

TECHNICAL PRODUCT BRIEF

Network-device hardening

Strengthen the devices that enforce network trust.

Why customers use this service

Review representative routers, switches and security appliances against an agreed baseline to identify weak administration, services, protocols and recovery controls.

What we assess

Administrative access	Identity, privilege and management-path restrictions.
Management services	Enabled protocols, interfaces and insecure legacy access.
Configuration baseline	Security settings, deviations and documented exceptions.
Network control plane	Protection of routing, switching and neighbour relationships.
Monitoring and time	Logs, SNMP access and reliable timestamping.
Software lifecycle	Supported versions, updates and known exposure.
Configuration recovery	Protected backups, integrity and restoration readiness.

Engagement outcome

A device-level hardening report with configuration evidence, baseline deviations and prioritised remediation actions.

How the engagement works

How we test or review

Damocles reviews device baselines and management-plane configuration and performs bounded protocol and access checks from approved management locations. Configuration review is distinguished from observed reachability; changes and load testing remain outside scope.

Testing and review perspectives

Management-plane tester

Attempts approved administrative reachability and protocol negotiation from permitted and non-permitted management positions.

Included when: Used to validate management-plane exposure.

Access: Test hosts, device addresses, protocols and expected access.

Limitations: No credential attack or load test is performed.

Device configuration reviewer

Examines AAA, privilege, services, SNMP, logging, time, control-plane and integrity settings.

Included when: Used for hardening assessment against the agreed baseline.

Access: Native configuration, software version, baseline and exceptions.

Limitations: Snapshot evidence does not prove continuous state.

Network operations owner

Explains operational dependencies, lifecycle constraints and approved exceptions.

Included when: Used where hardening choices affect management or availability.

Access: Ownership, support status, monitoring and change evidence.

Limitations: Operational statements do not replace technical evidence.

Customer access or evidence typically required

Test hosts, device addresses, protocols and expected access.; Native configuration, software version, baseline and exceptions.; Ownership, support status, monitoring and change evidence.

What you receive

A device-level hardening report with configuration evidence, baseline deviations and prioritised remediation actions.

Detailed technical coverage

Asset and software baseline

What is assessed	Damocles reconciles device inventory, model, role, software release, support state and approved baseline.
Perspective / access	Network operations owner. Assessment requires device inventory, native configuration, software state, agreed baseline, management test points and approved exceptions, selected specifically for asset and software baseline.
Evidence	Evidence records the device, setting, protocol, reachability, log, version or exception evidence relevant to asset and software baseline.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Asset and software baseline when the device role and relevant hardening control are included.
Limitations	The conclusion is limited to the sampled asset and software baseline; snapshot and sampled validation do not prove continuous state; changes and load tests are excluded.

Administrative authentication and AAA

What is assessed	Damocles reviews administrative authentication, central AAA, local fallback, MFA where supported and failure behaviour.
Perspective / access	Device configuration reviewer. Assessment requires device inventory, native configuration, software state, agreed baseline, management test points and approved exceptions, selected specifically for administrative authentication and aaa.
Evidence	Evidence records the device, setting, protocol, reachability, log, version or exception evidence relevant to administrative authentication and aaa.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Administrative authentication and AAA when the device role and relevant hardening control are included.
Limitations	The conclusion is limited to the sampled administrative authentication and aaa; snapshot and sampled validation do not prove continuous state; changes and load tests are excluded.

Role-based administrative privilege

What is assessed	Damocles maps administrator roles and command permissions and identifies unnecessary privilege or shared access.
Perspective / access	Device configuration reviewer. Assessment requires device inventory, native configuration, software state, agreed baseline, management test points and approved exceptions, selected specifically for role-based administrative privilege.
Evidence	Evidence records the device, setting, protocol, reachability, log, version or exception evidence relevant to role-based administrative privilege.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Role-based administrative privilege when the device role and relevant hardening control are included.
Limitations	The conclusion is limited to the sampled role-based administrative privilege; snapshot and sampled validation do not prove continuous state; changes and load tests are excluded.

Management-plane exposure

What is assessed	Damocles tests management-plane reachability from approved and representative non-management positions.
Perspective / access	Network operations owner. Assessment requires device inventory, native configuration, software state, agreed baseline, management test points and approved exceptions, selected specifically for management-plane exposure.
Evidence	Evidence records the device, setting, protocol, reachability, log, version or exception evidence relevant to management-plane exposure.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Management-plane exposure when the device role and relevant hardening control are included.
Limitations	The conclusion is limited to the sampled management-plane exposure; snapshot and sampled validation do not prove continuous state; changes and load tests are excluded.

