COMPLIANCE GUIDE

How Zero Networks Helps with Essential 8 Requirements

The Essential 8 (E8) is a cybersecurity framework developed by the Australian Cyber Security Centre (ACSC) that offers eight key strategies for organisations to protect against cyber threats. It can be a journey to understand and check off everything on the list – so we're breaking down the direct and indirect impacts of having advanced microsegmentation and MFA capabilities, and how they can help you simplify and accelerate your E8 timeline.

Direct Impact of Zero Networks on E8

The combination of Zero's identity-informed segmentation and network-layer MFA provides the most powerful, protective defence on the market, empowering organisations to secure east-west traffic as well as north-south traffic with precise controls.

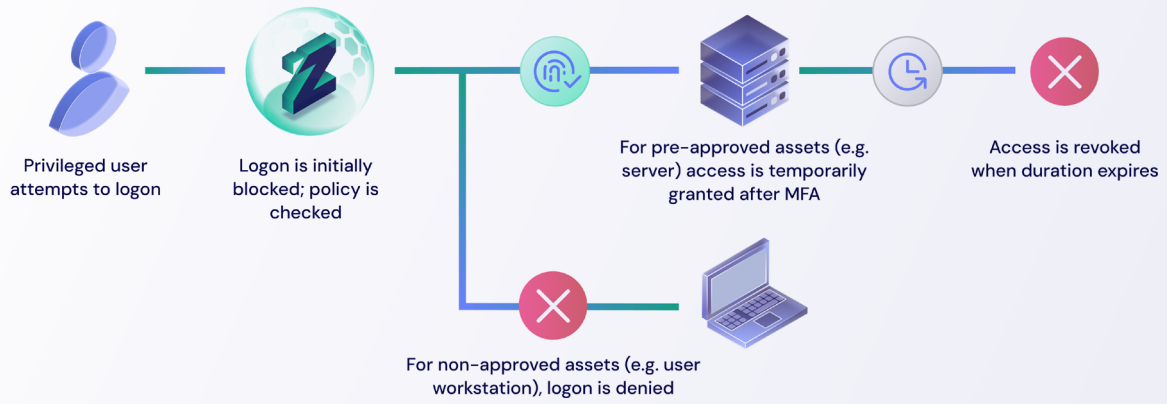
With Zero, organisations easily satisfy Requirement 5 and 7 of the Essential 8 – Restricting Admin Privileges and having Multi-Factor Authentication. With Zero's granular access controls and just-in-time MFA, only privileged users who pass authentication are allowed temporary access to pre-approved assets. That's right – privileged ports are only open for a specified amount of time (typically a few hours) and remain invisible to hackers. Plus, every MFA authentication – allowed or denied – is logged for easy monitoring and auditing.

The outcome?

- Credential theft risk is eliminated
- Lateral movement is blocked
- Admin logon rights are provisioned based on least privilege – and can only access approved assets
- Every logon is protected by the strongest MFA on the market

How JIT MFA Works with Zero

Privileged users are allowed to temporarily logon on pre-approved assets only after MFA



Indirect Impact: How Automated Microsegmentation Enables E8 Compliance

Having identity-informed microsegmentation and network-layer MFA creates a ripple-effect across the security of a network, touching on each requirement of E8. Take a deeper dive in the table below:

Requirement	Description	How Zero Helps
Requirement 1	**Application Control:** Only approved, trusted, and necessary applications should be allowed to execute on workstations and servers. This prevents unauthorised or malicious software (including ransomware) from running.	Zero Networks enforces least-privilege network access, allowing only authorised communication between applications and endpoints. This blocks lateral movement and prevents unapproved applications from communicating over the network.
Requirement 2	**Patch Applications:** Security vulnerabilities in applications (e.g., browsers, Microsoft Office, Java) must be patched within a specified timeframe (e.g., 48 hours for critical vulnerabilities) to prevent exploitation	Zero does not patch applications directly – however, it reduces the attack surface of a network by isolating and protecting vulnerable and legacy applications via segmentation and network-layer MFA. This containment limits exposure and provides protective controls while patching is underway.
Requirement 3	**Configure Microsoft Office Macro Settings:** Macros should be disabled for users who do not need them. For those who do, only digitally signed macros from trusted sources should be allowed, and macros from the internet must be blocked to prevent malware delivery.	Zero Networks can restrict network access for endpoints or users known to use macros, limiting the potential for macro-borne malware to communicate or spread across the environment. This network-level containment complements endpoint macro controls.
Requirement 4	**User Application Hardening:** Unnecessary features (e.g., Flash, ads, Java) in user applications and web browsers must be disabled or removed to reduce the attack surface and block risky content.	Zero Networks limits network access for hardened applications, ensuring only necessary communications are permitted. If a user application is compromised, the attacker is unable to move laterally in a microsegmented network. This prevents attacks from reaching critical systems and enforces a defence-in-depth approach.
Requirement 6	**Patch Operating Systems:** Operating systems must be patched for security vulnerabilities within required timeframes,	While Zero Networks does not patch OSes, it segments legacy and vulnerable systems, restricting traffic and reducing the risk of exploitation. This isolation can contain threats instantly and, in general, buys time for safe patching.
Requirement 8	**Regular Backups:** Daily backups of important data, software, and configuration settings must be performed and stored securely, ensuring data can be restored in case of ransomware or cyber incidents.	Zero Networks restricts access to backup systems, allowing only authorised devices and users. This segmentation protects backups from ransomware and unauthorised access, ensuring data integrity and availability during recovery.

ZERO. Networks

Connect with the Zero team to discover how you can streamline your Essential 8 alignment with automated microsegmentation.

Request a Demo