The Essential Eight:
Your Guide to Compliance Through Zero Trust

zscaler™

The Essential Eight is a list of eight priority cyber security areas on which Australian organisations should focus to prevent malware delivery, execution and persistence. The Essential Eight is an expected baseline which makes it much harder for malicious cyber actors to compromise systems.

The areas include:

1. **Application Control.** Prevents execution of unapproved/malicious programs.
2. **Patch Applications.** Patch/mitigate applications with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
3. **Configure Microsoft Office macro settings.** Limit the opportunities for macros to do damage.
4. **Harden user applications.** Disable unneeded features in Microsoft Office, web browsers and PDF viewers.
5. **Restrict administrative privileges.** A range of aspects to limit the ability of administrative accounts to have an overly broad impact.
6. **Patch operating systems.** Patch/mitigate operating systems with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of operating systems.
7. **Multi Factor authentication.** Add an additional layer of authentication to systems that need protection.
8. **Backups.** Backup and test recovery of important new/changed data, software and configuration settings. It should be stored, disconnected and retained for at least three months.

For more information see: https://www.cyber.gov.au/sites/default/files/2019-05/PROTECT%20-%20Essential%20Eight%20Explained%20%28April%202019%29.pdf

Why should I implement the Essential Eight?

Implementing the Essential Eight makes it much harder for adversaries to compromise IT systems. Furthermore, implementing the Essential Eight proactively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.

The value of the Essential Eight is better understood in the context of the threat environment which it helps to protect against. The metrics published in the ACSC Annual Cyber Threat Report - 1 July 2020 to 30 June 2021, help to provide this context:

- Over 67,500 cybercrime reports, which is an increase of nearly 13 per cent from the previous reporting period.
- Self-reported financial losses from cybercrime total more than $33 billion.
- Approximately one quarter of reported cyber security incidents affected entities associated with Australia's critical infrastructure.
- Over 1,500 cybercrime reports per month of malicious cyber activity related to the coronavirus pandemic (approximately 4 per day).

- More than 75 percent of pandemic-related cybercrime reports involved Australians losing money or personal information.
- Nearly 500 ransomware cybercrime reports, an increase of nearly 15 per cent from the previous financial year.
- Fraud, online shopping scams and online banking scams were the top reported cybercrime types.
- An increase in the average severity and impact of reported cyber security incidents, with nearly half categorised as 'substantial'.

Based on the cyber threat landscape summarized in the ACSC Annual Cyber Threat Report - 1 July 2020 to 30 June 2021, the ACSC recommends all Australian organisations prioritise implementation of the Essential Eight Maturity Model.

For more information see: https://www.cyber.gov.au/acsc/view-all-content/publications/acsc-annual-cyber-threat-report-2020-21

What is the Essential 8 Maturity Model?

The Essential Eight Maturity Model, first published in June 2017 and updated in July 2021, supports the implementation of the Essential Eight controls.

The Maturity Model is a score against each of the eight areas of focus. The scores range from 0-3; where 0 represents no implementation of the focus area, right up to 3 which is fully implemented. For more information see: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

What should I do if I cannot implement an Essential Eight requirement to Level 3 maturity?

The Essential Eight controls provide the strongest defence to cyber intrusions. The less mature an organisation's implementation of an Essential Eight requirement, the more important alternative and compensating controls become in providing alternative assurance. These compensating controls are typically sourced from vendor hardening guides and ACSC publications like the Information Security Manual and the ACSC's Strategies to Mitigate Cyber Security Incidents.

