

8-2021

MANAGING AND SECURING ENDPOINTS: A SOLUTION FOR A TELEWORK ENVIRONMENT

David Adame

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/etd>



Part of the [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

Recommended Citation

Adame, David, "MANAGING AND SECURING ENDPOINTS: A SOLUTION FOR A TELEWORK ENVIRONMENT" (2021). *Electronic Theses, Projects, and Dissertations*. 1316.
<https://scholarworks.lib.csusb.edu/etd/1316>

This Project is brought to you for free and open access by the Office of Graduate Studies at CSUSB ScholarWorks. It has been accepted for inclusion in Electronic Theses, Projects, and Dissertations by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.

MANAGING AND SECURING ENDPOINTS:
A SOLUTION FOR A TELEWORK ENVIRONMENT

A Project
Presented to the
Faculty of
California State University,
San Bernardino

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
in
Information Systems and Technology

by
David Adame
August 2021

MANAGING AND SECURING ENDPOINTS:
A SOLUTION FOR A TELEWORK ENVIRONMENT

A Project
Presented to the
Faculty of
California State University,
San Bernardino

by
David Adame
August 2021
Approved by:

Conrad Shayo, PhD, Committee Chair

Jay Varzandeh, PhD, Committee Member

© 2021 David Adame

ABSTRACT

This project introduces a business problem in which a water utility company – known as H2O District – was forced to discover and implement a solution that would enable the IT Department to effectively manage and secure their endpoints in a telework environment. Typically, an endpoint is defined as any device that is physically connected to a network. For the purposes of this project, the endpoints that the IT Department was concerned with consisted of Windows 10 PC's, Laptops, and Apple iOS devices that employees use to access company resources while working outside of the corporate network. To properly manage endpoints, the IT Department was focused on being able to carry out their responsibilities for providing software deployments, software updates, operating system support, and remote support or troubleshooting. Regarding the security of their endpoints, the IT Department was concerned with being able to properly ensure endpoint compliance and provide adequate threat protection.

Ultimately a decision was made to utilize various cloud services from Microsoft to assist the IT Department with carrying out their responsibilities in the new telework environment. The project analyzed the cloud technology used, e.g., Microsoft Azure Active Directory, Endpoint Manager, a Cloud Management Gateway, Intune, and Microsoft Defender for Endpoint; and examined some of the current on-premises infrastructure technology such as Microsoft Endpoint Configuration Manager, Active Directory, VPN, and Group Policy. The project

also documented the implementation steps for configuring the cloud services and onboarding the endpoints to be properly managed and secured.

The contribution of this project is: (i) to show how the H2O district examined the H2O district's current infrastructure, (ii) identified any shortcomings with their current technological solutions, (iii) developed an understanding of the IT Departments service level agreements, and (iv) ultimately created a solution that allowed H2O to carry out its core responsibilities in the new telework environment. The project proved successful upon implementation and the IT Department was able to gain significant benefits by migrating some of their workloads to the cloud. The project also reports on some of the potential challenges the organization may face. Those include keeping up with the growing trend in hybrid remote work, managing the flow of information, and establishing zero trust. The solution implemented in this project can serve as an example for IT Departments facing similar challenges; namely, effectively managing and securing their endpoints in a telework environment.

TABLE OF CONTENTS

ABSTRACT.....	iii
LIST OF FIGURES.....	viii
CHAPTER ONE: INTRODUCTION.....	1
Background.....	1
Purpose.....	4
Problem Statement.....	5
CHAPTER TWO: ENVIRONMENTAL ANALYSIS.....	7
Chapter Overview.....	7
Organizational Overview.....	7
Current IT Environment.....	8
Desktop Support.....	9
Laptop Support.....	10
Mobile Device Support.....	11
On-Premises Management Infrastructure.....	12
Cloud Management Infrastructure.....	12
Managing Endpoints.....	16
Software Deployment and Updates.....	17
Operating System Support.....	19
Remote Support or Troubleshooting.....	21
Securing Endpoints.....	22
Device Compliance.....	22

Threat Protection.....	23
Problems with Current IT Environment	23
CHAPTER THREE: MIGRATION STRATEGY AND IMPLEMENTATION	25
Chapter Overview	25
Cloud Solutions.....	25
Microsoft Azure AD	26
Microsoft Intune.....	28
Configuration Manager and Cloud Management Gateway	30
Microsoft Endpoint Manager	33
Microsoft Defender for Endpoint.....	35
Azure AD Join Concepts.....	38
Azure AD Registered Devices.....	38
Azure AD Joined Devices	40
Hybrid Azure AD Joined Devices	41
Co-Management	43
Configuring Cloud Services	45
Microsoft Intune Configuration	46
Synchronize Intune with Apple Business Manager	47
Microsoft Defender for Endpoint.....	50
Getting Devices Into Intune.....	53
BYOD Devices	53
Corporate Owned Desktops and Laptops	55

Corporate Owned Mobile Phones	58
Viewing Devices in Endpoint Manager Admin Center.....	60
Viewing Devices in Microsoft 365 Security Center.....	61
Summary	62
CHAPTER FOUR: POST IMPLEMENTATION.....	63
Chapter Overview	63
New Endpoint Management Capabilities	63
Software Deployment and Updates.....	63
Operating System Support.....	65
Remote Support or Troubleshooting	67
New Endpoint Security Capabilities	70
Device Compliance	70
Threat Protection.....	71
CHAPTER FIVE: CONCLUSION.....	73
Chapter Overview	74
New Opportunities and Challenges	74
Growing Trend in Hybrid Remote Work	74
Managing the Flow of Information.....	76
Establishing Zero Trust	78
Conclusion	80
APPENDIX A: ACRONYMS AND ABBREVIATIONS	83
BIBLIOGRAPHY.....	85

LIST OF FIGURES

Figure 2.1 – H2O Districts Current Endpoint Architecture	9
Figure 2.2 – Microsoft 365 Enterprise Licensing Packages	14
Figure 2.3 – Cloud and On-premises Infrastructure Synchronization	16
Figure 2.4 – Configuration Manager Site Server and Distribution Point	18
Figure 2.5 – Windows 10 Semi-Annual Channel Current OS Support.....	19
Figure 3.1 – Azure AD Connect.....	27
Figure 3.2 - Microsoft Intune Overview and Architecture.....	29
Figure 3.3 – Cloud Management Gateway Architecture	32
Figure 3.4 – Endpoint Manager Architecture	33
Figure 3.5 – Microsoft 365 Defender Platform.....	36
Figure 3.6 – Azure AD Registered Device	39
Figure 3.7 - Azure AD Joined Device	40
Figure 3.8 – Hybrid Azure AD Joined Device	42
Figure 3.9 – Configuration Manager and Intune Co-Managed Architecture	44
Figure 3.10 – Successful Intune Tenant Enabled.....	47
Figure 3.11 – Creating an Apple MDM Push Certificate from within Intune	49
Figure 3.12 – Apple Business Manager Successfully Synched with Intune.....	49
Figure 3.13 – Apple Enrollment Program Token Synched with Intune	50
Figure 3.14 – Microsoft Defender for Endpoint Connected Successfully.....	52
Figure 3.15 – Microsoft Defender for Endpoint Devices Onboarded	52
Figure 3.16 – Application Protection Policy for BYOD Devices	54

Figure 3.17 – Azure Active Directory Join from Settings Menu	57
Figure 3.18 – Apple Business Manager and Intune Integration	59
Figure 3.19 – Assign Device to Intune in Apple Business Manager	59
Figure 3.20 – iOS Device Enrolled in Intune with Enrollment Profile Assigned ..	60
Figure 3.21 – Microsoft Endpoint Manager Admin Center	61
Figure 3.22 – Microsoft 365 Security Center	62
Figure 4.1 – Application Deployment Types in Endpoint Manager	64
Figure 4.2 – Autopilot Reset within Endpoint Manager	66
Figure 4.3 – Windows 10 Update Ring Defined.....	67
Figure 4.4 – TeamViewer Connector for Intune.....	69
Figure 4.5 – Remote Assistance Session Capability for Endpoint.....	70
Figure 4.6 – Device Compliance in Endpoint Manager.....	71
Figure 4.7 – Microsoft 365 Security Center Alerts	72
Figure 4.8 – Threat and Vulnerability Management Dashboard	73

CHAPTER ONE

INTRODUCTION

Background

The 21st century saw an influx in technological innovations that enabled us to interact, share ideas, and improve our overall productivity. Among some of those innovations are faster internet speeds, advancements in wireless connectivity, cloud services, and an endless number of endpoints to connect from such as desktops, laptops, cell phones, tablets, wearable technology, and various IoT (Internet of Things) devices. The number of devices that we use to connect, and share information continues to grow at a rapid speed and shows no sign of slowing. In fact, by the year 2025 it is predicted that over 40 billion devices will be connected to the internet – up from 21.7 billion in 2020 alone (Leuth, 2020). Ultimately, the endless number of endpoints presents a challenge for IT Departments across the globe and adds to the struggle of determining an effective way to manage these devices and ensure adequate endpoint security.

