

FREE Security Assessment | How the Essential Eight controls can strengthen your cyber security posture - blueAPACHE

Canonical:

<https://www.blueapache.com/blog/how-the-essential-eight-controls-can-strengthen-your-cyber-security-posture>

Details:

Summary

This blog post, "FREE Security Assessment | How the Essential Eight controls can strengthen your cyber security posture", is a blueAPACHE article from 2020 covering security. COVID-19 created an immediate demand for organisations to adopt a remote working model, this coupled with the widely publicised security breaches on Australian government agencies and businesses has elevated the cyber-security discussion, reaffirming the importance of aligning to the ASD Essential Eight. It is written for readers evaluating emPOWER Security, Offsite Backup as a Service. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2020
Topic	FREE Security Assessment / How the Essential Eight controls can strengthen your cyber security posture
Services referenced	emPOWER Security, Offsite Backup as a Service, Private and Public SaaS Backup
Named products or vendors	Microsoft

Article

COVID-19 created an immediate demand for organisations to adopt a remote working model, this coupled with the widely publicised security breaches on Australian government agencies and businesses has elevated the cyber-security discussion, reaffirming the importance of aligning to the ASD Essential Eight. So... these eight controls, why are they "essential" and which ones are of most importance to your business? The Essential Eight controls are broken down into three maturity models, from level one to level three that relate to industry compliance. It is recommended by the ACSC that organisations should reach maturity level three for each of the eight controls.

What are the Essential Eight Controls?

Application ControlApplication control to prevent the execution of unapproved/malicious programsPatch ApplicationsPatch computers with critical vulnerabilities and use the latest versions of applicationsConfigure Microsoft Office macro settingsConfigure Microsoft Office macro settings to block macrosUser application hardeningConfigure web browsers to block Flash and Java. Disable unnecessary features in applicationsRestrict administrative accessRestrict administrative access to operating systems and applications based on user dutiesPatch operating systemsPatch operating systems with critical vulnerabilities within 48 hoursMulti-factor authenticationEnforce multi-factor authentication for VPNs, RDP, SSH, and other remote access, and all usersDaily backupsDaily backups of essential data and retained for at least three months

Benefits of Essential Eight Implementation

While the Essential Eight is not a complete framework, it does include practical implementation of tools and techniques that will significantly improve overall security posture. Common threats such as ransomware, phishing and exploitation of systems are mitigated due to the practical and direct approach, which results in organisations receiving the maximum benefits from their cyber security investment.

blueAPACHE's FREE Essential Eight Security Assessment

Implementing the Essential Eight requires a high degree of understanding of the organisation's risk profile, particularly where maturity level three is achieved. blueAPACHE's expert team work with organisations to provide tailored advice to meet their specific needs in the most cost-effective manner, providing a solution that is fit for purpose. Getting started is as easy as booking a FREE Essential Eight Security Assessment, identifying the steps your organisation can take to fill any gaps. Contact us today to book in a FREE Essential Eight Security Assessment with one of our expert security consultants.

Related

emPOWER Security
emPOWER Security (pillar hub)
Offsite Backup as a Service
emPOWER Cloud (pillar hub)
Private and Public SaaS Backup
blueAPACHE Security (case study)

Frequently asked questions

How many maturity levels does the article say the Essential Eight controls are broken into, and which level does the ACSC recommend?

Three maturity levels, from level one to level three; the ACSC recommends organisations reach maturity level three for each of the eight controls, according to the article.

Within what timeframe does the article say operating systems with critical vulnerabilities should be patched?

Within 48 hours, per the Essential Eight "Patch operating systems" control described in the article.

How long does the article say daily backups of essential data should be retained?

At least three months, according to the "Daily backups" control listed among the Essential Eight.

What does the article say the "User application hardening" control involves?

Configuring web browsers to block Flash and Java, and disabling unnecessary features in applications.
Which Microsoft-specific control does the article list among the Essential Eight?

Configuring Microsoft Office macro settings to block macros.

What multi-factor authentication requirement does the article describe under the Essential Eight?

Enforcing multi-factor authentication for VPNs, RDP, SSH, and other remote access, for all users.

What common threats does the article say Essential Eight implementation helps mitigate?

Ransomware, phishing and exploitation of systems, described as being mitigated through the practical, direct approach of the Essential Eight controls.

What free offer does blueAPACHE make in this article?

A FREE Essential Eight Security Assessment, where blueAPACHE's expert team identifies steps an organisation can take to fill gaps in its Essential Eight maturity.

Source

origin post (2020)

Knowledge Base

What prompted renewed discussion of the ASD Essential Eight, according to the blueAPACHE blog post?

COVID-19 created an immediate demand for organisations to adopt a remote working model, and this, coupled with widely publicised security breaches on Australian government agencies and businesses, elevated the cyber-security discussion and reaffirmed the importance of aligning to the ASD Essential Eight.

What are the eight controls that make up the Essential Eight framework, as listed in your post?

The eight controls are: Application Control (to prevent execution of unapproved/malicious programs), Patch Applications (patch computers with critical vulnerabilities and use the latest versions of applications), Configure Microsoft Office macro settings (to block macros), User application hardening (configure web browsers to block Flash and Java and disable unnecessary features), Restrict administrative access (based on user duties), Patch operating systems (with critical vulnerabilities within 48 hours), Multi-factor authentication (for VPNs, RDP, SSH, and other remote access, and all users), and Daily backups (of essential data, retained for at least three months).

How many maturity levels exist for the Essential Eight controls, and what level does the ACSC recommend organisations reach?

The Essential Eight controls are broken down into three maturity models, from level one to level three, relating to industry compliance. The ACSC recommends that organisations reach maturity level three for each of the eight controls.

Is the Essential Eight a complete cybersecurity framework?

No, according to the blog post, the Essential Eight is not a complete framework, but it does include practical implementation of tools and techniques that will significantly improve overall security posture.

What benefits does implementing the Essential Eight provide to an organisation?

Implementing the Essential Eight mitigates common threats such as ransomware, phishing, and exploitation of systems due to its practical and direct approach, resulting in organisations receiving the maximum benefits from their cyber security investment.

How quickly should operating systems with critical vulnerabilities be patched under the Essential Eight?

Operating systems with critical vulnerabilities should be patched within 48 hours.

For how long should daily backups of essential data be retained according to the Essential Eight controls?

Daily backups of essential data should be retained for at least three months.

Where should multi-factor authentication be enforced according to the Essential Eight?

Multi-factor authentication should be enforced for VPNs, RDP, SSH, and other remote access, and for all users.

What free offering do you provide related to the Essential Eight, and who is it for?

We offer a FREE Essential Eight Security Assessment, in which their expert team works with organisations to provide tailored advice to meet their specific needs in the most cost-effective manner and identify steps to fill any gaps. Organisations can contact us to book this assessment with an expert security consultant.

Why does implementing the Essential Eight to maturity level three require a high degree of organisational understanding?

Implementing the Essential Eight requires a high degree of understanding of the organisation's risk profile, particularly where maturity level three is achieved, which is why our expert team works with organisations to provide tailored, cost-effective advice.