

A GATHID LABS SERIES: EPISODE 2

Government Compliance and The Essential Eight

Achieving Essential Eight Compliance: How Gathid Simplifies Identity and Access

Government agencies and organisations working with sensitive data face increasing pressure to meet and demonstrate compliance with the Essential Eight—the cybersecurity framework developed by the Australian Signals Directorate (ASD) to protect against cyber threats.

While many solutions focus on helping organisations implement the Essential Eight, few address the real challenge: proving compliance.

This is where Gathid makes the difference. By enhancing visibility, automating access reviews, and providing daily compliance insights, Gathid helps organisations rapidly demonstrate that their identity and access governance aligns with the Essential Eight's maturity requirements—without requiring invasive integrations or lengthy manual audits.

What is the Essential Eight, and Why Does It Matter?

The Essential Eight is a set of cybersecurity strategies designed to mitigate common cyber threats. It is the Australian Government's recommended baseline for securing IT environments.

The framework consists of eight core controls:

1. **Application Control:** Prevents unauthorised applications from executing.
2. **Patch Applications:** Ensures vulnerabilities are promptly addressed.
3. **Configure Microsoft Office Macros:** Blocks malicious macros that could compromise systems.
4. **User Application Hardening:** Limits software and features that attackers commonly exploit.
5. **Restrict Administrative Privileges:** Ensures only necessary users have admin rights.
6. **Patch Operating Systems:** Keeps software up to date to close security gaps.
7. **Multi-Factor Authentication (MFA):** Requires additional verification for access.
8. **Regular Backups:** Protects against data loss and ransomware attacks.

Each control has four maturity levels (Zero to Three), reflecting an organisation's ability to mitigate cyber risks. Higher levels demand greater control, visibility, and enforcement—particularly over identity and access management (IAM).



The Role of Identity and Access in Essential Eight Compliance

While the Essential Eight covers a broad range of security measures, identity and access governance (IAG) is foundational to its success. Without clear oversight into who has access to what, when, and why, organisations cannot accurately assess compliance or enforce security controls.

Key identity-related challenges organisations face in Essential Eight compliance include:

- **Lack of Visibility:** Many organisations struggle to identify which users (human and non-human) have access to sensitive systems—especially across legacy, air-gapped, or disconnected environments.
- **Manual and Infrequent Access Reviews:** Traditional compliance audits occur annually or quarterly, creating gaps in oversight. By the time an audit is completed, the access data may already be outdated.
- **Proving Compliance for Auditors:** Auditors often request evidence of access governance maturity, but most organisations cannot easily generate reports that prove continuous compliance with Essential Eight controls.
- **Managing Least Privilege and Administrative Access:** The Essential Eight requires strict enforcement of least privilege principles, yet organisations struggle to consistently manage privileged accounts, role-based access, and just-in-time access requests.
- **Demonstrating Maturity Over Time:** Maturity Level Three requires consistent, repeatable controls—but how can organisations show continuous compliance without extensive manual effort?

This is where Gathid provides a game-changing solution.

How Gathid Helps Organisations Demonstrate Essential Eight Compliance

1. Immediate Visibility—No Bi-Directional Integration Required

Gathid provides immediate visibility into your identities and their access without needing bi-directional connectivity to critical systems. This is crucial for:

- Air-gapped, legacy, and disconnected environments that are intentionally or otherwise segregated from integrated identity governance tools.
- Government and regulated industries that need to ensure strict access control but have operational constraints.
- Security teams needing detailed, accurate visibility of identity and access risks without disrupting existing systems.



2. Automating Access Reviews and Ensuring Least Privilege Enforcement

Essential Eight mandates regular access reviews to ensure users only have the permissions they need. Gathid enables this process by:

- Mitigate the need for sample data sizes, Gathid enables a 100% review of all known identities across your enterprise, automatically, every day.
- Automating daily access reviews, reducing reliance on infrequent, manual audits.
- Identifying privilege creep and flagging excessive permissions, with context to related access before they become security risks.
- Tracking changes to identities and their access over time, making it easy to demonstrate maturity improvements.

With Gathid, organisations can move from annual compliance checks to daily visibility—a critical requirement for achieving Maturity Level Three.

