Devicie

Devicie Essential Eight: CAPABILITIES STATEMENT

INTRODUCTION

Australia's private sector cybersecurity investment is set to reach $4.6 billion by 2025[1], fuelled by the rise in volume and sophistication in security incidents, including ransomware, across industries.

With most enterprises now adopting some form of ongoing remote working arrangements, the need and demand for more robust security to protect employee devices has never been greater.

The Essential Eight Maturity Model from the Australian Cyber Security Centre (ACSC) – also known as the ASD Essential 8[2] – is widely accepted as a critical defence that every organisation should leverage in their fight against cyber crime.

Despite its importance, many organisations struggle to implement the Essential Eight controls effectively.

This document outlines how Devicie helps organisations to quickly implement key ASD Essential Eight controls on end-user devices.

CONTENTS

The Devicie difference

Devicie automates an uncompromising level of end-user device security for organisations and does this in a way that provides a radically better enablement and management experience for end users and IT teams. Devicie's cloud-native solution delivers a modern workplace as a service, solving the security versus productivity dilemma for end-user devices.

When it comes to security, Devicie automates defence in depth, including up to 300 security controls, across an organisation's end-user device fleet. This assists organisations in meeting maturity levels 1, 2 and 3 across each of the Essential Eight controls on end-user devices.

Devicie's Essential Eight capabilities are outlined below.

ASD Essential Eight

1 Application controls

- Devicie can control the execution of applications and components on workstations through Windows Defender Application Control and Applocker.
- Devicie can also provide basic risk assessment guidance on new application requests and on the back-catalogue applications.
- Through these technologies, Devicie can help organisations achieve Levels 1 through 3 on the employee endpoints.

2 Patch applications

- Devicie provides patches for applications available through Microsoft Intune within 24-48 hours of release and enforces updates on a standard 30/60/90 day cycle.
- Devicie can tailor release of patches and updates to suit the Essential Eight two-week cycle for third party applications, meeting the Level 2 requirements for workstations.
- Devicie can expedite urgent patches through the Intune ecosystem as required in 8-24 hours.

ASD Essential Eight

3 Configure Microsoft Office macro settings

- Devicie can control Microsoft Office macros at the user and machine level and enforces these controls at the end-user device.
- Through management of the native Office defences, Devicie enables organisations to achieve Level 3 maturity.

4 User application hardening

- Devicie can enforce browser, office and third party software configurations and settings where available.
- Devicie can deny-list and remove deprecated or risky applications, such as IE11 and PowerShell 2.0, achieving Level 3 requirements.
- Additional software security controls can also be applied for key applications such as Acrobat Reader.
- Devicie can provide the appropriate intel feeds to support the SOC in alerting and acting on possible violations and attacks.
- Devicie can support all of the controls one end-user devices to Level 3 maturity for organisations that require them.

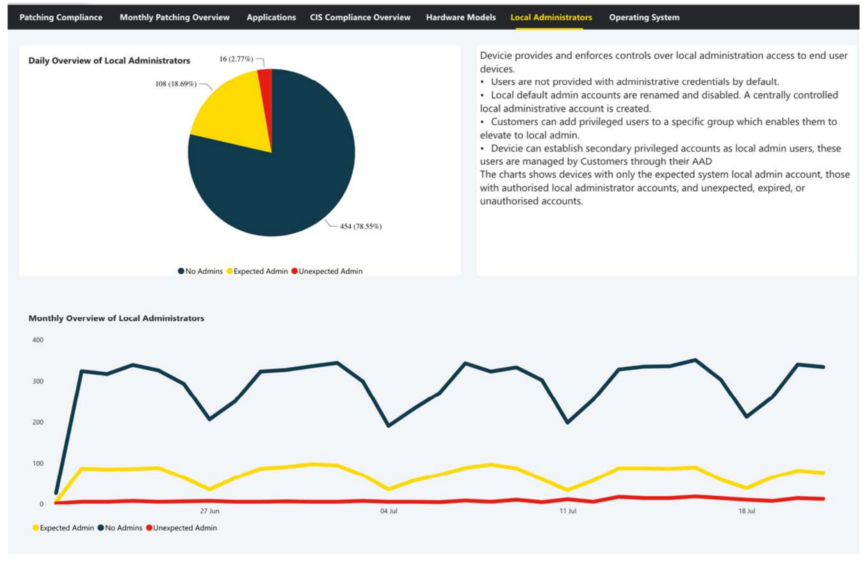
Devicie harnesses the power of automation to enable organisations to apply defence in depth controls across their end-user devices.

5 Restrict administrative privileges

- Devicie provides and enforces controls over local administration access to end-user devices.
- Users are not provided with admin credentials by default.
- Local default admin accounts are renamed and disabled. A centrally-controlled local admin account is created.
- Customers can add privileged users to a specific group which enables them to elevate to local admin.
- Devicie can establish secondary privileged accounts as local admin users. These users are managed by customers through their AAD.
- Through these controls, Devicie can help organisation configure their administrative access to end-user devices in line with maturity Levels 1 to 3.

