ASD Essentials and the Essential Eight

In October 2026 the Australian Signals Directorate evolved the Essential Eight into ASD Essentials. Each action is rated, domain by domain, by assessment: not assessed, not effective, partially effective or fully effective. A supplier cannot rate its own product into your program, so this datasheet gives the evidence for your assessment: what Senua AI's software does for each action that applies to it as an asset in your estate, and where it sits in your program. It states the software as shipped on the issue date.

The software as an asset in your estate

Principle	Action, in short	How the software meets it	Status
GOV-11 Supplier cyber security assurance	Choose suppliers on a supply chain risk assessment; keep current assurance evidence	The standards pages and datasheets, the cryptographic register and the registry under NDA, reissued with each release	Met
GOV-08 Executive AI accountability	Executive accountability for the use and risk of AI	The software learns only from your own data, records the evidence behind every block and blocks nothing until an administrator allows it; a statement per product is planned	Partly met
GOV-14 Legacy system management	Treat unsupported technology	A published support lifecycle and end-of-life policy	Planned
PRO-01 Secure system lifecycle	Design securely; minimal default privileges; limit exposed services	One network listener; the engine listens only on the local host; report only by default; no default credentials	Met
PRO-16 Cyber supply chain security	Check the integrity and authenticity of software and updates before use; verify provenance	Every release signed with ECDSA P-384 and SHA-384 by a key that never leaves AWS KMS; your installed system verifies the next release before unpacking; a first install is pinned by its SHA-256	Met
PRO-16	Track supplier and component exposure through advisories	Advisories under a published disclosure policy; a bill of materials with each release	Planned
PRO-13 Identity, credential and access management	Remove default and unused accounts	No default account or password: the first credential is random, set on your host at first run, and works once	Met
PRO-13	Keep keys, secrets and tokens in secure repositories	Secrets sealed in the encrypted store; session tokens and API keys kept only as SHA-256 hashes; signing keys in AWS KMS	Met
PRO-13	Phishing-resistant MFA	One-time codes (RFC 6238) required for every privileged account today; passkeys and single sign-on planned	Partly met
PRO-13	Unique credentials per system and account	Named accounts; a secret per delivery destination; a key per install	Met
PRO-12 Least privilege access	Grant only authorised roles, with minimum privileges	Roles and capabilities enforced by the engine itself; a revoked capability fails on the next request	Met
PRO-05 Secure administration	Record every administrative action with user, time and target	A tamper-evident audit log: an HMAC-SHA-256 chain with a sealed anchor, so an edit, truncation or rollback shows	Met
PRO-04 Secure configuration management	Approved baselines; detect drift	Settings are declared and sealed, each change audited; a hardening guide is planned	Partly met

Principle	Action, in short	How the software meets it	Status
PRO-06 Vulnerability management	Patch within risk-based timeframes	Fixes ship as signed releases at no charge; you apply them on your timeframes	Met, with yours
PRO-07 Trustworthy software	Run only supported, verified, authorised software	Signed binaries at a fixed install path; the engine is decrypted only into the memory of a verified process	Met
PRO-10 Regular and proven backups	Back up important data to protected storage	What the software learns is an encrypted store you can back up, under a key you hold	Your environment
PRO-18 Network segmentation	Allow only approved inbound and outbound pathways	Nothing outbound unless you declare it; TLS 1.3 to a declared trust list or a pinned key; the licence works offline	Met
DET-01 Centralised event logging	Forward security events to central storage; protect logs	Events delivered by signed webhook, REST or email; the audit chain shows any change; a SIEM-ready format is planned	Partly met

Where it sits in your program

Domain	Priority phase	What the software does there
Boundary services	1	Sits at your web front door, behind your own nginx, HAProxy or Envoy, judging each request against your own learned normal; report only until you switch on blocking
Identity services	1	Sees sign-in traffic at that boundary, for detection of anomalous authentication activity (DET-02)
Visibility and response	All phases	Learns what normal looks like for your own systems and records the evidence behind every block, for triage (DET-02 to DET-04)

The Essential Eight crosswalk

ASD's transition guide asks organisations to keep meeting obligations that still cite the Essential Eight. Strategy by strategy:

Strategy	The software
Application control	Signed binaries at fixed install paths, stable per release, so they can be allow-listed
Patch applications	Fixes ship as signed releases at no charge
Configure Office macro settings	Not applicable: no Office content
User application hardening	The console sends a content security policy and refuses to be framed; no plugins
Restrict administrative privileges	Roles enforced by the engine; every privileged action audited
Patch operating systems	Your environment
Multi-factor authentication	Required for every privileged account (ISM-1173); phishing-resistant sign-in planned
Regular backups	Your environment; the learned store is encrypted under your key

About this datasheet

Senua AI's own assessment, against ASD Essentials for enterprise IT and Transitioning from the Essential Eight (October 2026). It is not an ASD rating or endorsement. Planned items carry dates on the assurance roadmap, senuaai.com/technology/standards/roadmap/. Questions and the registry under NDA: sales@senuaai.com.