While some organizations have found a way to limit the number of endpoints through specific means by having control of their internal network, in the wake of the COVID-19 pandemic all of that has changed. Now for the first time, some organizations faced the task of moving most, if not all, of their operations into a telework environment. A recent annual endpoint survey from the SANS Institute in 2021 indicated that the COVID-19 pandemic caused 82% of organizations to report that now half their operations are remote – up from

13% only one year prior (Bromiley, p.2, 2021). This new environment presents a challenge for organizations at all levels given that the rise of remote workers correlates with a rise in endpoints now existing outside of the corporate network. IT Departments all over the world are now faced with the challenge of understanding how the new telework environment affects them, while at the same time determining which solutions will help them respond to such demands of a remote operation.

Endpoint management is a common task for IT Departments because endpoints – such as PC's, Laptops, Smartphones, and Tablets - are the primary areas in which end users access company resources. One of the reasons for managing an endpoint is to ensure that a device meets a specific configuration baseline required to reduce the risk of compromise. In fact, misconfiguration remained one of the top five causes of data breaches according to the 2020 Verizon Data Breach Investigations Report (Verizon, p. 13, 2020).

Another reason for managing and configuring endpoints is to ensure that an IT Department can carry out core responsibilities such as software deployment and updates, operating system support, and remote support or troubleshooting. Without a properly managed endpoint, an IT Department may find it difficult to assist customers to perform critical touch point job functions. Some examples of endpoint configurations would include ensuring a VPN configuration, enabling or disabling a specific computer policy, ensuring hard disk encryption, configuring access to resources, or deploying an application.

Regardless of where an endpoint physically exists, it is important for an IT Department to manage their endpoints and have visibility into their endpoints to provide adequate support and ensure proper configuration.

Endpoint Security is perhaps one of the more growing concerns and responsibilities of an IT Department. Not too long ago in a study from International Data Corporation (IDC), it was discovered that 70% of network breaches began on endpoint devices (Kirsch, 2016). Since then, IT Departments made significant strides in ensuring adequate endpoint security behind corporate firewalls by fortifying defenses against outside threats. Some of the common responsibilities for an IT Department when it comes to endpoint security can include ensuring device compliance and adequate threat protection. However, in the Post COVID-19 world the new environment in which endpoints and information now flows outside of the corporate firewalls poses a new challenge. In a December 2020 survey conducted by Forrester Consulting, some of the largest challenges facing IT leaders were: (i) being unable to maintain or prove endpoint compliance (59%), (ii) Unable to enforce security standards (53%) – such as configuration, vulnerability, and patch management – and, (iii) not knowing the health of their security controls (53%) (Forrester, p.5, 2021). With over half of IT leaders struggling to overcome endpoint security challenges, it is important to discover and implement solutions that can enable IT Departments to have full confidence in their endpoint security regardless of where an endpoint physically exists.

Purpose

This project will present a problem-solution based scenario in which a water utility company known as H2O District, consisting of over 1,300 employees and over 3,000 devices, were forced to assess their current environment and determine a path towards managing and securing endpoints in a telework environment. The project will take a dive into various products and services from Microsoft and provide a high-level overview of how the IT Department was able to implement these technologies to meet their current responsibilities. The products include cloud technologies such as Microsoft Azure, Endpoint Manager, Cloud Management Gateway, Intune, and Microsoft Defender for Endpoint. Additionally, the project will look at current on-premises infrastructure technologies such as Microsoft Endpoint Configuration Manager, Active Directory, VPN, and Group Policy. Throughout the project we will discover how each solution is able to help the H2O District's IT Department fulfill their responsibility of managing and securing the organization's endpoints in a telework environment.

The H2O District project will serve as an example for many other organizations of similar size or technological capacity. The project will demonstrate how these technological products are able to provide a solution for the IT Department by assisting them with managing and securing endpoint devices in a telework environment. The project will also explore new capabilities for the IT Department that it did not otherwise have before. By understanding

how these endpoint management technologies are used and implemented, IT leaders can begin to feel confident in their ability to manage and secure endpoints regardless of where they exist outside of their network.

Lastly, the project will conclude with some of the future challenges that the H2O District will face. It is not uncommon that many organizations will face a similar challenge with the increasing number of employees who are working from home. Some of the other challenges they will face is establishing and adopting an organizational strategy towards Zero Trust as well as Managing the flow of information across their endpoints. In essence, the solutions provided in this project will serve as a foundation for some of the future endeavors that any organization will face in a post COVID-19 pandemic environment.

Problem Statement

To gain a better understanding of the overall project needs, the following questions will be answered:

1. What are the current responsibilities of the IT Department and how can a solution(s) be developed to meet emerging responsibilities generated by a post COVID-19 pandemic telework environment?
2. What technological solutions exist in the current environment to allow the IT Department to effectively manage and secure endpoint devices in a telework environment?

3. How will the new technological changes affect the way the IT Department operates in a telework environment?

This project is organized as follows: Chapter 2 provides the Background and Analysis of the Project. Chapter 3 discusses Migration Strategy and Implementation. Chapter 4 will review the Post Implementation results. Lastly, Chapter 5 will Conclude by introducing future challenges and summarizing the results of the project.

CHAPTER TWO

ENVIRONMENTAL ANALYSIS

Chapter Overview

The purpose of this chapter is to understand the current IT operations and infrastructure that currently exists for H2O district. We will identify some of the current technology that the organization is using to manage and secure their endpoints and discuss the current level of service that the IT Department is responsible for so that the same level of service can exist in the new telework environment. Lastly, we will identify specific problems that exist within the IT Departments current operations and infrastructure, so that a new solution can be developed for managing and securing their endpoints in a telework environment.

Organizational Overview

A very brief overview of H2O District will be given to shed insight to the size of their operations. H2O District was established in 1958 and initially provided water services to around 48,000 residents. In 2021 the district is now responsible for serving water to over 1.2 million residents spread throughout a 555-mile radius. The H2O District has one main site where they conduct their business operations such as Customer Service, Human Resources, Public Services, Environmental Health and Safety, and Information Technology. H2O District also operates two remote sites that serve as their primary pumping and water treatment facilities. Most of the operations such as Engineering, Energy

Management, Water Quality treatment and Research and Development occurs at these two remote sites. H2O District Continues to grow and expand with projects to deliver safe and reliable drinking water to communities in its area of jurisdiction.

Current IT Environment

The current IT Department consists of 5 separate divisions: Applications Development, Network Administration, Information Security, and Information Governance, and *IT Customer Support*. This project will strictly focus on the responsibilities of the *IT Customer Support Division*. Although each Department has an overall responsibility, it is the IT Customer Support (ITCS) Division which is responsible for the initial configuration of managing and securing endpoints. Most of H2O Districts environment is designed to provide support for endpoints behind corporate firewalls within a trusted network. In Figure 2.1 you will see the areas in which H2O Districts endpoints are able to be serviced. Endpoints that reside behind the corporate firewall are able to be contacted and communicated with via clients that are installed onto the endpoints. Any endpoints that are located outside of the firewall – for example in a home, coffee shop, or hotel room – are unable to be properly managed or secured.

