FirstWave

Building a Cyber-Resilient Network:

The Essential Eight Framework

Cyber threats are constantly escalating, both in volume and sophistication. From phishing and ransomware to insider breaches and supply chain attacks, the risks extend across every layer of the modern enterprise network.

For public sector agencies and their managed service providers, the Australian Cyber Security Centre (ACSC) Essential Eight (E8) framework has become the recognized baseline for cyber maturity—even becoming mandated in some industries—as it provides a practical roadmap for reducing exposure and strengthening resilience.

The statistics are hard to ignore: **effective implementation of the Essential Eight can prevent up to 90% of common cyber incidents.***

This infopaper unpacks the E8 framework, explores why a holistic defence strategy matters, and shows how a layered model of prevention, detection, and control—like that offered by FirstWave—can help organizations move beyond just compliance toward genuine cyber resilience.

What is the Essential Eight?

The E8 is a set of eight mitigation strategies developed by the ACSC to protect against the most common and damaging types of cyberattacks including ransomware, phishing, data breaches, and exploitation of unpatched systems.

Each control focuses on an area of security that has proven impact, and together, they form an in-depth defence model that strengthens an organization's security posture at every layer.

The Essential Eight Maturity Levels

The ACSC defines four maturity levels for adoption of the E8 with each level reflecting an organization's ability to prevent, limit, and recover from cyberattacks.

Level 0 – Not Implemented **Minimal or no implementation of the E8 controls.** Security practices are inconsistent or reactive. The organization remains highly vulnerable to common attacks.	**Level 1 – Partly Implemented** **Basic security controls are in place, but coverage is incomplete or manually enforced.** Some protection exists, but attackers exploiting common tools and techniques could still compromise systems.
Level 2 – Mostly Implemented **Controls are consistently applied and enforced across the environment, with some automation.** Routine attacks are prevented, and policy enforcement is reliable. This level is often the minimum recommended baseline for most organizations.	**Level 3 – Fully Implemented** **All controls are fully integrated, automated, and continuously verified.** The organization can withstand sophisticated, targeted attacks and demonstrates measurable, sustainable cyber resilience.

Most entities aim for at least Level 2, enforcing consistent controls across the business. Achieving higher maturity means moving beyond compliance to measurable resilience, where security practices are proactive, automated, and continuously verified.

Why the Essential Eight? The Importance of Holistic Network Protection

Compliance alone doesn't create resilience.

True protection requires continuous visibility, consistent policy enforcement, and seamless coordination between your detection, prevention, and recovery capabilities.

A holistic network protection strategy, achieved by incorporating all of the E8, ensures that:

- **every asset is visible** so attackers have nowhere to hide
- **security configurations remain consistent** to reduce drift and human error.
- **threats are detected early** before they escalate into full-blown incidents
- **recovery is reliable,** minimizing downtime and data loss when disruptions occur.

For leaders responsible for large, complex networks, this shift from reactive to proactive is the difference between resilience and risk. The E8 framework provides this blueprint – all that's needed is an integrated approach that brings all eight strategies to life in a measurable, manageable way.

Mapping: Components that Solve for the Essential Eight

The ACSC defines four maturity levels for adoption of the E8 with each level reflecting an organization's ability to prevent, limit, and recover from cyberattacks.

Application Control

Application control ensures that only approved software can run within your environment. By blocking untrusted or unauthorized applications, you can prevent malware and rogue programs from executing, providing a safeguard against ransomware and insider threats. Consider it the digital equivalent of locking every door and window before an intruder even tries to enter.

How to implement

- Identify all applications running on your network and define an approved whitelist.
- Block unauthorized software from running on your systems.

Patch Applications

Unpatched applications are a cybercriminal's easiest entry point. This control requires regular updates to third-party software like browsers and office suites, closing security gaps before attackers exploit them.

Consistent patching turns software maintenance from an afterthought into a core defence mechanism, significantly reducing exposure to known vulnerabilities.

How to implement

- Regularly monitor for updates across your software inventory.
- Prioritize and deploy security patches promptly.

