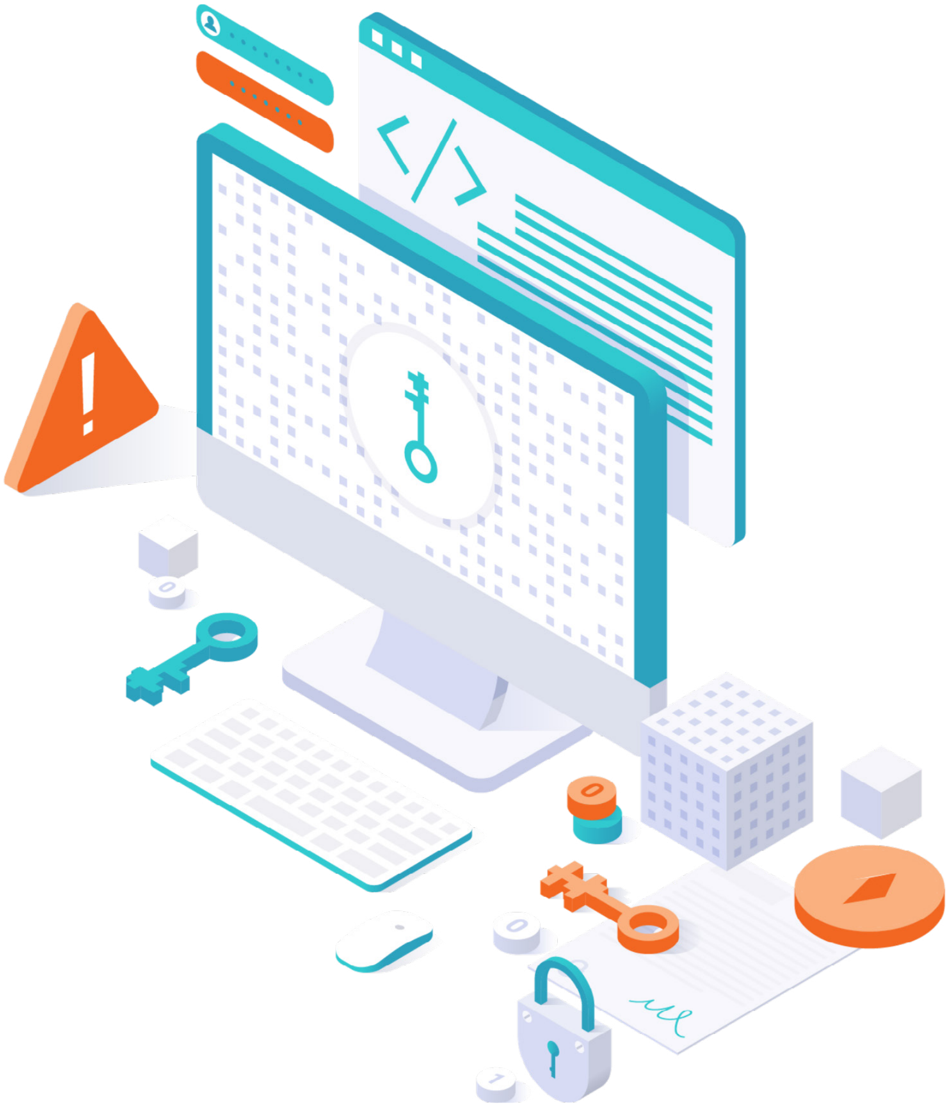
NEXTGEN GROUP

The Essential Eight

The Australian Cyber Security Centre (ACSC) has developed the Essential Eight cyber security strategies. Designed as the foundations for you to build your cyber security capabilities and defence against threats, they ensure alignment of cyber security strategies, cyber processes and cyber awareness throughout your organisation.



Has your business passed the Essential Eight check?

What is the Essential Eight?

The Essential Eight has been designed to protect Microsoft Windows-based internet-connected networks. Correctly implementing the Essential Eight can save your business time, money and effort if you have to respond to a large-scale cyber security incident.

What research backs it?

First published in June 2017 and updated regularly, implementation of the Essential Eight is based on the ACSC's experience in producing cyber threat intelligence, responding to cyber security incidents, and conducting penetration testing.

What vendors fit within the Essential Eight?

Designed to protect and mitigate cyber threats to SMEs, public and private organisations, and enterprises, the Essential Eight fits within vendors offering cloud security, cloud data management, open source software-defined infrastructure, information technology infrastructure management, DevOps, and Endpoint Detection and Response (EDR).

How NEXTGEN can support my cyber needs through Essential Eight

The specialist cyber team at NEXTGEN are highly trained and experienced IT security experts and ex-Australian military cyber security professionals. Industry recognised and awarded, the Cyber team supports vendors, specialist partners, and end-customers to successfully navigate the implementation of the Essential Eight strategies for your business or organisation.

Maturity levels

To assist with your implementation of the Essential Eight, four maturity levels have been defined. They are designed to assist implementation in a graduated manner based upon different levels of adversary tradecraft and targeting. The different maturity levels can also be used to provide a high-level indication of your organisation's cyber security maturity.