Secure management protocols

What is assessed	Damocles reviews enabled management protocols, versions, cryptography, certificates and source restrictions.
Perspective / access	Network operations owner. Current configuration export or read-only access, diagrams, owners and representative validation endpoints; customer inputs must identify the approved secure management protocols targets and expected behaviour.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results; the record names the tested secure management protocols object, path or control and its observed result.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
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.

SNMP and monitoring access

What is assessed	Damocles examines SNMP versions, communities or users, access views, permitted sources and monitoring dependencies.
Perspective / access	Device configuration reviewer. Device configuration or read-only access, the configured SNMP version, communities or users, access views, permitted manager source addresses, and expected collectors or monitoring-platform ownership where applicable.
Evidence	An SNMP configuration excerpt records the configured version, redacted user or community representation, view and access restrictions, permitted sources, and a representative polling or reachability result where safe and authorised.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies when SNMP or equivalent monitoring access is configured or expected for a device included in the hardening scope.
Limitations	Secrets are excluded from public evidence and configuration review is point-in-time; monitoring infrastructure is not load tested and excluded monitoring systems are not assessed.

Logging and time synchronisation

What is assessed	Damocles checks security logging configuration, destinations, severity or facility where applicable, event detail, NTP or other time sources, timezone and representative timestamp consistency.
Perspective / access	Network operations owner. Device configuration or read-only access, expected log destinations and time sources, and a representative generated or existing event where available.
Evidence	Logging and destination configuration excerpts, representative event or receipt evidence where available, the configured time source, and a sampled comparison of device and log timestamps.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies when logging and time synchronisation are configured and included in the device-hardening scope.
Limitations	Configuration and sampled evidence do not prove uninterrupted future logging; Damocles performs no load test or deliberate clock manipulation, and external SIEM investigation workflow is outside this row unless separately in scope.

Control-plane protections

What is assessed	Damocles reviews control-plane policing, routing authentication and protections relevant to the device role.
Perspective / access	Management-plane tester. Assessment requires device inventory, native configuration, software state, agreed baseline, management test points and approved exceptions, selected specifically for control-plane protections.
Evidence	Evidence records the device, setting, protocol, reachability, log, version or exception evidence relevant to control-plane protections.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Control-plane protections when the device role and relevant hardening control are included.
Limitations	The conclusion is limited to the sampled control-plane protections; snapshot and sampled validation do not prove continuous state; changes and load tests are excluded.

Unused services and interfaces

What is assessed	Damocles identifies enabled but unused services, listening interfaces and physical or logical ports and verifies intended shutdown state.
Perspective / access	Management-plane tester. Approved ranges, names, locations and the expected asset or interface inventory.
Evidence	A discovered-item register with address, service, version or location and reconciliation status.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed for customer-owned ranges, names, locations or interfaces listed in the authorised inventory.
Limitations	Discovery is point-in-time and cannot establish ownership or absence outside the approved inventory; intrusive enumeration stops at the agreed boundary.

Configuration backup and integrity

What is assessed	Damocles reviews configuration backup, encryption, access, integrity checking, restoration ownership and recent evidence.
Perspective / access	Network operations owner. The configuration-backup method, storage location or platform, access controls, encryption where applicable, recent backup evidence, integrity or version information, and the restoration owner and process.
Evidence	A backup configuration or policy excerpt, recent backup timestamp and version, access-control and integrity evidence, and restoration ownership or procedure evidence.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies when device configuration backups form part of the operational hardening scope.
Limitations	Review of backup evidence does not prove every backup is restorable; production restoration is not performed unless separately authorised, and excluded backup repositories or platforms are not assessed.

Patch and lifecycle constraints

What is assessed	Damocles compares software state with support and patch constraints and records operational blockers without performing upgrades.
Perspective / access	Management-plane tester. Assessment requires device inventory, native configuration, software state, agreed baseline, management test points and approved exceptions, selected specifically for patch and lifecycle constraints.
Evidence	Evidence records the device, setting, protocol, reachability, log, version or exception evidence relevant to patch and lifecycle constraints.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Patch and lifecycle constraints when the device role and relevant hardening control are included.
Limitations	The conclusion is limited to the sampled patch and lifecycle constraints; snapshot and sampled validation do not prove continuous state; changes and load tests are excluded.

Hardening validation and exceptions

What is assessed	Damocles validates sampled hardening settings and records approved exceptions, owners, expiry and compensating controls.
Perspective / access	Network operations owner. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results; the record names the tested hardening validation and exceptions object, path or control and its observed result.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
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.

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 Network-device hardening 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 Network-device hardening 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 Network-device hardening 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 Network-device hardening 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.

Device baseline inventory

Records device baseline inventory produced from the authorised Network-device hardening 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.

Management-plane exposure results

Records management-plane exposure results produced from the authorised Network-device hardening 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.

Hardening exception register

Records hardening exception register produced from the authorised Network-device hardening 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.