use, renewal, logout and revocation across representative accounts.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for tokens and credentials.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to tokens and credentials.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Tokens and credentials when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled tokens and credentials; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Transport security

What is assessed	Damocles observes certificate and protocol behaviour for application traffic and tests transport enforcement through an authorised interception setup.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for transport security.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to transport security.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Transport security when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled transport security; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Platform permissions

What is assessed	Damocles compares requested platform permissions with feature use and tests behaviour when representative permissions are denied or revoked.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for platform permissions.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to platform permissions.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Platform permissions when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled platform permissions; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Exported components and inter-process interaction

What is assessed	Damocles enumerates exported components and approved inter-process entry points and invokes them with controlled intents or messages.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for exported components and inter-process interaction.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to exported components and inter-process interaction.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Exported components and inter-process interaction when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled exported components and inter-process interaction; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Deep links

What is assessed	Damocles opens approved deep links with valid and manipulated routes, parameters and calling contexts and observes destination and authorisation handling.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for deep links.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to deep links.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Deep links when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled deep links; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Cryptographic use

What is assessed	Damocles traces application use of cryptographic APIs, keys, randomness and protected storage using runtime and supplied design evidence.
Perspective / access	Black-box mobile application user. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Performed when current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Privacy-relevant behaviour

What is assessed	Damocles observes collection, display, storage and transmission of privacy-relevant data through representative user actions.
-------------------------	---

Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for privacy-relevant behaviour.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to privacy-relevant behaviour.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Privacy-relevant behaviour when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled privacy-relevant behaviour; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Runtime protections

What is assessed	Damocles evaluates anti-tamper, debugger, emulator and root or jailbreak responses only where runtime protection testing is included.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for runtime protections.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to runtime protections.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Runtime protections when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled runtime protections; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Supporting APIs

What is assessed	Damocles exercises supporting API authentication, authorisation and data handling with the mobile client identities and approved endpoints.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for supporting APIs.
Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to supporting APIs.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Supporting APIs when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled supporting APIs; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Device, jailbreak, root and build limitations

What is assessed	Damocles records device model, OS, build, instrumentation and root or jailbreak state and limits conclusions to those conditions.
Perspective / access	Black-box mobile application user. Assessment requires the exact application build, agreed device state, test accounts, representative data and supporting evidence, selected specifically for device, jailbreak, root and build limitations.

Evidence	Evidence records the package, device file, log, permission, IPC, deep-link, network or runtime observation relevant to device, jailbreak, root and build limitations.
References	Mobile Application Security Testing Guide 2.0.0
Applicability	Applies to Device, jailbreak, root and build limitations when the behaviour exists in the supplied build and agreed device configuration.
Limitations	The conclusion is limited to the sampled device, jailbreak, root and build limitations; conclusions are build and device specific; unsafe device, data and supporting-service effects are excluded.

Methodologies and standards

Mobile Application Security Testing Guide 2.0.0 — Uses MASTG 2.0.0 procedures selected for the supplied platform and build.

Mobile Application Security Verification Standard 2.1.0 — Uses agreed MASVS 2.1.0 verification objectives without implying complete MASVS coverage.

Common Weakness Enumeration 4.20 — Classifies confirmed weakness types using CWE 4.20.

Common Vulnerability Scoring System 4.0 — Calculates technical severity and records a CVSS 4.0 vector separately from customer impact.

Guidelines for Software Development June 2026 — Provides secure-development guidance relevant to the software procedure in scope.

Standards and control mappings

Information Security Manual June 2026 — supporting-evidence

References: ISM-1922

Assessed: Mobile application behaviours mapped to agreed MASVS areas.

Evidence: Mobile coverage records and confirmed findings for the supplied build.

Applicability: Only mobile application development and the supplied mobile build.

Limitations: Does not assess the complete development lifecycle or every MASVS requirement.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Mobile application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Coverage matrix

Records coverage matrix produced from the authorised Mobile application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Retest and residual-risk record

Records retest and residual-risk record produced from the authorised Mobile application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Build and device coverage record

Records build and device coverage record produced from the authorised Mobile application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Local storage and runtime evidence

Records local storage and runtime evidence produced from the authorised Mobile application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Mobile and supporting-API trace

Records mobile and supporting-API trace produced from the authorised Mobile application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Scope and safety limitations

- Only expressly authorised assets, identities, locations and activities are assessed.
- Higher-risk, disruptive, destructive and third-party activity requires separate written authority.
- Point-in-time evidence cannot establish continuous operation or conditions outside the engagement.

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

Review metadata

Owner: Technical Assurance

Last reviewed: 2026-08-10

Next review due: 2026-12-10

Scope this engagement with Damocles Security
damocles.com.au/contact

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

This brief supports engagement scoping. The authorised scope, rules of engagement and applicable agreement govern delivery.