APNIC

Corporate Device Management

Brad Hosking

Using Zoom for this webinar

- Keep chat settings to “All Panellists and Attendees”
- Use chat to share text, information, URLs amongst all attendees
- If you wish to ask a question to the presenters:
  - Click the Q&A button
  - Type your question
  - The presenters will then answer your questions at an appropriate time
  - Note: Only the presenters will see your question, not other attendees
  - Please don’t use chat to ask questions of the presenters, we might not see it

Corporate Device Management – Securing your employees devices

Overview

Overview

- Why Device Management is important
- What type of device management software is out there?
- Stakeholders
- Management of different OS
- Our Journey
- Q&A

Corporate Device Management – Securing your employees devices

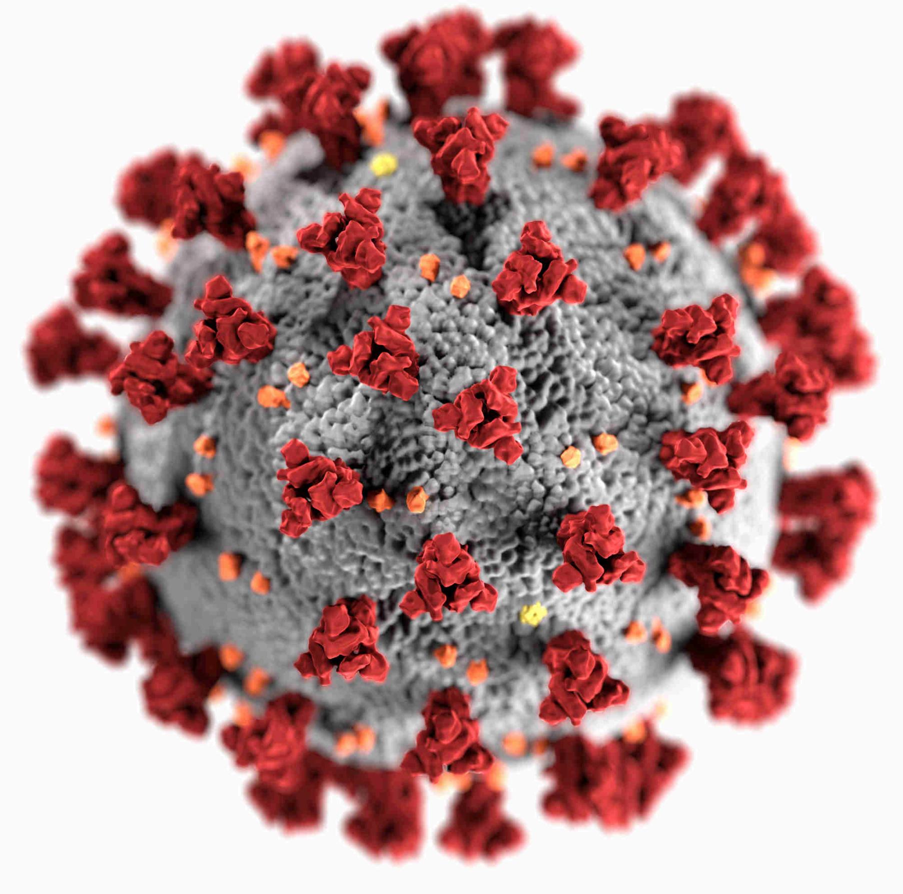
Why Device Management is Important

Why?

- Layered security approach
- Visibility
- Automation/Deployment
- Reduction in IT Costs
- Productivity
- Compliance/Governance

NETWORKING FROM HOME

And this happened…



- Workforces need to be able to work from anywhere reasonable
- IT Admins don't control these networks
- Statistics 2 in 5 people* WFH in Feb 2021 (41%)
- Increased productivity
- Issues with servicing devices no longer in an office

*A year of COVID-19 and Australians work from home more | Australian Bureau of Statistics (abs.gov.au)

https://www.abs.gov.au/media-centre/media-releases/year-covid-19-and-australians-work-home-more

Corporate Device Management – Securing your employees devices

Device Management Solutions

Where to start?

Intune

jamf

Microsoft® System Center™ Configuration Manager

vmware® airwatch®

jumpcloud™

kandji

MobileIron

Miradore

Things to consider

- Are you cloud/hybrid or only on-premise?
- Are you on premise but need to go cloud/hybrid?
- Configuration options
- Compliance reporting
- Separate reporting or consolidated if multi-OS?
- Managed updates
- Automations
- Integrations
- Do you have systems with this solution already?

