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.**

Prevent malware delivery and execution

Application control to prevent execution of unapproved/malicious programs including Apple shell script and installers.

- Jamf Pro manages Gatekeeper/XProtect - Apple approved applications via Mac Apps Store or identified developers
- Jamf Pro can deploy within Configuration Profiles settings for Restricted Software that manages safelist approved applications or blocklist.
- Power to deploy third party tools - Jamf integrations with Security tools to further provide restrictions
- Jamf Protect monitors and alerts in real-time to detect, block, and quarantine malicious processes on macOS devices

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 Pro's ability to deploy and manage App Store Applications including the enforcement of auto-update to latest version provided by Apple's App Store.
- Jamf provides patch management reports for over 80 titles including managing dependencies
- Jamf Pro includes Patch Management for monitoring compliance and deploying updates
  > Option to use External Source (Inhouse, Community) for patch titles
- Device compliance and conditional access integration to Microsoft End Point Manager with Jamf Pro. If a device is not compliant, the user is notified and easy remediation via the Jamf Self Service Application
- Jamf Protect monitors and reports on malicious applications and updates to ensure patches are from trusted sources

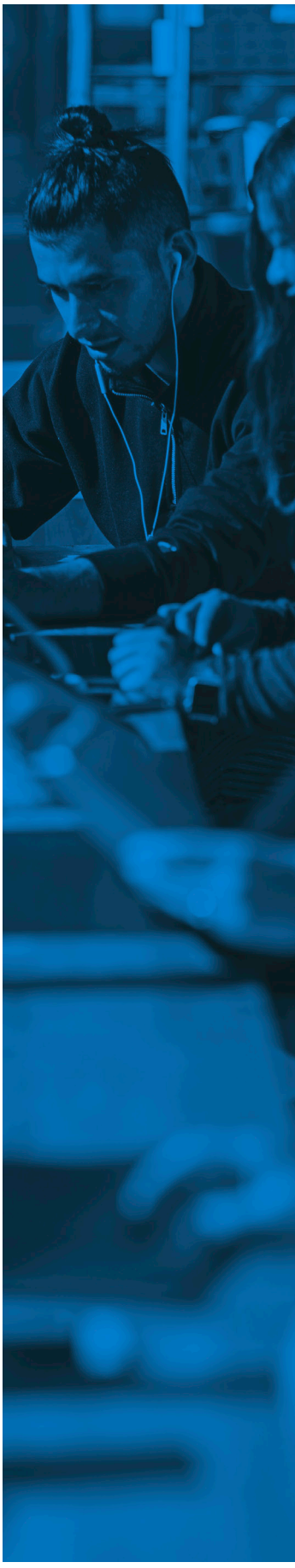
Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

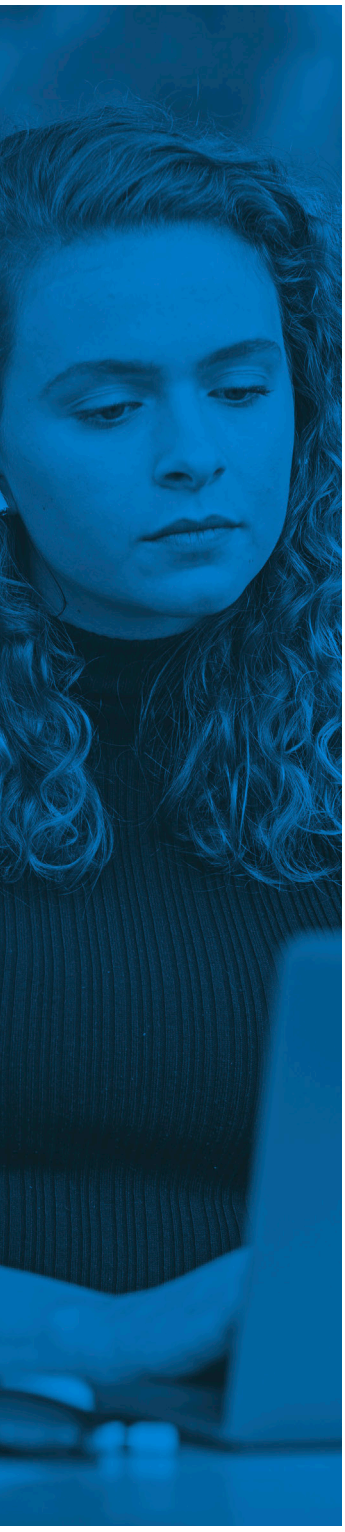
- Microsoft provide growing list of preference keys to manage preferences
- Manage MS Office through the use of Configuration Profiles within Jamf Pro (Application Schema)

Jamf Protect monitors downloads for malicious files and files with executables with Microsoft Office macros, alerts and provides detailed reporting that can be sent into 3rd party Security Information & Event Management (SIEM) tools.

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 Pro rich list of Configuration Profiles to manage macOS device settings and various application settings
- Jamf Pro Policy engine provides a system to customise application settings
- Jamf Pro Extension Attributes provide detailed reporting and notification features
- Implement Agency guidelines to enforce security baseline (CIS examples)
- Jamf Protect monitors, detect, block, and quarantine malicious processes
- Jamf Protect Insights provide CIS benchmark reporting and other security incident alerts





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 Pro binary runs as privileged account granting system level access to management only functions
- Self Service trigger for policies not requiring elevated user privileges
- Jamf Pro's ability to report on local account privileges
- Jamf Protect monitors the settings and usage of the login window and guest accounts on macOS devices
- Jamf Protect reports on privilege (sudo) escalation, failed password attempts and collate Unified Logging

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 Pro Patch Management built-in
- Jamf Pro utilizes Apple's MDM commands to enforce OS updates on Supervised macOS devices
- Jamf Pro features creating automatic notifications of compliance
- Jamf Protect reports on macOS version, and other macOS built in security tools (i.e. XProtect, MRT) for total visibility into malicious activity and status.

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 Pro Intune integration - Conditional Access
- Jamf Pro SAML integration - Self Service, User Initiated Enrolment
- Jamf Connect enables authentication with a cloud identity provider (IdPs)
- Jamf Connect enables enforcement of multifactor authentication (MFA) requirements

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.

- Use Jamf Pro to deploy and configure backup software or agents, with enforced corporate settings

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.