

TECHNICAL PRODUCT BRIEF

External network penetration testing

Understand what an internet attacker can reach.

Why customers use this service

Test exposed hosts, services and remote-access paths to identify exploitable weaknesses that could provide an initial foothold or expose sensitive information.

What we assess

Internet attack surface	Hosts, ports and services reachable from outside the organisation.
Service security	Configuration, encryption and known weakness exposure.
Remote access	Authentication, MFA and post-connect security controls.
Public applications	Exposed administrative and supporting web interfaces.
Information exposure	Details that make targeting or exploitation easier.
Exploit paths	Practical routes from exposure to controlled access.
Detection opportunities	Observable activity that can support defensive improvement.

Engagement outcome

A prioritised report with validated attack paths, reproducible evidence, remediation guidance and retest results.

[How the engagement works](#)

How we test or review

Damocles reconciles internet observations with the authorised asset inventory, then safely validates exposed services from unauthenticated and supplied remote-user viewpoints. Configuration evidence is reviewed separately from live behaviour; denial-of-service, destructive exploitation and uncontrolled credential attacks remain excluded.

Testing and review perspectives

Unauthenticated internet attacker

Enumerates and interacts with approved public hosts and services from an ordinary external network without customer credentials.

Included when: Used for public discovery, pre-authentication behaviour and internet-exposure validation.

Access: Approved public ranges, hostnames, DNS zones, ownership boundaries and testing windows.

Limitations: Cannot establish authenticated, internal or source-restricted behaviour.

Authenticated remote-access user

Signs into an approved VPN or remote-access gateway and examines MFA, session establishment, assigned access and revocation.

Included when: Used only where post-authentication remote-access behaviour is included.

Access: A dedicated account, MFA method, client requirements and expected post-connect access.

Limitations: Conclusions apply only to the supplied identity, device posture and gateway path.

Perimeter configuration and ownership reviewer

Reconciles observed exposure with firewall, gateway, DNS, certificate and asset-ownership evidence.

Included when: Used when configuration or ownership records are supplied to explain external observations.

Access: Current exports, asset owners, expected services, source restrictions and third-party authority records.

Limitations: Configuration review is point-in-time and does not prove live enforcement unless separately validated.

Customer access or evidence typically required

Approved public ranges, hostnames, DNS zones, ownership boundaries and testing windows.; A dedicated account, MFA method, client requirements and expected post-connect access.; Current exports, asset owners, expected services, source restrictions and third-party authority records.

What you receive

A prioritised report with validated attack paths, reproducible evidence, remediation guidance and retest results.

Detailed technical coverage

Public attack-surface discovery

What is assessed	Damocles enumerates approved DNS zones and public ranges, correlates certificate names, hostnames and virtual hosts, and reconciles every discovery with the expected public asset inventory.
Perspective / access	Unauthenticated internet attacker. Approved public IP ranges, DNS zones, expected public asset inventory and ownership contacts.
Evidence	A discovered-asset record containing each name, address, certificate relationship and confirmed or unresolved ownership status.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed for customer-owned public ranges and zones expressly listed in scope.
Limitations	Point-in-time discovery cannot prove ownership or absence outside approved ranges; enumeration stops at third-party and rate-safety boundaries.

Exposed hosts and services

What is assessed	Damocles confirms listening ports, protocols, banners, product or version indicators, authentication surfaces and externally reachable management services on each discovered host.
Perspective / access	Unauthenticated internet attacker. Approved public targets, expected service inventory and, when reconciliation is included, read-only perimeter configuration evidence.
Evidence	A host-and-service record with address, port, protocol, observed service, response detail and management or authentication exposure.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed for reachable hosts inside approved public ranges.
Limitations	Service identification may be inconclusive when banners are suppressed; intrusive fingerprinting stops if service stability is affected.

