jamf

Jamf & the **Essential 8**

Strategies to Mitigate Cyber Security Incidents for Apple devices

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 series of baseline mitigation strategies to help organisations mitigate cyber security incidents - The Essential 8. To assist organisations with their implementation of the Essential 8, four maturity levels have been defined and are based on mitigating increasing levels of an adversary's tradecraft and targeting.

While the Essential Eight is designed to protect Windows endpoints. many organisations require the same controls for their Apple devices. The Essential 8 will not stop adversaries from compromising an organisations overall cyber security posture if they invest time, money, and effort to compromise a target. Organisations should consider the Essential 8 as part of the 360-mitigation strategy approach.

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

Prevent malware delivery and execution

1. Application control to prevent the execution of executables, software libraries, scripts, installers or control panel applets on workstations from within standard user profiles.

Jamf offers:

- Monitoring, alerts, real-time blocking malware, and quarantine of malicious apps and process with support for custom block lists
- Application management - Apple approved apps via App Store or identified developers
- Configuration Profiles and policies to configure blocklist or safelist of approved applications
- Detection and alerts for malicious command and control (C2) communications enabled to be exported and centrally logged to a SIEM / SOAR

2. Patch applications. Apply patches, updates or vendor mitigations for security vulnerabilities in applications.

Jamf offers:

- Risk assessment of applications with continuous version checking to detect and report apps that are outdated or vulnerable
- Deployment and management of applications including the enforcement of auto-update to latest version provided by Apple's App Store
- App Installers, which automatically package, host, deploy and update third-party apps when a new version is available
- Identification of malicious sites to block risky application downloads on protected devices

3. 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:

- Enforce management of Microsoft Office macros with robust array of preference keys
- Monitoring and alerts for downloads of malicious files and files with executables containing Microsoft Office macros
- Detailed reporting that can be sent into 3rd party Security Information & Event Management (SIEM) tools

4. User application hardening. Block access to risky sites. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

Jamf offers:

- A rich list of configuration profiles to manage devices and application settings
- Web content filtering to block web advertisements and unapproved sites
- Monitoring, detection, blocking and quarantine of malicious processes
- Policy engine to enforce security benchmarks like CIS and NIST
- Customised extension attributes to provide rich reporting and notification features

Limit the extent of cyber security incidents

5. Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges.

Jamf offers:

- Self service trigger for policies not requiring elevated user privileges
- Reporting on local account privileges, privilege escalations, failed password attempts and collation of unified logging
- Zero Trust Network Access (ZTNA) to limit application access via identity-based assertions
- Device risk assessments are factored into access policies, ensuring that least privilege access is enforced

6. Patch operating systems. Patch or mitigate devices and mobile devices with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