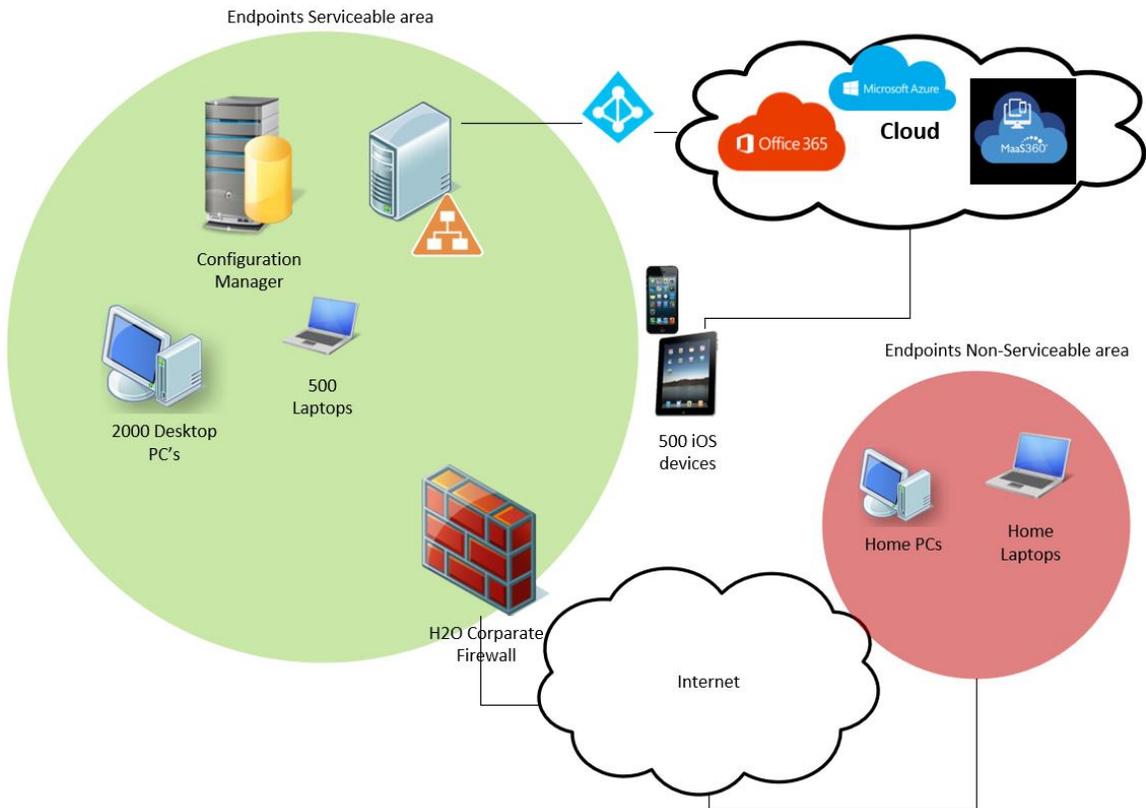


Figure 2.1 – H2O Districts Current Endpoint Architecture

Desktop Support

The IT Department unit is currently responsible for supporting just over 2,000 desktop PC's consisting of 5 different models, all currently no older than 5 years and are covered by an extended warranty. All the desktop PC's are currently running Microsoft Windows 10 Enterprise Operating System since support for Windows 7 ended on January 14, 2020 (support.micorosft.com, n.d). The IT Department routinely refreshes all their desktop PC's every 5 years – meaning that they retire the old system and replace it with a new system. Each

desktop PC is joined to the same domain, except for about 20 desktop PC's that run proprietary vendor applications and exist on a separate computer network.

The IT Department is not responsible for managing the desktops that are supported by the vendors. Although, there are about a dozen Apple iMac's running various versions of MacOS in the environment, support is limited and not required as part of the IT Departments Service Level Agreement.

Laptop Support

The IT Department is currently responsible for supporting over 500 laptops consisting of 5 different models running various versions of the Windows 10 operating system. End users regularly take their laptops onsite and offsite to perform work functions and access company cloud resources. Some end users such as managers or researchers are also given an elevated local administrator permission on their laptops which will allow them to perform tasks such as installing software and making system level changes. Upon arrival, the laptops are hooked up to the network and a standard version of Windows 10 Enterprise is deployed with a standard software configuration. Laptops are joined to the same Active Directory domain as the desktop PC's. Supporting the laptops is dependent on physically plugging the laptop into H2O's corporate network via the laptops ethernet port and which allows for line of site with the domain controller for authentication, as well receiving updates from the Configuration Manager server. Each laptop is also configured with a VPN connection that allows the user

to connect to onsite resources such as network drives. Users are constantly reminded to connect their laptops when on site to receive updates. Lastly, support for laptops is generally limited to walk-ins when the user is onsite since the laptops are unable to be serviced outside of the network as highlighted in Figure 2.1.

Mobile Device Support

The IT Department is also responsible for supporting just over 500 mobile devices which consist of Apple iPhones and iPads running various versions of iOS. The IT Department typically inventories the iPad and then issues the device to the end user. The current models are on a 3-year refresh rate, meaning that employees will receive a new phone every 3 years. There are currently 3 different models that require support from the IT Department. Typically, management personnel and field personnel are equipped with cell phones. The current responsibilities for the IT Department regarding the support for mobile devices is typically keeping track of who the device belongs to, pushing out a configuration profile, as well as assisting with troubleshooting via in-person support. The IT Department currently utilizes IBM MaaS360 which is a Mobile Device Management Solution for iOS devices. Additionally, the IT Department has an Apple Business Manager account, which essentially allows for the IT Department to synchronize their iOS devices to the IBM MaaS360 MDM solution. In Apples setup guide, the Apple Business Manager (ABM) is described as an

application that makes it “easy to automate device deployment, purchase apps, distribute content, and create Managed Apple IDs for employees” (Apple, 2019).

On-Premises Management Infrastructure

The IT Department is currently supporting a traditional on-premises infrastructure consisting of over 50 different servers both physical and virtual, A single Active Directory forest & domain, and a single datacenter that exists at their primary site of business. The IT Department routinely manages servers and keeps them up to date, with monthly patching cycles, and routine evaluation of upgrades, or retiring systems that no longer serve a purpose. Additionally, the IT Department uses both a single onsite and single remote site as a backup storage location to ensure business continuity in the event of a disaster or loss of operations at the main site.

Cloud Management Infrastructure

The H2O district has spent the last few years migrating some of their applications and services to Microsoft Azure’s cloud platform, primarily leveraging their Office 365 applications and Identity services. The organization utilizes a Microsoft 365 E5 licensing agreement with Microsoft. The Microsoft 365 E5 licenses allows for H2O District to utilize software services such as Office 365, which includes applications such as Word, Excel, PowerPoint, and Outlook and Microsoft Teams. The Microsoft 365 E5 license also allows for other services

that assist with Device and App management, Identity and Access management, Threat Protection, and Information Protection, Compliance and Security Management and much more (Microsoft, n.d). An overview of what is included in the licensing structure can be seen in Figure 2.1.