Remote-access services

What is assessed	Damocles identifies unauthenticated portal and gateway exposure; with a supplied identity it tests authentication, MFA, session establishment, expected post-connect access and revocation, then reconciles results with supplied gateway configuration.
Perspective / access	Unauthenticated internet attacker; Authenticated remote-access user; Perimeter configuration and ownership reviewer. Approved gateway URLs or addresses, a dedicated remote-access identity and MFA method, expected post-connect access matrix, revocation contact and optional read-only gateway export.
Evidence	Portal responses, authentication and MFA results, session establishment evidence, post-connect connectivity checks, revocation result and cited configuration excerpts.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Authenticated procedures apply only when a dedicated test identity is supplied; configuration reconciliation applies only when evidence is provided.
Limitations	Credential spraying and lockout testing are excluded unless separately authorised; testing stops on account lockout, instability or unexpected production access.

Perimeter management interfaces

What is assessed	Damocles identifies internet-reachable administrative interfaces and protocols, tests their authentication surfaces and intended source restrictions, and correlates observations with supplied gateway or firewall policy.
Perspective / access	Perimeter configuration and ownership reviewer. Assessment requires approved public targets, dedicated identities where required, perimeter exports and ownership records, selected specifically for perimeter management interfaces.
Evidence	Evidence records the host, port, protocol, response, configuration or ownership evidence relevant to perimeter management interfaces.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Perimeter management interfaces when the described public service or boundary is authorised and present.
Limitations	The conclusion is limited to the sampled perimeter management interfaces; internet observation is point-in-time; disruptive, destructive and unauthorised assets remain excluded.

Authentication behaviour

What is assessed	Damocles exercises each approved external login surface for account enumeration, MFA behaviour, legacy paths, error differences and bounded lockout or throttling using dedicated identities where supplied.
Perspective / access	Authenticated remote-access user. Assessment requires approved public targets, dedicated identities where required, perimeter exports and ownership records, selected specifically for authentication behaviour.
Evidence	Evidence records the host, port, protocol, response, configuration or ownership evidence relevant to authentication behaviour.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Authentication behaviour when the described public service or boundary is authorised and present.
Limitations	The conclusion is limited to the sampled authentication behaviour; internet observation is point-in-time; disruptive, destructive and unauthorised assets remain excluded.

TLS and protocol security

What is assessed	Damocles negotiates externally available protocol and TLS versions, cipher suites and certificates, checks downgrade and legacy behaviour, and compares observations with supplied perimeter cryptographic settings.
Perspective / access	Unauthenticated internet attacker; Perimeter configuration and ownership reviewer. Approved public endpoints and, when configuration comparison is included, current TLS or service configuration.
Evidence	Negotiated protocol and cipher results, certificate chain details, downgrade observations and the corresponding configuration excerpt.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed for encrypted or security-sensitive protocols exposed by approved targets.
Limitations	Results describe the tested endpoint and time; no traffic interception, certificate replacement or disruptive protocol testing occurs without separate authority.

Known exploitable service conditions

What is assessed	Damocles correlates safely observed product, version and configuration indicators with verified exploit prerequisites, then performs controlled confirmation only where the rules of engagement permit it.
Perspective / access	Unauthenticated internet attacker. Approved targets, observed or supplied versions, relevant configuration evidence, exploit-safety constraints and an escalation contact.
Evidence	The observed prerequisite, affected service and version evidence, controlled confirmation result and any stopping condition reached.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed where reliable indicators match a known condition and confirmation is explicitly authorised.
Limitations	No destructive payload, persistence, denial of service or material data access is attempted; confirmation stops on instability or when the minimum proof is obtained.

Information disclosure

What is assessed	Damocles inspects banners, response headers, certificates, public metadata, exposed files and error responses for information that materially assists initial access.
Perspective / access	Unauthenticated internet attacker. Approved public hostnames, addresses and URLs, plus any known public-file exclusions.
Evidence	The exposed response, file, certificate, banner or metadata item with its target and retrieval path.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed only against content directly reachable from approved public targets.
Limitations	The review does not access third-party repositories or extract sensitive data beyond the minimum needed to confirm exposure; testing stops when customer or personal data is encountered.