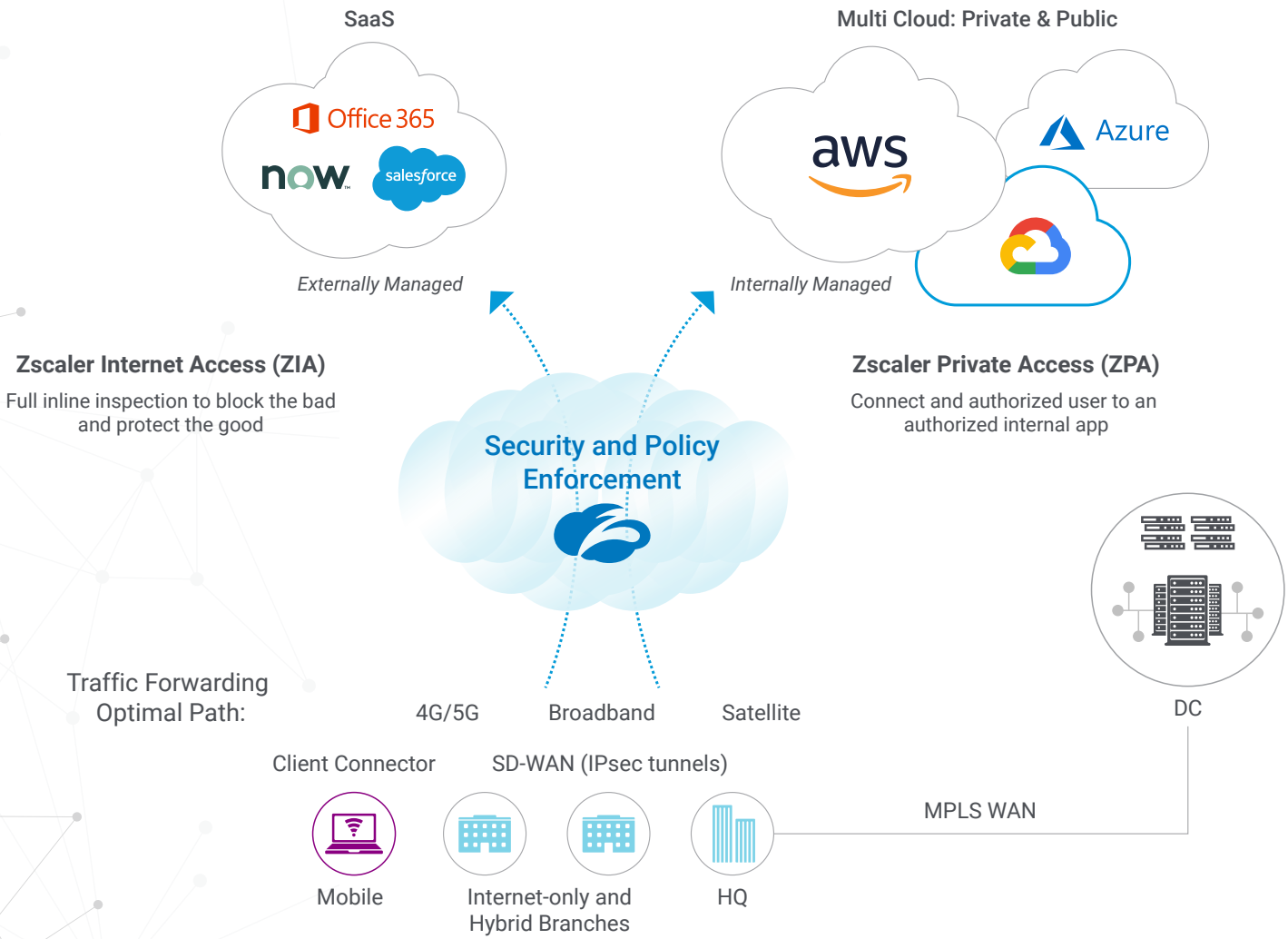
The less mature an Essential Eight implementation, the more important it is to implement detection and recovery controls.

What is ZPA?

Zscaler Private Access (ZPA) is a cloud service from Zscaler that provides seamless, zero trust access to private applications running on public cloud or within the data center. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity versus extending the network to them. Users are never placed on the network. This zero-trust network access (ZTNA) approach supports both managed and unmanaged devices and any private application (not just web apps).