Configure Microsoft Office Macro Settings

Macros remain one of the most common delivery methods for malware. By restricting or disabling macros (especially those from the internet), organizations eliminate a major threat vector for phishing and ransomware. It's a simple yet powerful step: stop malicious code before it can ever execute inside your environment.

How to implement

- Disable or tightly restrict macros, particularly from external sources, in Office documents.
- Enforce policies via configuration management.

User Application Hardening

Hardening user applications means disabling risky or unnecessary features within browsers, PDF readers, and email clients. This reduces the attack surface by removing capabilities that adversaries often exploit.

When applications are configured for security first, everyday user activity becomes far less dangerous – even when mistakes happen.

How to implement

- Remove or disable high-risk application features.
- Turn off unsafe browser plugins (like Flash).
- Block ads or remote code in PDF reader.
- Remove legacy protocols where possible.

Restrict Administrative Privileges

Excessive admin rights are ideal for attackers. Limiting privileged access ensures that even if a user account is compromised, the damage is contained. This control enforces the principle of least privilege, ensuring only authorized staff can make system-level changes for ultimate compliance and risk reduction.

How to implement

- Limit admin access to essential staff only and tightly control their use.
- Separate standard and privileged accounts.
- Monitor privileged activity.

Patch Operating Systems

Outdated operating systems expose your IT environment to exploitation. Keeping your OS versions current and promptly applying security updates prevents attackers from using known flaws to gain a foothold.

Patching is one of the most cost-effective defences available – and one of the most often overlooked.

How to implement

- Apply OS updates and firmware patches quickly and consistently.
- Verify deployment and monitor for failed updates.

Multi-Factor Authentication (MFA)

Passwords alone are no longer enough. MFA requires users to verify their identity through an additional factor—like a code or biometric—before gaining access. This single change prevents most credential-based attacks, protecting remote access, privileged accounts, and cloud applications from unauthorized entry.

How to implement

- Enforce MFA for remote access, privileged accounts, and high-risk systems.
- Monitor for non-compliant access attempts.

Regular backups

Reliable, tested backups ensure that even when defences fail, operations don't. By backing up critical data and configurations daily, as well as validating those backups, organizations can recover quickly from ransomware, system corruption, or accidental deletion. In essence, backups can turn a potential disaster into a temporary inconvenience.

How to implement

- Perform daily backups of data and configurations.
- Test restoration procedures.
- Monitor backup success.

Each of the above eight strategies contributes to a single goal: resilience. Together, they build a security foundation capable of protecting against most modern attack scenarios – especially when implemented in unison across all systems and users.

Achieving the Essential Eight with FirstWave

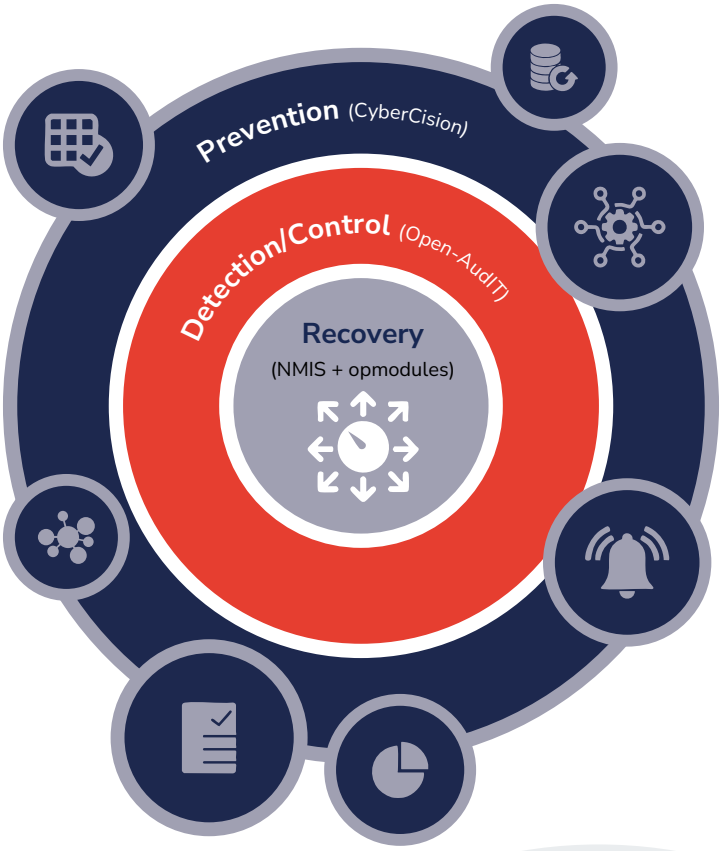
FirstWave's approach to cybersecurity mirrors the E8 philosophy: multiple layers of defence working together to reduce risk and build operational resilience.