Corporate Device Management – Securing your employees devices

Stakeholders

Stakeholders

- Consider all stakeholders
- Communication
- Consider an ITSC
- Know who is accountable
- Advise what is monitored
- Culture

Corporate Device Management – Securing your employees devices

MacBook + Windows + Mobile = Challenge

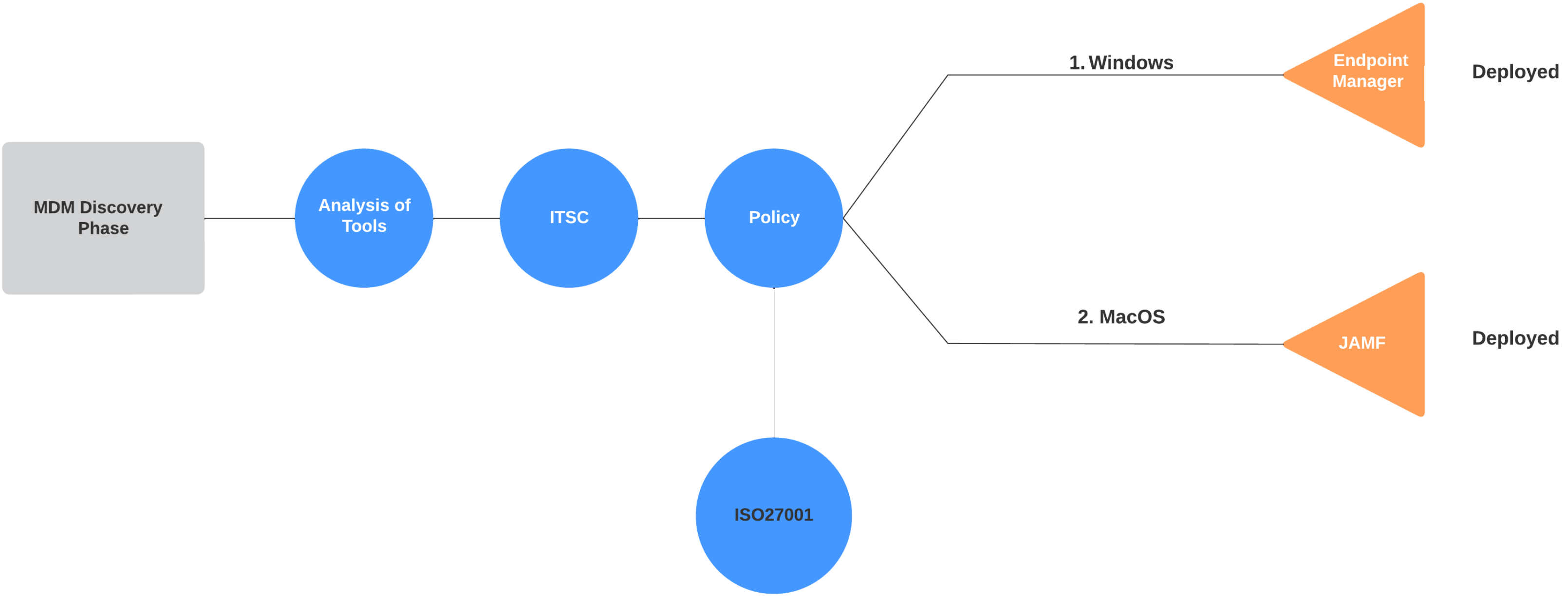
How hard is Multi-OS?

- Some MDMs don’t cover all options
- Supporting two solutions might be an option
- Having two options is more $$$
- More administration required
- Possibly simpler admin with dedicated solutions
- It can be done!

