

TECHNICAL PRODUCT BRIEF

Remote access and VPN review

Validate secure access from remote users and devices.

Why customers use this service

Review remote-access architecture, identity, device trust and post-connect controls to identify paths that could turn stolen credentials or an unmanaged device into internal access.

What we assess

Authentication and MFA	Identity checks, enrolment, recovery and bypass resistance.
Device trust	Posture, certificates and managed-device controls.
Post-connect access	Networks and services available after connection.
Segmentation	Separation of users, administrators, suppliers and sensitive systems.
Client and gateway security	Configuration, updates and exposed management services.
Credential lifecycle	Certificate, secret and account issuance and revocation.
Logging and response	Session traceability and useful security events.

Engagement outcome

A remote-access review with validated access paths, configuration evidence, prioritised remediation and validation results.

How the engagement works

How we test or review

Damocles evaluates portal exposure, identity and MFA behaviour, client posture, cryptography, routing and post-connect access using supplied remote identities and configuration evidence. Availability testing, uncontrolled credential attempts and production changes are excluded.

Testing and review perspectives

Unauthenticated remote client

Examines portal and gateway exposure, pre-authentication protocols and error behaviour.

Included when: Used for internet-facing remote-access entry points.

Access: Approved hostnames, addresses and testing window.

Limitations: Cannot establish post-connect access.

Authenticated remote-access user or managed device

Signs in with a dedicated identity and tests MFA, posture, routes, session access and revocation.

Included when: Used for approved post-authentication behaviour.

Access: Account, MFA, client or managed device and expected access.

Limitations: Applies only to that identity and device state.

Portal, gateway and identity-configuration reviewer

Correlates observed behaviour with gateway, certificate, identity, routing and logging configuration.

Included when: Used when configuration evidence is supplied.

Access: Exports, policies, certificates, route assignments and session logs.

Limitations: Configuration does not prove every live client path.

Customer access or evidence typically required

Approved hostnames, addresses and testing window.; Account, MFA, client or managed device and expected access.; Exports, policies, certificates, route assignments and session logs.

What you receive

A remote-access review with validated access paths, configuration evidence, prioritised remediation and validation results.

Detailed technical coverage

Remote-access architecture

What is assessed	Damocles maps portals, gateways, identity providers, client paths, trust zones and downstream dependencies.
Perspective / access	Authenticated remote-access user or managed device. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for remote-access architecture.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to remote-access architecture.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Remote-access architecture when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled remote-access architecture; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

Authentication and MFA

What is assessed	Damocles tests login, account enumeration, MFA enrolment and enforcement, recovery and bounded lockout behaviour with dedicated identities.
Perspective / access	Authenticated remote-access user or managed device. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for authentication and MFA.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to authentication and MFA.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Authentication and MFA when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled authentication and MFA; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

Certificate and credential lifecycle

What is assessed	Damocles follows certificate and credential issue, storage, renewal, expiry and revocation for representative remote users or devices.
Perspective / access	Authenticated remote-access user or managed device; Portal, gateway and identity-configuration reviewer. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for certificate and credential lifecycle.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to certificate and credential lifecycle.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Certificate and credential lifecycle when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled certificate and credential lifecycle; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

Client and device posture

What is assessed	Damocles tests approved device trust and posture conditions and compares compliant and controlled non-compliant client outcomes.
Perspective / access	Authenticated remote-access user or managed device; Portal, gateway and identity-configuration reviewer. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for client and device posture.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to client and device posture.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Client and device posture when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled client and device posture; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

VPN cryptographic configuration

What is assessed	Damocles reviews and observes VPN protocol, cipher, certificate and key-exchange configuration without disruptive downgrade testing.
Perspective / access	Portal, gateway and identity-configuration reviewer. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for vpn cryptographic configuration.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to vpn cryptographic configuration.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to VPN cryptographic configuration when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled vpn cryptographic configuration; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

Split tunnelling and routing

What is assessed	Damocles records split-tunnel policy, assigned routes, DNS behaviour and unintended local or internet path interaction.
Perspective / access	Portal, gateway and identity-configuration reviewer. Named source and destination test points, expected flow matrix and a safe test window.
Evidence	Source-to-destination results linked to rule, route or boundary evidence.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when both ends of the network path and the enforcing device are owned or expressly authorised for testing.
Limitations	Results cover the tested source, destination, protocol and route; testing stops on instability and does not authorise third-party or denial-of-service activity.