Configuration exposure

What is assessed	Damocles examines externally observable default pages, management and diagnostic paths, exposed configuration files, service disclosures and relevant supplied perimeter settings.
Perspective / access	Perimeter configuration and ownership reviewer. Approved public targets and, where available, the expected service baseline and relevant perimeter configuration excerpts.
Evidence	The exposed page, path, file, response or configuration excerpt is retained with its public host and service context.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to externally reachable services and management surfaces named in the authorised target inventory.
Limitations	Only information exposed to the tested internet position or present in supplied configuration is assessed; no unauthorised file retrieval is attempted.

Chained initial-access paths

What is assessed	Damocles connects separately confirmed exposure, disclosure, authentication and exploit-prerequisite observations into a realistic initial-access path and validates only the least invasive step needed to substantiate the chain.
-------------------------	---

Perspective / access	Authenticated remote-access user. The approved public targets, dedicated accounts where needed, evidence from preceding procedures and explicit authority for the minimum confirmation step.
Evidence	An ordered path records each host, service, prerequisite, observation and controlled validation step leading toward initial access.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies when two or more confirmed in-scope observations create a credible initial-access sequence.
Limitations	The chain stops at the agreed proof point; Damocles does not establish persistence, pivot internally or assume unvalidated prerequisites.

Third-party ownership boundaries

What is assessed	Damocles reconciles discovered names, addresses and services with ownership records and stops active interaction when written authority cannot be established.
Perspective / access	Perimeter configuration and ownership reviewer. Assessment requires approved public targets, dedicated identities where required, perimeter exports and ownership records, selected specifically for third-party ownership boundaries.
Evidence	Evidence records the host, port, protocol, response, configuration or ownership evidence relevant to third-party ownership boundaries.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Third-party ownership boundaries when the described public service or boundary is authorised and present.
Limitations	The conclusion is limited to the sampled third-party ownership boundaries; internet observation is point-in-time; disruptive, destructive and unauthorised assets remain excluded.

Disruptive and credential-attack exclusions

What is assessed	Damocles records and applies scan-rate, credential-attempt, exploitation, destructive-action and denial-of-service boundaries before testing begins and whenever a stopping condition is reached.
Perspective / access	Unauthenticated internet attacker. Assessment requires approved public targets, dedicated identities where required, perimeter exports and ownership records, selected specifically for disruptive and credential-attack exclusions.
Evidence	Evidence records the host, port, protocol, response, configuration or ownership evidence relevant to disruptive and credential-attack exclusions.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Disruptive and credential-attack exclusions when the described public service or boundary is authorised and present.
Limitations	The conclusion is limited to the sampled disruptive and credential-attack exclusions; internet observation is point-in-time; disruptive, destructive and unauthorised assets remain excluded.

Methodologies and standards

Technical Guide to Information Security Testing and Assessment SP 800-115 — Uses NIST SP 800-115 guidance to plan, execute, analyse and report the authorised procedure.

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.

Standards and control mappings

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — contextual

References: Framework-level mapping

Assessed: The engagement produces point-in-time technical evidence about the configured and observed security behaviour within the authorised External network penetration testing scope.

Evidence: Coverage status, procedure results and findings can inform the customer's control assessment and risk treatment records.

Applicability: Framework-level context is provided when the customer uses NIST SP 800-53 to organise its security control program.

Limitations: No individual NIST control is published as verified; organisational implementation, continuous operation, governance and complete catalogue coverage remain outside the engagement.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised External network 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 External network 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 External network 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.

Public attack-surface register

Records public attack-surface register produced from the authorised External network 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.

Host and service evidence

Records host and service evidence produced from the authorised External network 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.

Initial-access path record

Records initial-access path record produced from the authorised External network 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.