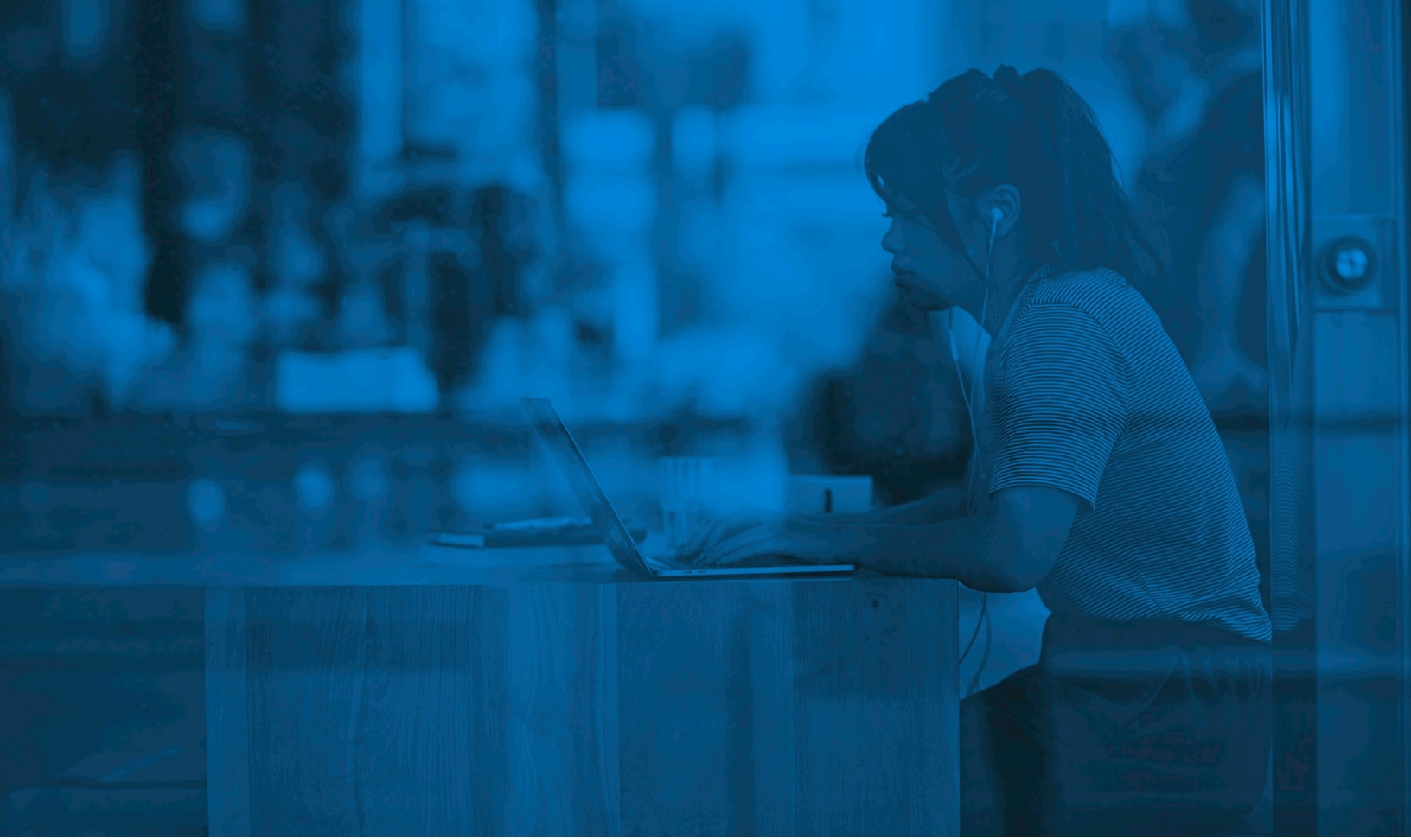
Jamf offers:

- Patch management to enforce OS updates on Apple devices
- Device hygiene checks, including vulnerable OS, risky profiles, jailbreak/rooting and more
- Reporting on OS version and built-in security tools for total visibility into malicious activity and status
- Risk-based application access policies for devices with 'extreme risk' OS vulnerabilities

7. Multi-factor authentication including for VPNs, RDP, SSH and other remote access for all users performing a privileged action or accessing an important (sensitive) data repository.

Jamf offers:

- IP-based multi-factor to authenticate users to any internet-facing service
- Cloud Identity authentication, password sync, and use of MFA with one-time passwords.
- ZTNA for SaaS or Enterprise apps, enforce principles of least privilege access through MFA identity assertions.
- Microsoft Conditional Access integration
- SAML integration - Self Service, User Initiated Enrolment



Recover data and system availability

> **8. Daily backups** of important data, software and configuration settings, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
>
> **Jamf offers:**
>
> - Enforcement of connections to backup facilities protected using Zero Trust Network Access policies and only approved backup services are utilized
> - Category-based content filtering that enables organizations to restrict access to Shadow IT services, such as unapproved cloud and file storage services.

Conclusion

Jamf makes it easy to implement and follow the Australian Cyber Security Centre's Essential 8 Strategies to Mitigate Cyber Security Incidents.

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