Post-connect segmentation

What is assessed	Damocles tests approved and denied post-connect destinations from a supplied remote client and records assigned identity and network context.
-------------------------	---

Perspective / access	Authenticated remote-access user or managed device. Named source and destination test points, expected flow matrix and a safe test window.
Evidence	Source-to-destination results linked to rule, route or boundary evidence.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when both ends of the network path and the enforcing device are owned or expressly authorised for testing.
Limitations	Results cover the tested source, destination, protocol and route; testing stops on instability and does not authorise third-party or denial-of-service activity.

Administrative access

What is assessed	Damocles examines portal and gateway administration paths, permitted sources, authentication and separation from user access.
Perspective / access	Authenticated remote-access user or managed device. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for administrative access.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to administrative access.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Administrative access when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled administrative access; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

Logging and session audit

What is assessed	Damocles traces representative authentication, session, access and revocation events into the supplied logging workflow.
Perspective / access	Authenticated remote-access user or managed device. Log-source inventory, representative event identifiers, workflow records and responsible contacts.
Evidence	Source-health state, event timestamps, investigation timeline and linked action or escalation record.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when the relevant telemetry and analyst or customer workflow can be observed during the review window.
Limitations	Absent or delayed telemetry prevents a detection conclusion, and observation of one event cannot prove continuous detection of all attacks.

Third-party access

What is assessed	Damocles samples dedicated third-party identities for sponsorship, access, expiry, device requirements and revocation.
Perspective / access	Authenticated remote-access user or managed device. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for third-party access.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to third-party access.

References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Third-party access when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled third-party access; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

Availability dependencies

What is assessed	Damocles identifies identity, gateway, network, DNS, certificate and provider dependencies that affect remote-access availability.
Perspective / access	Portal, gateway and identity-configuration reviewer. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for availability dependencies.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to availability dependencies.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Availability dependencies when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled availability dependencies; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

Revocation and emergency change

What is assessed	Damocles validates account, certificate and session revocation and reviews emergency-change and restoration procedures.
Perspective / access	Unauthenticated remote client. Assessment requires approved gateways, dedicated identities, MFA, test clients or devices, expected routes and configuration evidence, selected specifically for revocation and emergency change.
Evidence	Evidence records the portal response, authentication decision, certificate, assigned route, session, log or post-connect result relevant to revocation and emergency change.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Revocation and emergency change when the remote-access path and representative identity or device are included.
Limitations	The conclusion is limited to the sampled revocation and emergency change; results apply to supplied clients and identities; availability and uncontrolled credential testing are excluded.

Methodologies and standards

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — Provides Release 5.2.0 control context only where a verified mapping is declared.

Information Security Manual June 2026 — Provides ASD ISM control context only for the declared mapping and observed behaviour.

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 Remote access and VPN review 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 Remote access and VPN review 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 Remote access and VPN review 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 Remote access and VPN review 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.

Portal and gateway inventory

Records portal and gateway inventory produced from the authorised Remote access and VPN review 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.

Remote session and posture evidence

Records remote session and posture evidence produced from the authorised Remote access and VPN review 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.

Post-connect access results

Records post-connect access results produced from the authorised Remote access and VPN review 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 observations to agreed objectives as traceable technical evidence. The review is not a certification, does not establish complete compliance, and does not confirm 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 observations to agreed objectives as traceable technical evidence. The review is not a certification, does not establish complete compliance, and does not confirm controls outside the authorised scope.

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