What is ZIA?

Zscaler Internet Access (ZIA) is a secure internet and web gateway delivered from the cloud. ZIA inspects all internet traffic and delivers secure connectivity to third-party SaaS applications, like Office 365 and ServiceNow. The ZIA platform protects organisations from data loss, as well as delivering a cloud access security broker, web filtering, and firewall software.



How do ZIA and ZPA Help to Complement the Essential Eight Requirements?

	Essential Eight Requirement	Zscaler Complementary Capability	Information Security Manual Control References
1	**Application Control**	Though ZIA does not inhibit the installation or running of applications, its use can reduce the impact of unapproved software by inhibiting their ability to connect to unauthorised internal and external sites.	0843; Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Other applicable controls include: 1490, 1656, 1657, 1658, 1544, 1659, 1582, 1660, 1661, 1662, 1663.
2	**Patch Applications**	ZIA can be configured to only allow patches from known and approved patching sites.	1690: Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Other applicable controls include: 1691, 1692, 1693, 1698, 1699, 1700, 1704, 0304
3	**Configure Microsoft Office macro settings**	The Zscaler Cloud Sandbox can be used to help detect document-based threats involving malicious macros.	1671: Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Other applicable controls include: 1674, 1487, 1675, 1676, 1488, 1672, 1673, 1489, 1677, 1678

	Essential Eight Requirement	Zscaler Complementary Capability	Information Security Manual Control References
4	**Harden user applications**	Zscaler's zero trust architecture provides users with secure, direct access to internal and cloud apps with Zscaler Private Access (ZPA), applications are never exposed which eliminates the ability for an attacker to move laterally. ZIA can block specific file types such as java from reaching the end point. ZIA also provides both black and whitelisting of Internet sites and anti-malware capabilities.	1485: Web browsers are configured to block web advertisements. 1486: Web browsers are configured to block Java from the Internet. 1542: Microsoft Office is configured to prevent activation of Object Linking and Embedding packages. Other applicable controls include:1654, 1667, 1668, 1669, 1670, 1412, 1585, 1655, 1621, 1622, 1664, 1665
5	**Restrict administrative privileges**	ZIA can block administrative accounts from reaching the web or emails.	1175: Technical security controls are used to prevent privileged users from reading emails, browsing the Web and obtaining files via online services. Other applicable controls include: 1507, 1647, 1648, 1508, 1653, 1380, 1687, 1688, 1689, 1649, 1387, 1685, 1686, 1509, 1651, 1650, 1652
6	**Patch operating systems**	ZIA can be configured to only allow patches from known and approved patching sites.	1694: Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Other applicable controls include: 1695, 1696, 1701, 1702, 1407, 1501

	Essential Eight Requirement	Zscaler Complementary Capability	Information Security Manual Control References
7	**Multi Factor authentication**	Zscaler integrates with all the leading single sign-on (SSO) and federated identity management vendors. Zscaler also allows organisations to provide their own authentication solution. Which enables the deployment of multi factor authentication.	1504: Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. 1173: Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Other applicable controls include: 1679, 1680, 1681, 1505, 1401, 1682, 1683, 1684
8	**Backups**	ZPA can be configured to limit the user's ability to only store their backups using specific applications (and therefore align with organisational standards).	1511: Backups of important data, software and configuration settings are performed at least daily Other applicable controls includes: 1515, 1705, 1706, 1707, 1708

*ZIA/ZPA provide complimentary control assurance for the Essential 8. Zscaler provides an industry best practice service that enhances Internet gateway security for agencies of all sizes. Not only allowing for controlled access to approved sites, malware protection and ensuring users authenticate before being able to access external services. Zscaler also provides extensive logging capabilities of both what sites were accessed and what data was either uploaded or downloaded by the end user.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Branch Office, Austraila
Level 35 Tower One, 100
Barangaroo Avenue
Sydney NSW 2000
+61 2.9225.7864

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com