Microsoft 365 E5

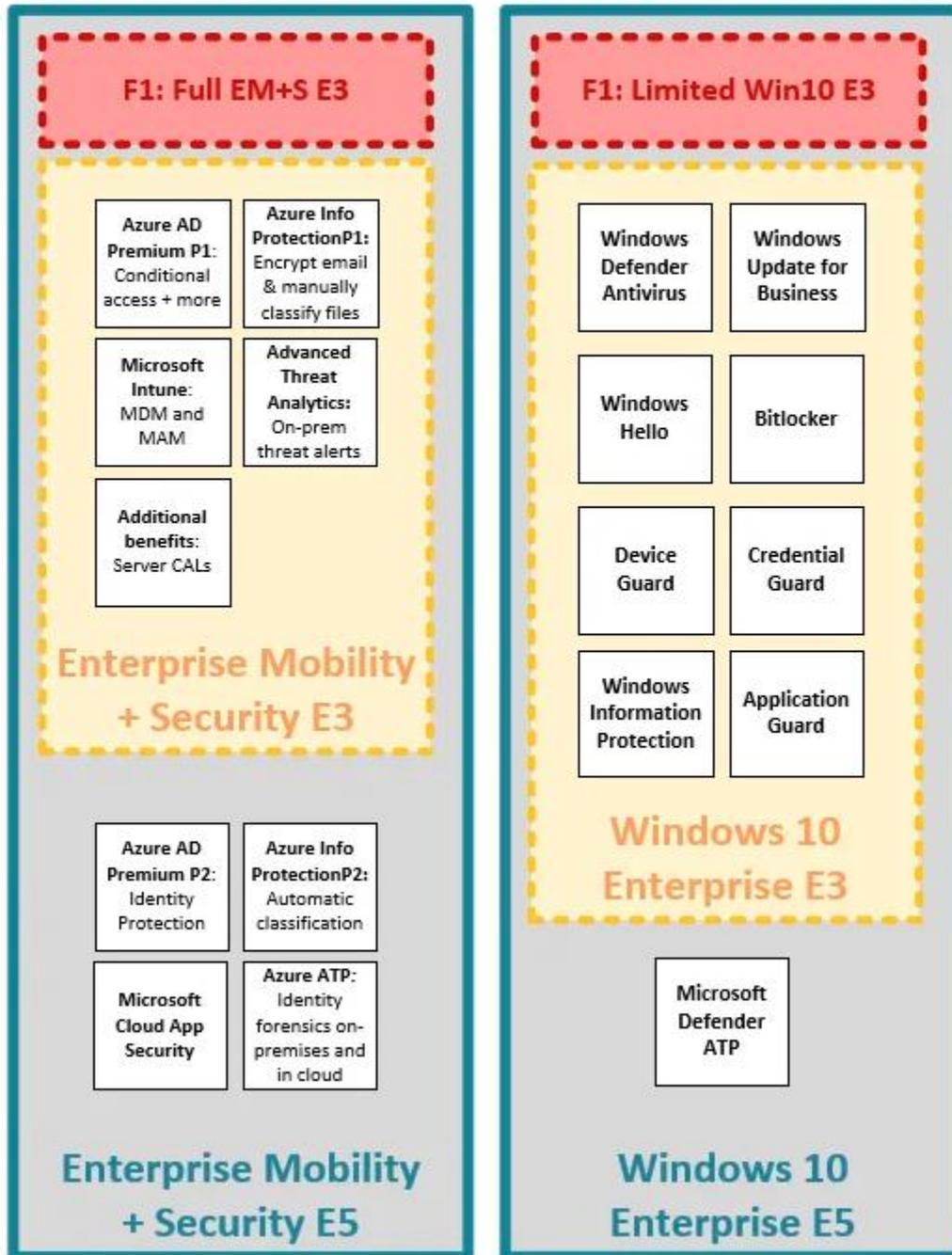


Figure 2.2 – Microsoft 365 Enterprise Licensing Packages (Fields, 2019)

The organization currently utilizes Active Directory Federation Services with support for Single-Sign On (SSO) for their on-premises devices – which allows users to access resources without constantly being prompted for credentials. Most Office 365 applications can be accessed from work, home, or any mobile device if a user authenticates with their username and password. As a prerequisite towards migrating to a hybrid infrastructure, H2O District synchronized their on-premises Active Directory Domain Services with their Azure AD tenant by using Azure AD connect, which allows their organization to utilize Microsoft’s cloud platform with Azure AD handling the identity and authentication within the cloud (Figure 2.3) while simultaneously continuing to operate using their existing Active Directory DS infrastructure and policies.

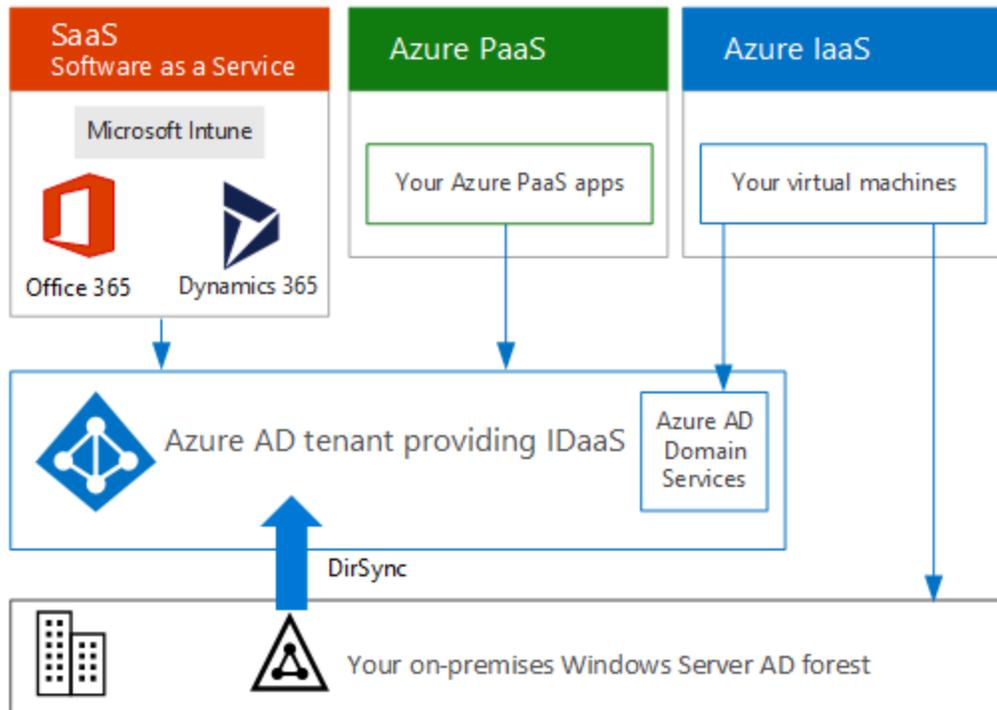


Figure 2.3 – Cloud and On-premises Infrastructure Synchronization

Managing Endpoints

The IT Department is responsible for providing a certain level of service when it comes to managing H2O endpoints. Much of the service level agreements are dependent on the existing endpoint architecture that is built behind corporate firewalls. Although there are many aspects to managing endpoints, for the sake of this project the IT Department is concerned with supporting the following core responsibilities which include Software Deployment and Updates, Operating System Support, and Remote Support or Troubleshooting.

Software Deployment and Updates

Software or Application Deployment is typically defined as “all of the steps, processes, and activities that are required to make a software system or update available to its users” (Sumologic, n.d). The IT Department currently uses two approaches when it comes to deploying applications to endpoints. About 75% of the IT Departments applications are currently deployed using Microsoft Endpoint Configuration Manager. The MS Configuration Manager allows applications deployment from a central location. The architecture allowing for this solution requires a centralized Configuration Manager site server and distribution point to be deployed, and clients to be installed on the endpoints as seen in Figure 2.4. The remaining 25% of the IT Departments applications are stored on a network share and are manually installed by technicians as a desktop PC or laptop is being prepped for an end user.

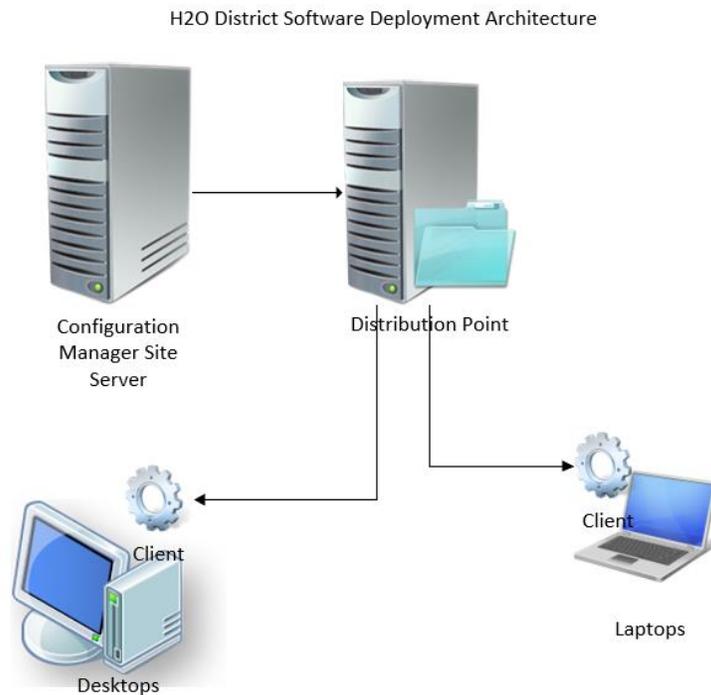


Figure 2.4 – Configuration Manager Site Server and Distribution Point

The IT Department is responsible for performing weekly software updates outside of business hours. Software updates can include a patch that fixes a bug in an application, an update that includes enhancements, or monthly security updates. The IT Department currently utilizes their Configuration Manager server to deploy software updates to their environment by creating an application or package and targeting the group of devices. For laptops, software updates are received when the laptop is connected to the network. Lastly, if a user is not a local administrator for laptops then a technician must assist with installing

software in-person given that there are no remote capabilities available for laptops.

