jamf

WHITE PAPER

Essential 8 Strategies to Mitigate Cyber Security Incidents

Organisations are continuously exposed to an everchanging landscape of cyber security risks. The Australian Cyber Security Centre (ACSC) has created eight key mitigation strategies as an essential baseline – the Essential 8 – to help prevent cyber security incidents. This guide from Jamf — the standard in Apple enterprise management — will discusses how Jamf solutions align to the Essential Eight Maturity Model.

WHAT IS THE ESSENTIAL 8?

First published in 2017, the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has developed a set of recommended strategies to help organisations mitigate cyber security incidents. The most effective of these recommendations have been collated into eight strategies.

The Essential 8 strategies recommend a specific implementation order. However, strategies can be customised based on an organisation's risk profile and the antagonists that concern the organisation most. Learn how Jamf solutions align to the Essential 8 Maturity Model.

If you're new to Apple security and just want the basics, please see our e-book **Apple Device Security for Beginners.**

Essential 8 Migration Strategies

- Application Control
- Patch Applications
- Configure Microsoft Office Macros
- User Application Hardening
- Restrict Admin Privileges
- Patch Operating System
- Multi-Factor Authentication
- Daily Backups

Prevent malware delivery and execution

Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.

Jamf offers:

- Management of Gatekeeper/Protect - Apple approved applications via Mac App Store, or identified developers
- Manage configuration Profiles and Policies to configure blocklist or safelist of approved applications
- Power to deploy third party tools - Jamf integration with Security tools to further provide restrictions

Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

Jamf offers:

- Ability to deploy and manage App Store Applications
- Jamf Patch management (monitor and deploy, update)
- Jamf Patch management reports, test, manage dependencies for over 60+ titles
- Option to use External Source (Inhouse and/or Community) for patch titles

Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

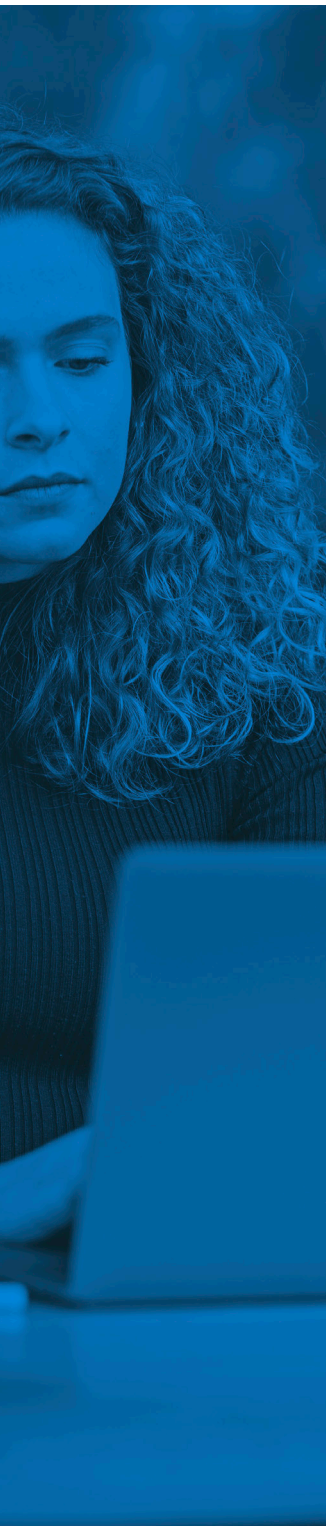
Jamf offers:

- Microsoft provide growing list of preference keys to manage preferences
- Manage MS Office through the use of Configuration Profiles within Jamf Pro (Application Schema)

User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

Jamf offers:

- A rich list of Configuration Profiles to manage environment
- Powerful policy engine provides system to customise application
- Customised Extension attributes provide rich reporting and notification features
- Implement Agency guidelines to provide security baseline (CIS examples)



Limit the extent of cyber security incidents

Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

Jamf offers:

- Jamf Binary runs as privileged account
- Self Service trigger for policies not requiring elevated user privileges
- Ability to report on local account privileges

Patch operating systems Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

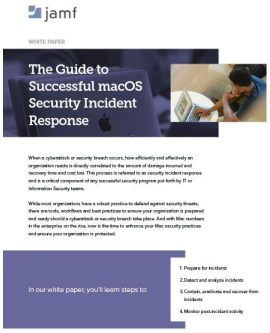
Jamf offers:

- Built-in patch management
- Options to configure profiles to manage OS patching
- Automatic creation of notifications of compliance

Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

Jamf offers:

- Intune integration - Conditional Access
- SAML integration - Self Service, User Initiated Enrolment



Read our whitepaper on **The Guide to Successful macOS Security Incident Response.**

Recover data and system availability

Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

Jamf offers:

- Pre-configure agents and application management
- Deployment of third party applications and agents

Conclusion

Jamf makes it easy to implement and follow the Australian Cyber Security Centre's Essential Eight Strategies to Mitigate Cyber Security Incidents.

To put these security features to the test, request a Free Product Trial.