Corporate Device Management – Securing your employees devices

Our Journey

Deployment Roadmap



Analysis

- What type of solution will we be managing
  - Cloud managed
- What do we need to manage?
  - Windows 10/11
  - macOS
  - iPads (Corporate)
- What did we have that we could already use?
  - Microsoft 365 – Microsoft Endpoint Manager (Intune)
- Could the tools we have manage these solutions?
  - Windows & iPad
  - macOS (but with issues)

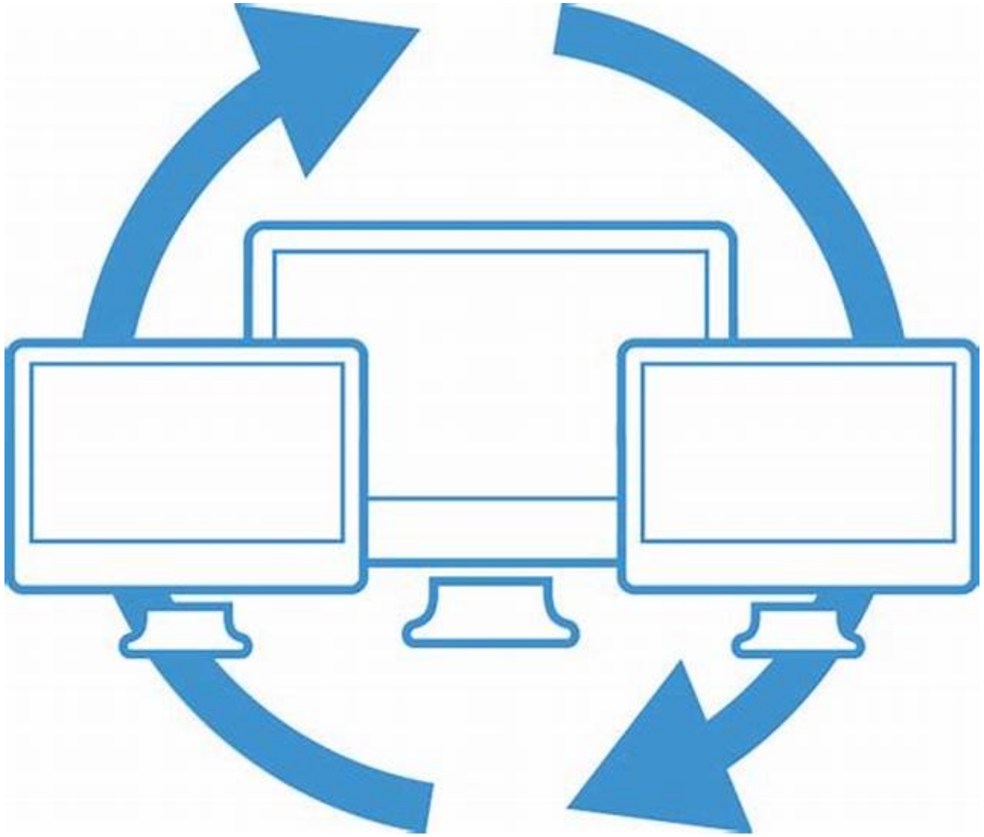
Outcome of analysis

- Windows
  - Microsoft Endpoint Manager fulfilled all requirements
  - Reporting via solution ensured compliance
- iPad
  - Microsoft Endpoint Manager fulfilled all requirements for both management and app deployment
  - Reporting via solution ensure compliance
- macOS
  - Microsoft Endpoint could deploy, however, application management was not easy
  - No SSO integration via Microsoft Endpoint Manager
  - JAMF Pro and JAMF Connect chosen as it fulfilled all requirements
  - JAMF Connect integrated SSO

