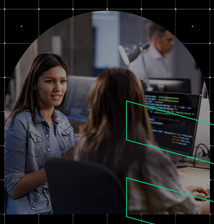
Mitigate cyber security incidents with essential eight



The Essential Eight is a list of mitigation strategies developed by the Australian Cyber Security Centre (ACSC) to assist organisations in protecting their systems against cyber security threats.

The Australian Signals Directorate (ASD) considers the Essential Eight as one of the most effective defence strategies against cybercriminals for all organisations.

The minimum set of cyber security incidents mitigation strategies include:

Strategies to prevent attacks

1 Application control

Security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented robustly, it ensures only approved applications can be executed.

How Nexon can help:

We deploy and manage application whitelisting software recognised by Australian Signals Directorate (ASD) to ensure that only authorised applications run on your devices.

2 Patch applications

Once a patch is released by an application vendor, the patch should be applied in a timeframe commensurate with an organisation's exposure to the security vulnerability and the level of cyber threat the organisation is aiming to protect themselves against.

How Nexon can help:

Leveraging Microsoft Intune or managing your endpoints, we ensure your applications and operating systems patches are kept up to date on corporate devices. Our Zero Trust Network access solutions allow you to implement a policy that blocks access to resources until an out of date web browser that is being used to access is updated on all devices - corporate or not.

3 Configure Microsoft Office macro settings

Microsoft Office files can contain embedded code (known as a macro). To block malicious macros, you should only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

How Nexon can help:

We audit and update your Microsoft workplace environment to ensure security controls are enabled and configured for your business needs.

4 User application hardening

Flash, ads and Java are common ways to execute malicious code. Configure web browsers to block Flash , ads and Java and disable unneeded features in Microsoft Office and PDF viewers to harden applications accordingly.

How Nexon can help:

We audit and update applications used to make sure they're configured and deployed securely. By setting application policy based on the presence of Java or Flash as part of a Zero Trust network access deployment we can block or limit access to Java or Flash across all users.

Strategies to limit the extent of attacks

5 Restrict administrative privileges

Restricting administrative privileges makes it more difficult for an adversary's malicious code to spread. An environment where administrative privileges are restricted is more stable, predictable, and easier to administer and support.

How Nexon can help:

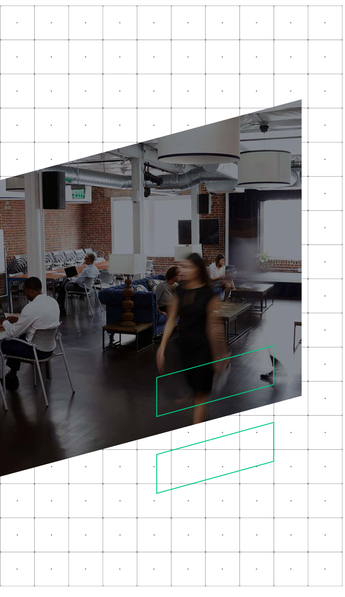
We audit and update applications used to make sure they're configured and deployed securely. By setting application policy based on the presence of Java or Flash as part of a Zero Trust network access deployment we can block or limit access to Java or Flash across all users.

6 Patch operating systems

Once a patch is released by servers, network devices and other network-connected devices vendors, the patch should be applied in a timeframe commensurate with an organisation's exposure to the security vulnerability and the level of cyber threat the organisation is aiming to protect themselves against.

How Nexon can help:

We audit and update applications used to make sure they're configured and deployed securely. By setting application policy based on the presence of Java or Flash as part of a Zero Trust network access deployment we can block or limit access to Java or Flash across all users.



7 Use multi-factor authentication

When implemented correctly, multi-factor authentication can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on a network.

How Nexon can help:

Zero Trust network access is part of a comprehensive SASE solution delivered by Nexon to:

- Verify employee identity
- Provide easy and secure access to web and SaaS applications, improving cloud and work from home security
- Apply policies to ensure that only patched applications and operating systems can join the network.

Strategies to recover data and system availability

8 Regular backups

Regular back ups of new or changed data, software and configuration settings ensure information can be accessed quickly following cyber security incidents.

How Nexon can help:

Zero Trust network access is part of a comprehensive SASE solution delivered by Nexon to:

- A reliable last line of defence to safeguard backups from ransomware
- Instant recovery - quickly restore and deliver a full system recovery
- Reduce downtime during a security incident avoiding operational disruption.
- End to end encryption - secure data at rest and in-flight in the Cloud

Create your strategy for the essential eight with Nexon

Our team of cyber security experts work with you to consult, deploy and manage security controls and technology to build a security architecture that meets your unique business needs and compliance requirements.

Learn more about our solution at

https://nexon.com.au/lp/sase-your-way

Ready to talk? Call us at 1300 800 000

Contact to us today to find out more about our comprehensive Cloud and security services to protect your data, platforms and people.

1300 800 000
enquiries@nexon.com.au
nexon.com.au

Cisco Partner
Gold Provider