Operating System Support

Support for Operating Systems (OS) is crucial in ensuring all endpoints are in compliance and up to date, or have the latest features enabled. This means the IT Department must be able to deploy the Windows 10 OS to all endpoints as well as patch the operating system. Microsoft releases feature updates to their OS every 6 months known as a Semi-Annual Channel which is seen in a screenshot from Microsoft’s website in Figure 2.5. This means that twice a year Microsoft will make significant enhancements to the front and back end of their Windows 10 OS by enabling more features for the end user. The OS that the IT Department currently supports is Windows 10 Enterprise, with different versions ranging from 1809 up to the current 20H2.release.

Semi-Annual Channel

Version	Servicing option	Availability date	OS build	Latest revision date	End of service: Home, Pro, Pro Education, Pro for Workstations and IoT Core	End of service: Enterprise, Education and IoT Enterprise
20H2	Semi-Annual Channel	2020-10-20	19042.928	2021-04-13	2022-05-10	2023-05-09
2004	Semi-Annual Channel	2020-05-27	19041.928	2021-04-13	2021-12-14	2021-12-14
1909	Semi-Annual Channel	2019-11-12	18363.1500	2021-04-13	2021-05-11	2022-05-10
1809	Semi-Annual Channel	2019-03-28	17763.1879	2021-04-13	End of service	2021-05-11
1809	Semi-Annual Channel (Targeted)	2018-11-13	17763.1879	2021-04-13	End of service	2021-05-11
1803	Semi-Annual Channel	2018-07-10	17134.2145	2021-04-13	End of service	2021-05-11
1803	Semi-Annual Channel (Targeted)	2018-04-30	17134.2145	2021-04-13	End of service	2021-05-11

Figure 2.5 – Windows 10 Semi-Annual Channel Current OS Support

The IT Department also maintains a customized operating system image of Windows 10 Enterprise that they deploy to each new desktop PC or laptop that arrives. As the IT Department retires old equipment and refreshes their environment, the new device is equipped with the latest Windows 10 Enterprise image. Each image that the IT Department deploys is typically configured with a standard application set, and often requires additional software to be installed during a post-imaging process. The latest image is constantly maintained and updated every six months with the release of new feature updates.

Occasionally, an OS will break and require the IT Department to perform a fix. If an OS breaks on a desktop device and cannot be repaired manually, then a technician will re-image the computer. Re-imaging the computer implies that the current OS and applications will be completely wiped, and that the latest version of the operating system image will be deployed. Re-imaging typically helps a computer that is simply not responding correctly or has symptoms of a corrupted operating system.

The IT Department uses Configuration Manager to assist with the imaging process. The latest version of the customized Windows 10 image is uploaded to the Configuration Manager, and then deployed via task sequence to the new device, using either a Pre-Boot Execution (PXE) environment via LAN, or a bootable media device such as a USB flash drive. Once the system is imaged then a technician will complete a post imaging process which requires that all the

application configurations, drivers, and services be working before allowing the end user to login.

Remote Support and Troubleshooting

Help Desk Technicians typically receive requests from end-users reporting issues with their devices or applications. Technicians must be able to support and troubleshoot desktop PC's remotely from their workstation. Remote support implies that a technician can see what their user is seeing and be able to take control of their user's device. Additionally, technicians must have the ability to perform remediations or assist their user with whatever issue they are experiencing. The technicians typically use Microsoft's built-in Windows 10 application known as Remote Assistance, or Remote Control through Configuration Manager when the user is available. If the user is unavailable, the technicians will use Microsoft's Remote Desktop application to connect remotely to the system.

The IT Department can only support endpoints that are connected directly to H2O's network. Often, end-users are forced to leave their laptop with an IT technician so that they can diagnose an issue that they are experiencing. When the laptops leave the network and are in the field, the end-users must wait until they arrive back onsite to receive support since there is not a remote solution available for troubleshooting.

Securing Endpoints

The IT Department is responsible for providing a certain level of security when it comes to their endpoints. Although there are many facets of endpoint security such as network access control, endpoint detection and response data loss protection, insider risk and conditional access, the IT Department is primarily concerned with ensuring device compliance and providing proper threat protection.

Device Compliance

IT Department is currently responsible for ensuring that a device is compliant with IT security policies and that each system is configured and secured properly. Most of the device compliance for on-premises devices are enforced setup via Group Policy. In essence, Group policy is responsible for enforcing what users can or cannot do on a system by adding or removing access to resources. Since desktops are joined to the same domain, group policies are applied at a domain-level, as well as separate organization units (OU's) depending on the function and for the computer system.

Additionally, the IT Department can use the Configuration Manager to push out specific software updates and configurations to ensure that devices are compliant. An example of device compliance can be something like ensuring that the operating system is up to date, or that the system has the correct software

version installed. To answer these questions, the IT Department uses the Configuration Manager to generate reports on endpoint compliance.

Threat Protection

The IT Department is tasked with ensuring that each device has some form of threat protection on each of the H2O district's endpoints. One of the first lines of defense in threat protection is Antivirus or Antimalware protection. Currently the IT Department ensures each endpoint is equipped with the latest version of Trend Micro Smart protection for the Endpoint suite. The IT Department can manage and view threats for their on-premises endpoints using a centralized hub which will give analysts insight on to what type of threats exist on the endpoints. Additionally, the IT Department will field calls from users who are explaining that their devices are exhibiting abnormal behavior. For the most part, the current threat protection solution relies on the threat signatures being updated automatically when devices are connected to the network.

Problems with Current IT Environment

While the IT Department can handle various workloads and maintain control for their on-premises endpoints, there are several problems with managing and securing endpoints in a telework environment. The problems the IT Department is facing include:

- An Influx of VPN connections from over 80% teleworkers leads to poor network bandwidth
- Support for laptops and iPhones are limited to in-person
- No support for MacOS or iOS devices
- Some employees can locally administer company-owned laptops
- Laptops must be physically connected back to the network through ethernet every 90 days or they will lose connectivity
- No remote support or troubleshooting for endpoints exist outside of the network
- Inability to deploy applications or software updates to remote endpoints
- Lack of operating system support, specifically redeploying Windows 10 for remote endpoints in the event of OS corruption
- Inability to ensure device compliance for remote endpoints
- Inability to view active threats from remote endpoints.
- Slow incident response times regarding threats on endpoints
- Lack of 3rd party integration for threat protection with services such as Configuration Manager or Azure AD

In moving forward with the project, it is important to note these key problems and design a solution that will resolve them. We will discuss this next.

CHAPTER THREE

MIGRATION STRATEGY AND IMPLEMENTATION

Chapter Overview

Chapter 3 covers the strategy for migrating and configuring H2O District's existing infrastructure, and offloading workloads to the cloud. Utilizing the cloud infrastructure and services will allow for the IT Department to manage and secure remote endpoints in a telework environment. This chapter highlights the key decisions that were made, why they were made, and the expected outcome after implementation. Ultimately the goal for this project is to find out what solutions currently exist, and how H2O's infrastructure can be improved or configured to manage and secure endpoints in a telework environment.

Cloud Solutions

Given that H2O has existing infrastructure both on-premises and in the cloud, the next goal would be to explore solutions that would allow them to fulfill the IT Departments responsibilities for managing and securing endpoints in a telework environment. After examining the requirements for the IT Department's current level of service and current infrastructure that exists, four of Microsoft cloud services were reviewed and three were found to offer viable solutions for managing and securing endpoints in a telework environment. The cloud services the IT Department chose to implement include Microsoft Intune, Microsoft Endpoint Manager, and Microsoft Defender for Endpoint. The cloud service that

was not chosen but is worth mentioning is the utilization of a Cloud Management Gateway.

