snare

A PROPHECY SOLUTION

The Essential Eight Logging Breakdown

What Essential Eight Maturity Really Requires from Your Logging Architecture

Essential Eight Is Not Just About Controls

It’s About Evidence.

The Australian Cyber Security Centre Essential Eight framework is widely adopted across Australian enterprise and government environments.

Most organisations can describe their controls.

Far fewer can prove — with defensible evidence — that those controls are consistently monitored and enforced.

Logging is where **that proof lives.**

This breakdown clarifies what Essential Eight maturity actually demands from your logging and monitoring architecture.

Where Logging Directly Impacts Essential Eight

Following is a practical interpretation of logging requirements across key Essential Eight controls.

1 | Application Control

Essential Eight Expectation:

Only approved applications are allowed to execute.

Logging Implication:

- Application execution events must be captured
- Policy enforcement events must be logged
- Failed execution attempts must be traceable
- Historical logs must support audit validation

Without execution logs, application control cannot be proven.

2 | Restrict Administrative Privileges

Essential Eight Expectation

Privileged accounts are tightly controlled and monitored.

Logging Implication:

- Privilege elevation events must be logged
- Administrative session activity must be recorded
- Failed privilege attempts must be retained
- Audit trails must be tamper-resistant

At Maturity Level 3, logging integrity becomes critical.

3 | Patch Applications & Operating Systems

Essential Eight Expectation:

Systems are updated within defined timeframes.

Logging Implication:

- Patch deployment events must be logged
- Failed updates must be visible
- Configuration drift must be traceable
- Historical evidence must support audit review

You cannot validate patch compliance without system event visibility.

4 | Multi-Factor Authentication (MFA)

Essential Eight Expectation:

Strong authentication is enforced for privileged and remote access.

Logging Implication:

- Successful and failed authentication events logged
- MFA bypass attempts recorded
- Remote access events retained
- Identity infrastructure fully audited

Identity visibility is foundational to Essential Eight maturity.

5 | Regular Backups

Essential Eight Expectation:

Backups are performed and tested.

Logging Implication:

- Backup success/failure events logged
- Restore test activity recorded
- Administrative access to backup systems monitored

Without logging, backup validation cannot be independently verified.

The Maturity Gap Most Organisations Face

Many organisations:

✓ Implement controls
✓ Deploy tools
✓ Document policy

But:

✗ Do not monitor silent log failures
✗ Rely on SIEM retention limits
✗ Cannot replay historical raw events
✗ Have no tamper-resistance validation
✗ SIEM retention limits create forensic visibility gaps

Essential Eight maturity is not about deploying controls.

It is about proving they are operational.

Essential Eight Logging Maturity Quick Test

Ask your team:

- Can we detect if a critical log source stops reporting?
- Are administrative users prevented from altering log evidence?
- Can we retrieve raw logs beyond standard SIEM retention windows?
- Would our logs withstand regulator scrutiny?

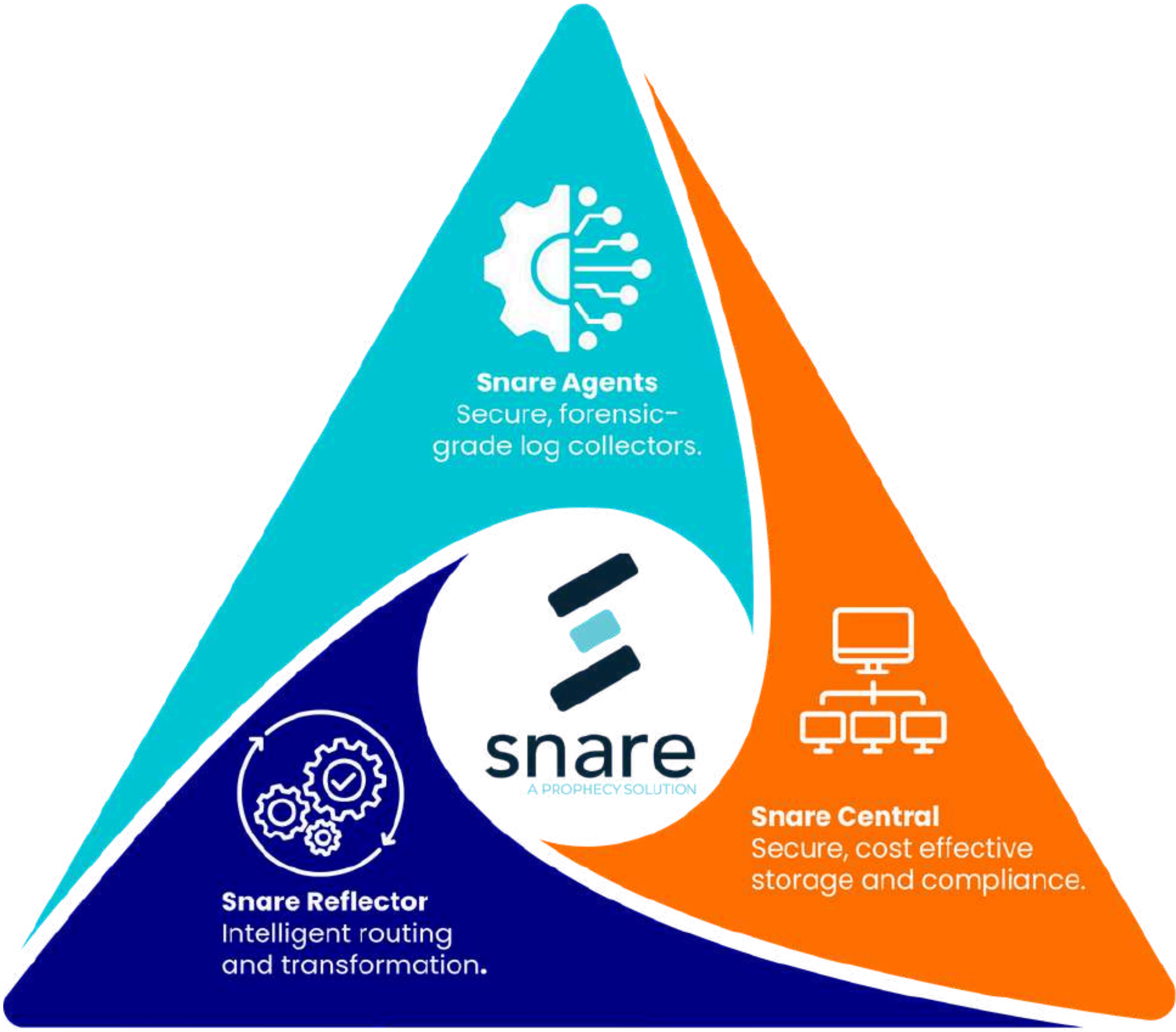
If the answer to any of these is uncertain, your Essential Eight posture may not be as strong as reported.

How Snare Supports Essential Eight Alignment

Snare strengthens Essential Eight maturity by enabling:

- Forensic-grade log collection at source
- Tamper-resistant storage controls
- Missing log detection
- Long-term retention independent of SIEM licensing
- Replay capability for investigation validation

Logging Shouldn't Be the Hard Part.


Snare Agents
Secure, forensic-grade log collectors.
snare
A PROPHECY SOLUTION
Snare Central
Secure, cost effective storage and compliance.
Snare Reflector
Intelligent routing and transformation.

Next Steps

Use this breakdown in your next Essential Eight review

Map your logging posture against maturity levels

Request an Essential Eight Logging Benchmark session

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com

snare
A PROPHECY SOLUTION