ITSC & Policy

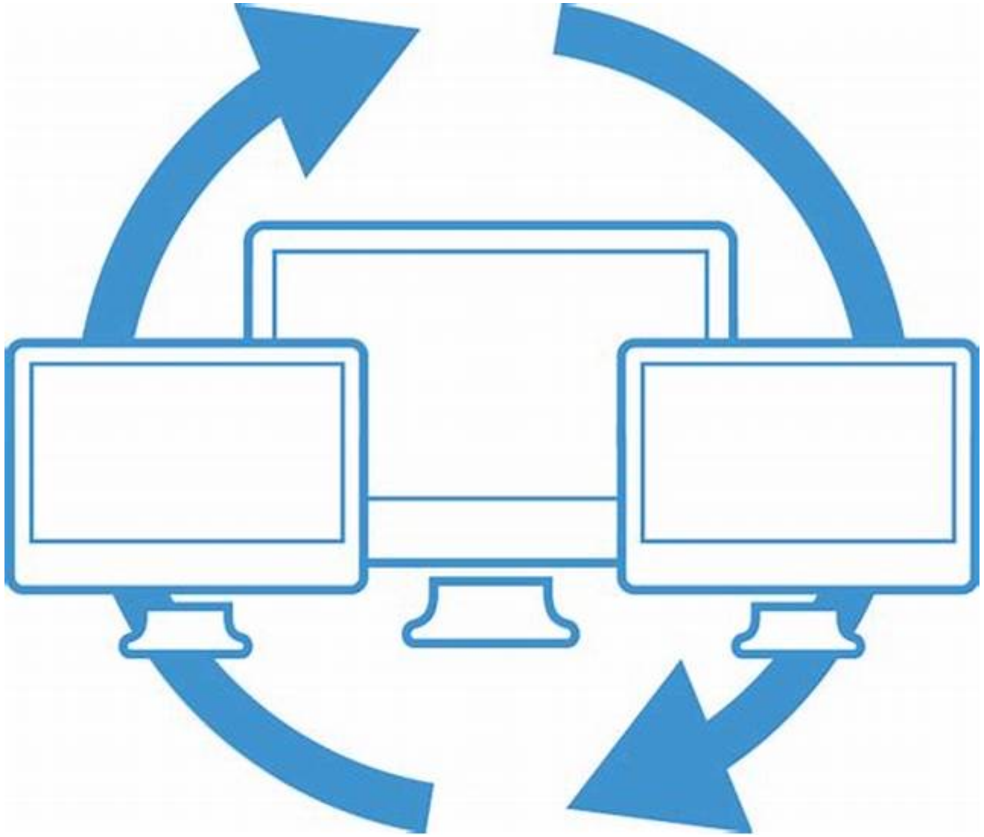
- ITSC to ensure that all parties were heard
- Policy driven – AUP which reflects on ISO27001 goals
- Security driven approach
- Selection of solutions integrate to current systems
- Compliance reporting
- Application reporting which reflected against the allowed apps

Deployment - Windows



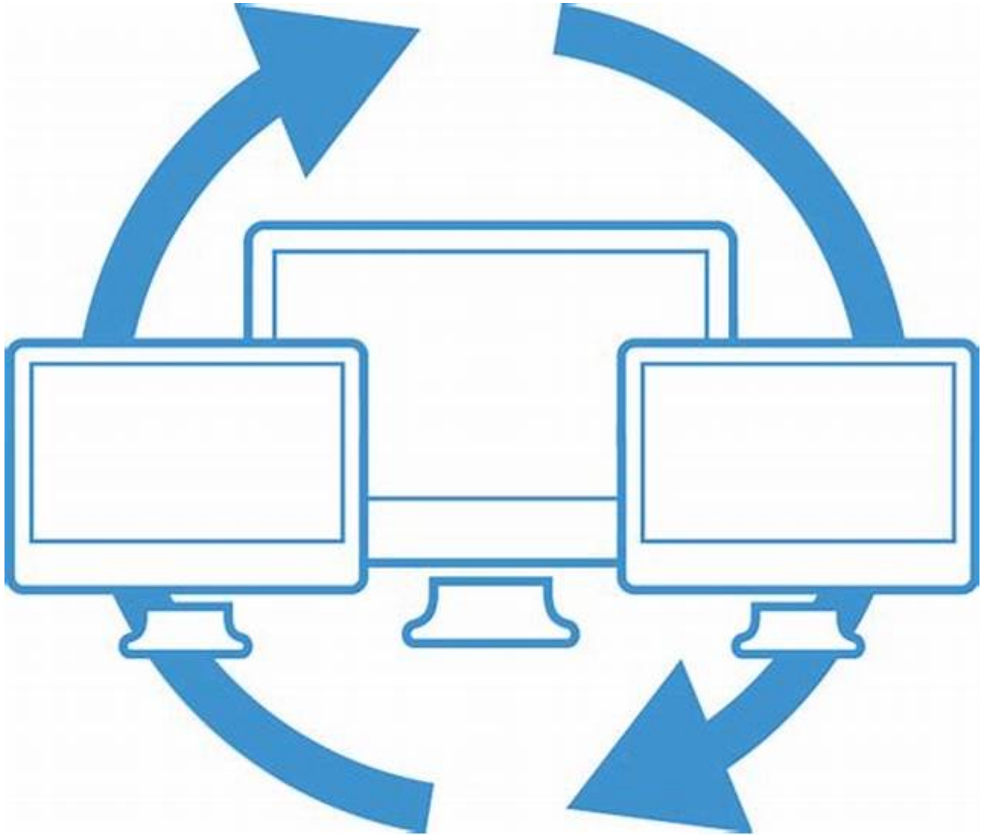
- Windows 10/11
  - Integrated to replacement program of devices
  - Azure AD Connected Devices
  - Integrated to Single Sign-On solution
  - Application deployment via MSI
  - Policy deployment
  - Autopilot enabled for new devices