Microsoft Azure AD

Microsoft Azure is Microsoft's cloud platform service that was developed under the codename "Red Dog" and introduced in the year 2008 (Foley, 2018). Since then, Microsoft's website shows that Azure has grown into over 160 data centers worldwide and is now it is a global leader in cloud computing platforms and services. Azure offers multiple services that provide numerous businesses from all sectors the ability to build, test, deploy, and manage applications anywhere worldwide.

Microsoft Azure Active Directory is a cloud-based identity access management service, which allows employees to sign in and access resources such as Office 365, the Azure Portal, and any other applications (*Insert Web source here*). When comparing Azure Active Directory to Active Directory Domain Services, it can be noted that Azure AD is used primarily for managing identity and resources in the cloud, whereas Active Directory DS is used for managing identity and resources on-premises.

It has been noted that about 88% of organizations have migrated in some or another to the cloud (Swoyer, Magoulas, 2020). *The H2O District* discovered the benefits of the cloud in the year 2016, and began to build and migrate the H2O infrastructure to the cloud, thus creating a hybrid-like platform, where some

applications, identities, and services exist in the cloud, and other management resources still exist internally on-premises. However, like many others, H2O was unprepared to manage an enormous number of remote endpoints in response to the COVID-19 pandemic. Figure 3.1 below summarizes how the Azure AD connect service was previously configured, and how it synchronized identities from the on-premises Active Directory Forest into the Azure AD cloud.

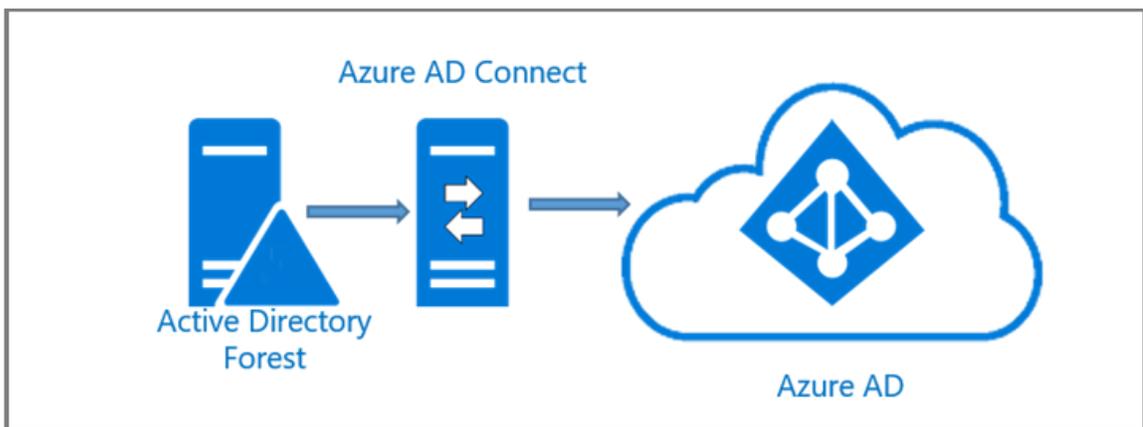


Figure 3.1 – Azure AD Connect

Microsoft Azure AD plays a pivotal role in allowing the configuration of additional cloud services that we will cover in this project. In fact, the infrastructure provided in Figure 3.2 would not have been possible without the existing infrastructure in Figure 3.1. Fortunately, the investment in hybrid infrastructure prior to the pandemic will help move the project forward and enable the IT Department to manage and secure remote endpoints. Ultimately, a

decision was made to migrate workloads to the cloud in effort to limit the number of VPN connections on-premises and allow for more management and security capabilities.

Microsoft Intune

Microsoft Intune was originally launched in 2011 and officially integrated into the Azure cloud in December 2016 (Mearian, 2019). Microsoft Intune was created to give organizations a Mobile Device Management (MDM) platform and allow for application management. As technology is rapidly evolving and applications and information is accessed from various endpoints, it is important that organizations manage and secure their data wherever it exists.

One great feature about Microsoft Intune is that since the platform was integrated with Microsoft Azure, organizations do not require any existing infrastructure to manage devices. Instead, organizations can simply configure Intune through their existing enterprise license. Because H2O District already had an existing Microsoft 365 E5 license, the IT Department was able to quickly switch on Intune and start configuring the policies they needed to manage and secure remote H2O endpoints.

Intune currently supports Windows 10, MacOS, iOS/iPad iOS, and Android operating systems. This means H2O District is able to support multiple operating systems and can enroll just about any device into Intune. Additionally, Intune allows for capabilities such as remote-wipe, device-lock, passcode reset,

configuration profiles and redeploying the OS. An Overview of Intune is provided in Figure 3.2 below.

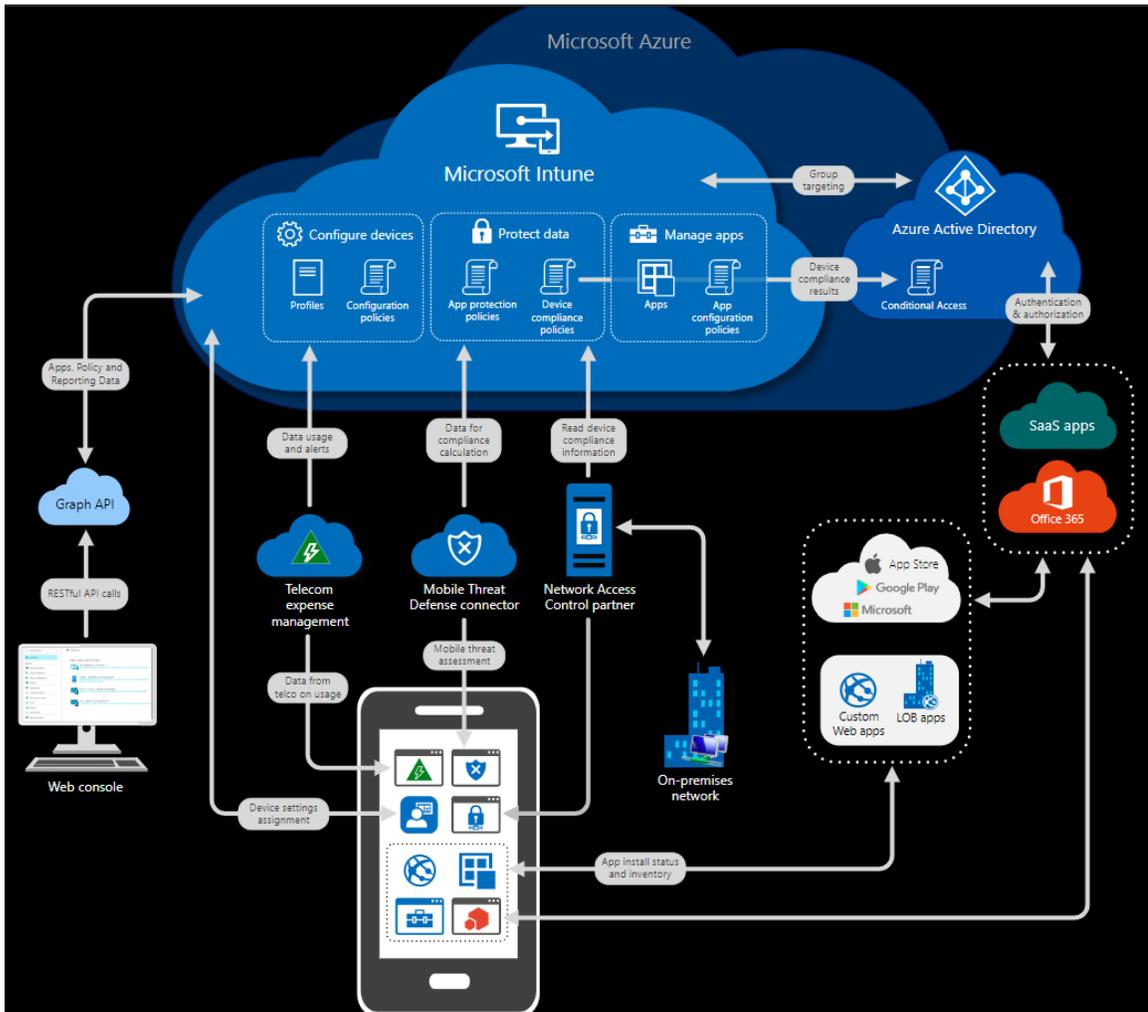


Figure 3.2 - Microsoft Intune Overview and Architecture (docs.microsoft.com, 2020)

Intune allows the IT Department to configure devices, protect data, and manage apps all within the cloud. Leveraging Intune would be a dramatic

improvement from having very little support for laptops and mobile devices. Once a device is enrolled into Intune the IT department will have further capabilities for properly managing or securing the device. Given that endpoints would be rapidly leaving H2O Districts corporate network, a decision was made to quickly onboard devices into Intune and configure profiles to meet the IT Departments overall defense in depth strategy.