FirstWave's integrated platform turns the E8 framework into practice by unifying the key layers of defence:

- **Prevention** through intelligent email and web threat filtering.
- **Detection** through continuous asset discovery and compliance auditing.
- **Control** through proactive network management and backup verification.

Prevention

Prevention is your first line of defence, stopping threats before they infiltrate your environment. This includes blocking phishing emails, malware downloads, and unauthorized access attempts at the network edge.



CyberCision

FirstWave CyberCision filters malicious content at the network edge, blocking phishing emails, malware attachments, and unsafe URLs before they reach users. CyberCision also integrates MFA to secure administrative and remote access – directly supporting several E8 controls including macro settings, user application hardening, and MFA enforcement.

By stopping threats before they enter the network, CyberCision reduces workload downstream and creates a stronger security baseline.

Discover CyberCision

Detection

The second defence layer assumes that some threats or weaknesses will make it past the perimeter, and focuses on identifying them quickly and enforcing internal security policies.

Open-AudIT

Visibility is the foundation of compliance. **FirstWave Open-AudIT** automates discovery of all systems, devices, and applications in an environment. It identifies missing patches, outdated configurations, and unauthorized software in a single scan, turning weeks of manual effort into minutes. This continuous visibility enables organizations to maintain up-to-date application and operating system patching, enforce privilege policies, and track compliance against E8 requirements.

Discover Open-AudIT

Control

Despite best efforts, incidents can still happen—for example, a novel ransomware might encrypt some files—so the control layer emphasizes damage control and system recovery.

NMIS

Achieving resilience comes down to control. **FirstWave NMIS (Network Management Information System)** monitors infrastructure performance and verifies that critical processes, like backups and patch cycles, are running smoothly.

NMIS alerts IT teams to failed backups, post-patch instability, or network issues that could undermine resilience. This keeps organizations in constant alignment with E8 controls around Patch Operating Systems and Regular Backups, while maintaining network health and stability.

Beyond core network monitoring, FirstWave's opModules extend NMIS with advanced analytics, reporting, and automation capabilities:

- **opEvents:** Centralised log and event management.
- **opConfig:** Automated configuration and compliance management.
- **opHA:** Distributed network management.
- **opAddress:** IP address audit and management.
- **opCharts:** Interactive dashboards and charts.
- **opReports:** Advanced analysis reporting.
- **opFlow:** Visualised network performance.

You can also extend NMIS to include **Secure Traffic Manager (STM),** a DPI (Deep Packet Inspection)-powered network traffic management solution for secure routing and threat filtering at the network edge. STM provides real-time visibility into network flows and the ability to block malicious or non-compliant traffic, supporting safe web usage for end-users.

Discover NMIS

The Business Impact of Essential Eight with FirstWave

Compliance: Tools to help meet your obligations.
Risk reduction: Detect & prevent threats, control access with MFA.
Visibility: See all systems, applications, devices, & network assets.
Scalability: ASD recommended, email & web threat protection.

Resilience isn't built overnight, but rather engineered through consistent, layered defence. The result is measurable maturity, reduced risk, and a network that can adapt faster than the threats against it.

With FirstWave's layered platform, organizations can speed up vulnerability detection, simplify remediation, and provide confidence that your security controls will remain effective every day – all aligned with E8 maturity goals.

The Essential Eight provides the framework; FirstWave helps you operationalize it.

Ready to strengthen your network reliability, security, and compliance?

Discover NMIS

Get opCharts

Get opEvents

Want to learn more before you deploy?

Contact our team for expert guidance and support.

FirstWave