Maturity Level Zero

This signifies there are weaknesses in an organisation's overall cyber security posture.

Maturity Level One

The focus of this maturity level is adversaries content to simply leverage commodity tradecraft that is widely available to gain access to, and likely control of, systems.

Maturity Level Two

The focus of this maturity level is adversaries operating with a modest step-up in capability.

Maturity Level Three

The focus of this maturity level is adversaries who are more adaptive.

The Essential Eight

1

Application Control

Used to prevent the execution of malicious code including executable files such as compiled HTML, HTML applications. Antivirus software can't detect all unapproved programs, so this control is necessary to add the extra level of security needed for business systems.

2

Patch Applications

This involves the implementation of new patches and vulnerability scans to detect new issues in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. When a threat is detected, action should be taken to mitigate it immediately and automatically.

3

Configure Microsoft Office Macro Settings

If you are running a macro, then it is best to enable it only from a trusted location, giving limited access or ensuring the certificate used in signing the macro is trustworthy. You should also be able to track activities like processes, services, or applications launched unknown to the user that might indicate a possible attack.

4

User Application Hardening

The process of limiting what an application can do on a system that regularly interacts with content from the web. This is achieved by hardening features in Microsoft Office, PDF viewers or web browsers that are not needed, like blocking Flash and advertisements on web browsers, or blocking JavaScript on certain websites.

5

Restrict Administrative Privileges

Allowing privileged access to systems and applications to select employees. Users with minimal privileges should not be given any more than is necessary to complete daily tasks. This prevents malicious actors from taking over important security controls and configurations.

6

Patch Operating Systems

Similar to patching applications, patching operating systems involves regularly checking for newly-released patches. This not only mitigates the risk of attack, it reduces any potential damage. Upgrade to the newest operating system and patches instead of using unsupported versions.

7

Multi-factor Authentication

Passwords are no longer an adequate form of authenticating users and protecting them against hacks. Hardening devices to the maximum extent, ensuring a visual notification appears for every authentication request, and storing software certificates in the devices' trusted platform module makes it much more difficult for threat actors to gain unauthorised access.

8

Regular Backups

Regular offline and online backups are highly recommended. Having backups or an alternate system ready to go, in the event of ransomware or another type of operational failure, ensures your data and software are more likely to be recoverable. These should also have measures to alert users or indicate a breach, and specify proper incident response actions.

Our Vendors

okta

The Okta Identity Cloud is an independent and neutral platform that securely connects the right people to the right technologies at the right time. Okta help partners grow at scale by enabling them to provide end-customers with a range of cloud services lifecycle solutions across Single Sign-on, Adaptive Multi-factor Authentication, Advanced Server Access, and Access Gateway.

netskope

Netskope is a cloud security company with a mission to evolve security for the way people work today. Their patented Cloud XD technology eliminates blind spots by going deeper than other security providers to quickly target and control activities across thousands of cloud services and millions of websites. Netskope helps the world's largest organisations take advantage of cloud and web without sacrificing security.

CROWDSTRIKE

Designed from the ground up to deliver best-of-breed security offerings, the CrowdStrike Falcon platform's single-lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. CrowdStrike Falcon correlates trillions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

rubrik

Rubrik is the market leader in Cloud Data Management, the world's first platform to orchestrate data for hybrid cloud enterprises anytime, anywhere. Rubrik blends future-proof architecture with consumer-grade simplicity to pioneer a fresh approach to an old problem. This incorporates Backup and Recovery, Replication and DR, and Data Archiving.

CLOUDIAN

Data center managers, broadcasters, researchers, and software developers need solutions to help them contend with the explosive growth in unstructured data. Cloudian's technology allows all sizes and types of users – from media, to medical, to industrial – to realize the benefits of object storage in their own data centers.

solarwinds

SolarWinds Inc. develops enterprise information technology infrastructure management software. Their IT Monitoring and Management tools are built for System Administrators and Network Engineers who need powerful and affordable tools. Solarwinds solutions including Network Management, Systems Management, Database Management, and IT Security.are renowned for ease of use and technical reliability.

MICRO FOCUS

is now opentext

Micro Focus enterprise software helps tens of thousands of customers worldwide embrace the dilemma of digital transformation- how to run and transform at the same time.OpenText has completed the purchase of Micro Focus. OpenText powers and protects information to elevate every person and every organisation to be their best.

ORACLE

Oracle provides best-of-breed capabilities across a broad SaaS and PaaS portfolio, with a supporting IaaS and on premise software and infrastructure pedigree to support 'all in' cloud, hybrid cloud or on-premise strategies. Oracle's strongest position is at the core of the enterprise, delivering critical applications and platforms and cutting edge technologies such as IoT, machine learning and blockchain. Oracle is at the forefront of integrating these technologies into modern business.

About NEXTGEN Group

With a highly specialised team - including Australian ex-military cyber security professionals - the NEXTGEN Cyber team helps you navigate the evolving and complex IT security landscape.

Get in touch with us today

nextgen.group/contact-us

NEXTGEN
GROUP