Configuration Manager and Cloud Management Gateway

Microsoft Endpoint Configuration Manager is Microsoft's product that was released in October of 2019 (docs.microsoft.com, n.d). Although the product was initially created in 1994 as the Systems Management Server (SMS), it was then rebranded in 2007 as the System Center Configuration Manager, and more recently branded as the Endpoint Configuration Manager. The Endpoint Configuration Manager is now being used by many IT Departments for centrally deploying operating systems, software updates and applications, monitoring and reviewing systems for compliance, recording inventory, and allowing remote administration. The Endpoint Configuration Manager is primarily used to manage devices on-premises that are typically joined to a domain and managed using Active Directory Domain Services. However, after rebranding the Configuration Manager, Microsoft decided to integrate the Configuration Manager with cloud services such as Azure, Intune, and Defender for Endpoint.

One important distinction to note when referring to the Endpoint Configuration Manager is that devices must have a client installed on them that point to a centralized server, and are typically joined to a domain to be managed on-premises. Because Configuration Manager requires a centralized server as well as clients to be installed on each device, often systems that are taken off-premises can have trouble communicating back to the domain or are nearly unreachable. Configuration Manager can be configured to communicate with clients that are located outside of the domain or users connected remotely via VPN, however it requires that a server be placed in a separate area on the network and that firewall configurations are made to allow those connections on-premises. Often, security teams or network administrators are hesitant to open ports and allow unnecessary traffic inbound on-premises.

The answer to connecting to remote clients outside of the network would be the Cloud Management Gateway (CMG) as seen in Figure 3.3. The CMG allows for Configuration manager to communicate with clients using the internet – no VPN required. “By deploying the CMG cloud service in Microsoft Azure, you can manage traditional clients that roam on the internet without additional on-premises infrastructure. You also don’t need to expose your on-premises infrastructure to the internet.” (Microsoft, 2021) Another benefit of the CMG is that devices do not need to be joined to the domain, they can simply exist at an employee’s home, or practically anywhere that the device can receive an internet connection. This capability gives the IT Department the power to now manage

remote endpoints in a telework environment in a similar way as the on-premises environment. An overview of the CMG architecture can be understood in Figure 3.3.

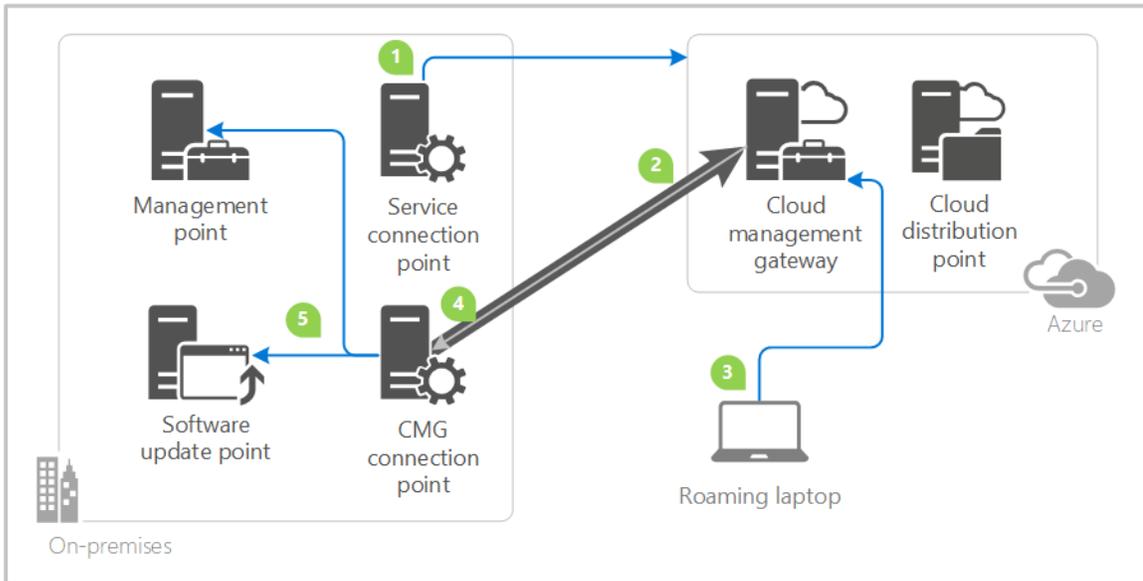


Figure 3.3 – Cloud Management Gateway Architecture

The benefit once again is that devices do not need to be connected via VPN, there is no additional infrastructure that needs to be setup on premises, or no unnecessary traffic inbound from internet connected devices. Ultimately the IT Department decided that it would continue to use the Configuration Manager to manage on-premises devices but did not want to extend those management capabilities outside of the organization. Therefore, devices that leave the internal network would be managed strictly using Intune. Although capable, Configuration

Manager and the CMG was not chosen to manage endpoint devices in a telework environment.

Microsoft Endpoint Manager

Another product launched in November 2019, and that is Endpoint Manager – not to be confused with Endpoint *Configuration* Manager. Endpoint Manager is Microsoft’s rebranding of Intune, Configuration Manager, and various other management products all integrated into what is known as Endpoint Manager. “Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot” (Microsoft, 2021). An overview and architecture of Endpoint Manager can be seen in Figure 3.4.

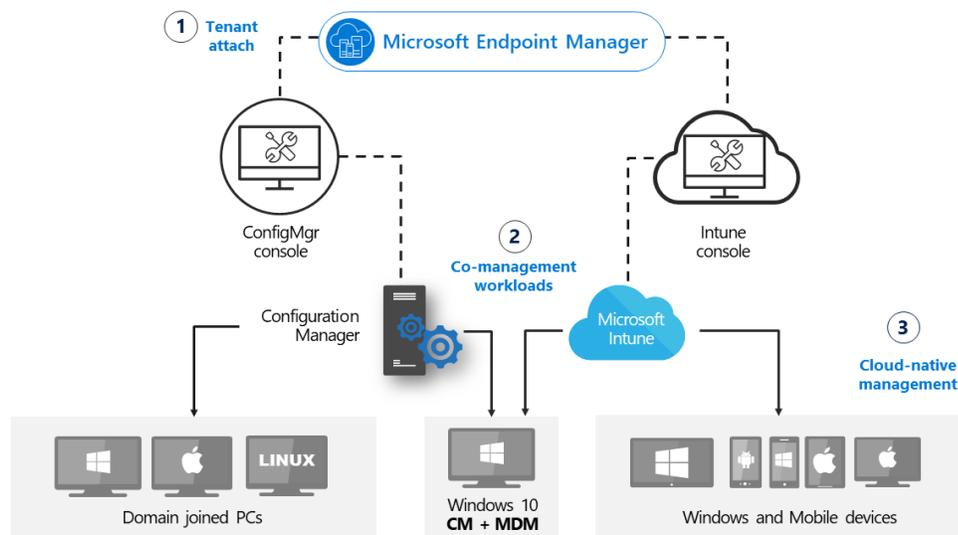


Figure 3.4 – Endpoint Manager Architecture

Much of Microsoft's licensing, branding, and naming convention is typically an attempt to simplify all their management products into a single console. We can think of Endpoint Manager as a sort of overarching interface that will allow the management of all endpoint devices throughout an organization (Microsoft, 2019). Whether endpoints are joined through Azure AD, Configuration Manager, or Intune, they can all be managed and secured wherever an internet connection can be found. Throughout the project it's important to understand that Intune, Configuration Manager, and Endpoint Manager all serve a purpose for managing endpoint devices.