Deployment - macOS



- macOS
  - Integrated to the replacement program of devices via ABM
  - Utilises JAMF Pro & JAMF Connect
  - Integrated to Single Sign-On
  - Integrated reporting/compliance
  - Policy deployment
  - Application deployment and upgrades using automation

Deployment – Mobile/Tablet



- Mobile/Tablet
  - Currently only corporate own devices
  - Deployed via Microsoft Endpoint Manager (Intune)
  - Application purchases centrally managed and deployed
  - Future BYOD options available.

Outcomes

- Security solutions integrated to all devices for both endpoint and SIEM.
  - Deployed via the MDMs to the devices
  - Configured by the MDM
- Visibility of devices out of scope
- Device locations not tracked by software
- Asset management simpler for physical devices and applications
- Applications now being updated weekly
- Management of OS upgrades controlled by IT

Challenges

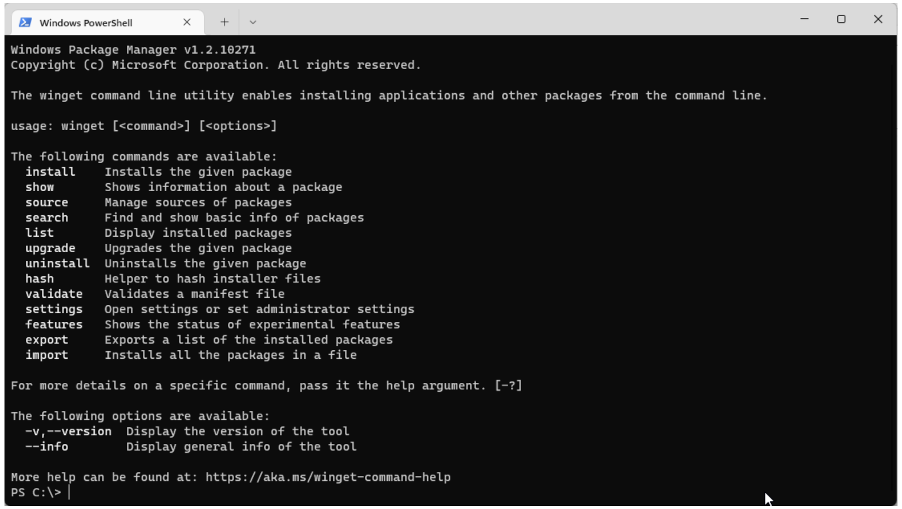
- Demographics of staff
  - Very IT savvy users
  - Staff had been managing their own devices for a long time (culture)
- User profiles in Windows
- Different operating system
- Budget
- Timeframe for rollout

Corporate Device Management – Securing your employees devices

Future Roadmap

Future roadmap

- Integrate devices with Device Trust for Zero Trust
- Change app deployment for Windows (MSI→ winget)
- Migration of automated updates in JAMF
- BYOD to allow for device trust for mobile devices
- Future integrations with SSO



```
Windows Package Manager v1.2.10271
Copyright (c) Microsoft Corporation. All rights reserved.

The winget command line utility enables installing applications and other packages from the command line.

usage: winget [<command>] [<options>]

The following commands are available:
  install    Installs the given package
  show       Shows information about a package
  source     Manage sources of packages
  search     Find and show basic info of packages
  list       Display installed packages
  upgrade    Upgrades the given package
  uninstall  Uninstalls the given package
  hash       Helper to hash installer files
  validate   Validates a manifest file
  settings   Open settings or set administrator settings
  features   Shows the status of experimental features
  export     Exports a list of the installed packages
  import     Installs all the packages in a file

For more details on a specific command, pass it the help argument. [-?]

The following options are available:
  -v,--version  Display the version of the tool
  --info        Display general info of the tool

More help can be found at: https://aka.ms/winget-command-help
PS C:\> |
```

Corporate Device Management – Securing your employees devices

Q&A

Thank You!