3. Proving Compliance with Audit-Ready Reports

One of the biggest compliance challenges is proving that access controls meet Essential Eight maturity levels. Gathid simplifies compliance reporting by:

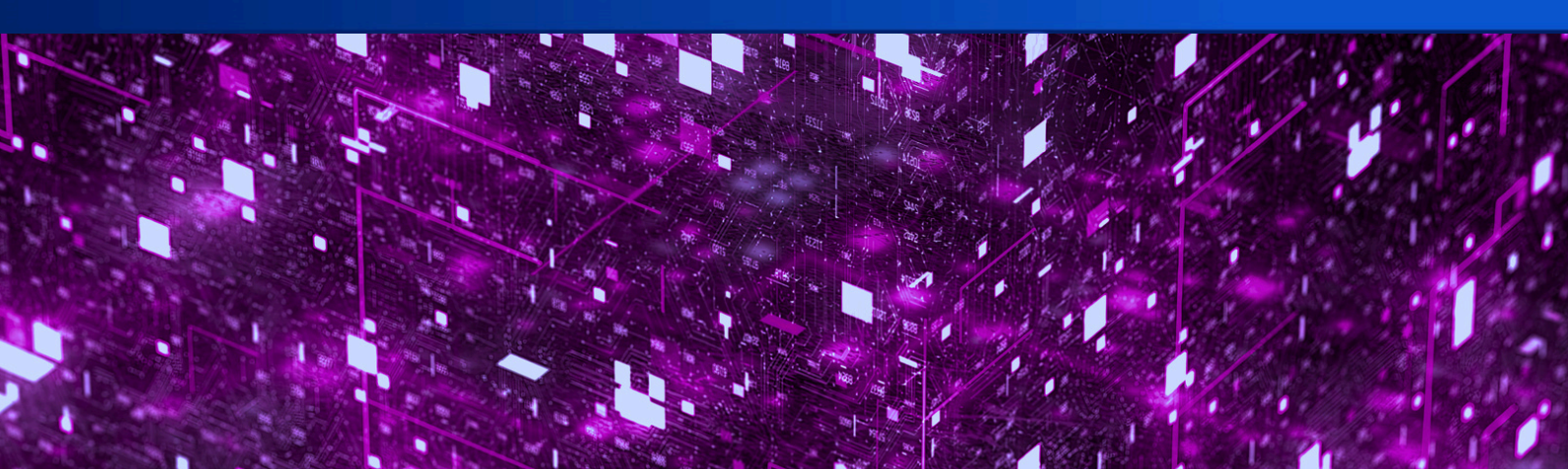
- Generating daily reports on user access, privileged accounts, and security controls.
- Tracking day-to-day changes to identity governance, making audits more transparent and efficient.
- Providing auditors with immediate insights into who has access to sensitive systems—and why.

Instead of spending months gathering evidence for an audit, organisations using Gathid can prove access compliance every single day.

4. Enforcing Essential Eight Identity Controls with Data-Driven Insights

Gathid helps organisations meet and prove compliance with specific Essential Eight controls, including:

- **Restrict Administrative Privileges:** Provides full visibility into who has admin rights, how they're used, and whether they align with least privilege principles.
- **Multi-Factor Authentication (MFA):** Identifies accounts lacking MFA enforcement, ensuring only verified users access critical systems.
- **Application Control and Patch Management:** Ensures only authorised users can execute applications, reducing the risk of unauthorised software installations.
- **Continuous Risk Insights:** Gathid's graph-based approach to identity mapping allows organisations to see access risk changes daily, preventing misconfigurations before they become security incidents.



Why Gathid is Key to Demonstrating Essential Eight Compliance

Unlike traditional compliance tools that focus on checking boxes, Gathid helps organisations:

- Understand, action, and prove that their identity and access controls meet Essential Eight requirements.
- Reduce compliance effort by automating access reviews and privilege ownership modelling.
- Continuously improve compliance maturity without disrupting existing IT operations.

For government agencies, financial institutions, and regulated industries, Essential Eight compliance isn't just a security requirement—it's a mandate. With Gathid, organisations can enhance their compliance maturity effortlessly, reduce risk, and maintain regulatory alignment—without the complexity of traditional IAM tools.

Get Started with Gathid Today

- Gain immediate visibility into identity risks
- Simplify access reviews and compliance reporting
- Prove Essential Eight maturity, every day

[Schedule a Demo](#) | [Learn More](#) | [Read Online](#)