DEVICIE DASHBOARD:
Restrict Administrative Privileges

This sample dashboard shows telemetry over the preceding month on the number of end-user devices with only the Devicie system admin account, those with known and authorised individual admin accounts, and those with unknown, unauthorised or unexpected admin accounts.


Patching Compliance
Monthly Patching Overview
Applications
CIS Compliance Overview
Hardware Models
Local Administrators
Operating System
Daily Overview of Local Administrators
16 (2.77%)
108 (18.69%)
454 (78.55%)
● No Admins ● Expected Admin ● Unexpected Admin
Monthly Overview of Local Administrators
400
300
200
100
0
27 Jun
04 Jul
11 Jul
18 Jul
● Expected Admin ● No Admins ● Unexpected Admin

Devicie provides and enforces controls over local administration access to end user devices.

- Users are not provided with administrative credentials by default.
- Local default admin accounts are renamed and disabled. A centrally controlled local administrative account is created.
- Customers can add privileged users to a specific group which enables them to elevate to local admin.
- Devicie can establish secondary privileged accounts as local admin users, these users are managed by Customers through their AAD

The charts shows devices with only the expected system local admin account, those with authorised local administrator accounts, and unexpected, expired, or unauthorised accounts.

ASD Essential Eight

6 Patch operating systems maturity

- Devicie makes patches for the operating systems available through Intune within 24-48 hours of release and enforces updates on a standard 30/60/90 day cycle.
- As with the application updates, Devicie can tailor release of patches and updates to suit the Essential Eight 2-week cycle, meeting the Level 2 requirements for end-user devices.
- Devicie can enforce migration to latest operating system releases within required time windows and provides a pilot programme over the first 14 days of release to achieve this.
- Devicie only deploys supported operating systems, ensuring compliance with the Level 3 requirement.

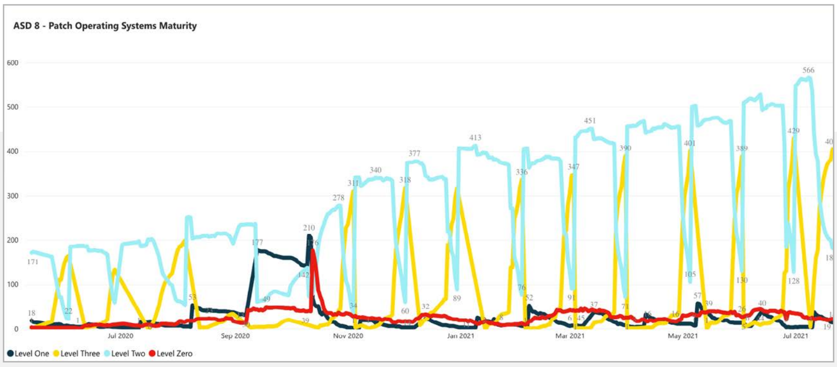
The following sample dashboard chart shows the Patch Tuesday cycle as updates are tested through the pilot group and then rolled out to the broader user base. The graph shows issues with a patch in October 2020 affecting a legacy business-critical application resulting in a pause in the schedule before resolution and return to the normal patching cycle.

7 Multi-factor authentication maturity

- This is largely out of scope for Devicie, as it is focussed at the workstation for devices accessed through AAD accounts, and therefore cannot enforce meaningful controls over MFA ASD8 requirements.
- However, with additional Intune API rights, Devicie can monitor and report on MFA status across user accounts.
- This auditing and logging, and associated visualisations, is pivotal for organisations to achieve Level 1 to 3 maturities.

8 Regular backups maturity

- Devicie ensures user data is located on cloud storage, such as OneDrive, and as a result it subject to the versioning controls and backups inherent to the services.
- Software and configuration are packaged within Devicie, allowing for rapid rebuild of workstations and their return to a 'known good' state in the event of a failure or other loss of integrity or data.
- This supports persistence of data, and restoration of end-user devices and configurations, assisting organisations with their data recovery and business continuity strategies and solution, key aspects of successfully implementing regular and reliable backups to meet maturity Levels 1 to 3.



DEVICIE DASHBOARD:
Patch Operating Systems

Contact us for a chat.

We'd love to walk you through our platform and answer questions pertaining to your environment.

[1] GlobalData

[2] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

ABOUT DEVICIE

Devicie automates an uncompromising level of end-user device security for organisations, and does this in a way that provides a radically better enablement and management experience for end users and IT teams. We have solved the security versus productivity dilemma for end-user devices, with a cloud-native solution that delivers a modern workplace as a service.

Website	devicie.com
Email	askus@devicie.com
LinkedIn	in