In addition to being able to manage devices from Endpoint Manager, there is also the benefit of having visibility into the overall security compliance of endpoints. Endpoint Manager allows for the deployment and management of Defender for Endpoint which we will demonstrate later in the project. Endpoint Manager can also be connected to configuration manager to allow for an all-in-one console for reporting and insight into all endpoints – whether they are Windows, MacOS, iOS or Android devices. Endpoint Manager will certainly give the IT Department centralized visibility into both the management and security of their endpoint devices.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is Microsoft's next generation antivirus platform that provides a holistic cloud endpoint security solution (Microsoft, n.d). Some of the key capabilities of Defender for Endpoint is risk-based vulnerability management, attack surface reduction, endpoint detection and response, automated investigation and remediation, and a unified security management. With the increase in sophisticated attacks that coincides with the adoption of new technology, security is ultimately a concern. Additionally, as complex infrastructure grows with cloud services and data begins to leave the on-premises network, properly securing endpoints is a growing concern. Defender for Endpoint is one aspect of Microsoft's larger Defender platform which can be seen in Figure 3.5. Defender for Endpoint also allows for organizations to leverage the power of Artificial Intelligence built by Microsoft to prevent, detect, respond, and even mitigate malware or viruses from causing further damage to an organization.



Figure 3.5 – Microsoft 365 Defender Platform (docs.microsoft.com, 2020)

Microsoft Defender for Endpoint exists in the cloud and is accessible through Endpoint Manager or the MS365 Security Center. Defender can be enabled for each remote endpoint whether regardless of which network they are located on. As of April 2021, the current operating systems that Defender supports are the following:

Supported Windows versions

- Windows 7 SP1 Enterprise (Requires ESU for support.)
- Windows 7 SP1 Pro (Requires ESU for support.)
- Windows 8.1 Enterprise
- Windows 8.1 Pro

- Windows 10 Enterprise
- Windows 10 Enterprise LTSC
- Windows 10 Education
- Windows 10 Pro
- Windows 10 Pro Education
- Windows server
 - Windows Server 2008 R2 SP1
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server, version 1803 or later
 - Windows Server 2019
- Windows Virtual Desktop

Other supported operating systems

- Android
- iOS
- Linux
- MacOS

Upon reviewing current capabilities for Microsoft Defender for Endpoint, a decision was made to migrate H2O districts current assets from Trend Micro Smart Protection, and onboard them into Defender for Endpoint. Given that Windows Defender can also integrate into Endpoint Manager and Configuration

Manager, it was decided that Defender was a far superior route to take with securing both on-premises and remote devices. Additionally, no license upgrades or infrastructure is needed since H2O district already had a license as well as infrastructure that allowed for the implementation of Defender into their environment.

Azure AD Join Concepts

When joining devices to Azure AD, it is important to note the different methods that Azure classifies each registered device. This section will cover the various methods to synchronize endpoints with Azure, as well as the significance of each method.

Azure AD Registered Devices

Figure 3.6 shows how Azure AD registered devices allow users to use their own personal devices to sync up with Microsoft Azure. Personal devices are commonly referred to as Bring Your Own Device (BYOD) criteria. A BYOD example is supposing a user wants to use their mobile phone to download and sync with Outlook or OneDrive. Another scenario is when an employee wants to access resources using their own personal computer or laptop, and sign into their Office 365 applications such as Word or Excel using their Azure AD credentials. When viewing these types of devices on any of Microsoft's platform's you will see them listed as *Azure AD registered*.

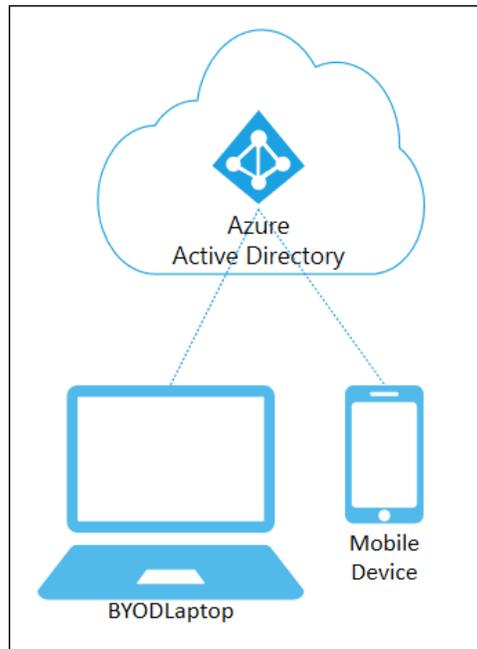


Figure 3.6 – Azure AD Registered Device (docs.microsoft.com, 2019)

It is important to understand that an Azure Registered device does not give the IT Department the right to manage or secure the device itself. Instead, only the specific information that can be on these devices is controlled. For example, the device could be set to have a required compliance policy before data is accessed, meaning that the device should be updated to the latest operating systems, or cannot be jailbroken. However, the ability to force the device to upgrade to the latest operating system is not possible with simply a registered device. Instead, only policies such as which data and apps can be configured on these devices can be set.

Azure AD Joined Devices

Figure 3.7 shows how an Azure AD Joined device is connected through Microsoft Azure. Azure AD joined devices allows for organizations to register devices and only have them connect only to Azure AD. A scenario featuring Azure joined devices is if the organization owns the endpoint device and would like to manage them using only Azure resources such as the Intune, and Endpoint Manager. Azure AD joined devices are meant to be managed using cloud resources and not so much on-premises resources. When viewing these types of devices on any of Microsoft's platform's you will see them listed as *Azure AD joined*.

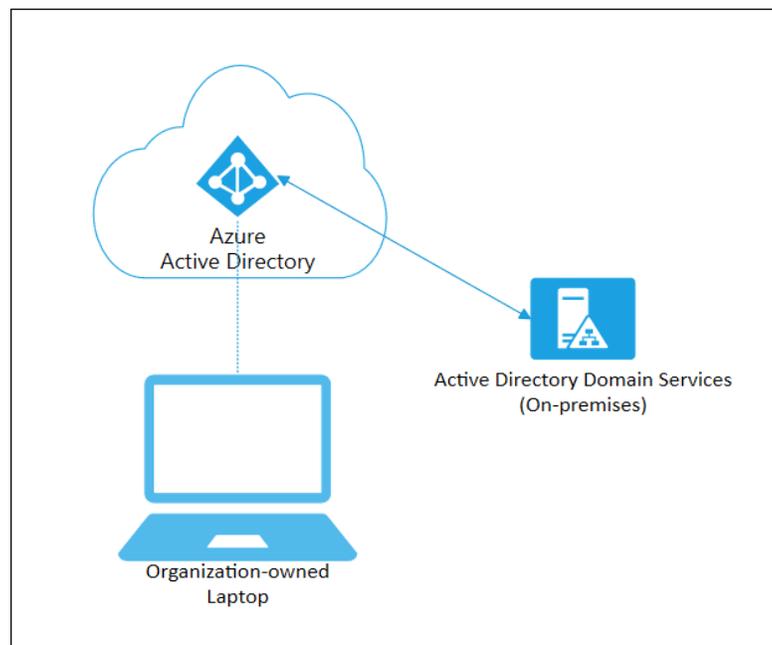


Figure 3.7 - Azure AD Joined Device (docs.microsoft.com, 2019)

An Azure Joined Device gives System Admins the rights to manage or secure the device itself. For example, the device can be configured to have specific settings disabled, to only allow specific apps installed, forced to update, as well as locked or remote wiped. All changes can be forced from within Intune and pushed out to the endpoint devices. An Azure AD Joined device gives the IT Department full control of the information as well as configuration of the endpoint device.

Hybrid Azure AD Joined Devices

Figure 3.8 shows how a Hybrid Azure AD joined device is synchronized to Microsoft Azure and Active Directory. Hybrid Azure AD joined devices allow for organizations to continue to utilize their on-premises Active Directory DS infrastructure, while simultaneously being able to leverage the power of Azure AD. An example of a Hybrid Azure AD joined devices would be where a device is currently joined to the on-premises AD-DS domain and co-managed using Configuration Manager and Intune. When viewing these types of devices on any of Microsoft's platform's you will see them listed as *Hybrid Azure AD*.

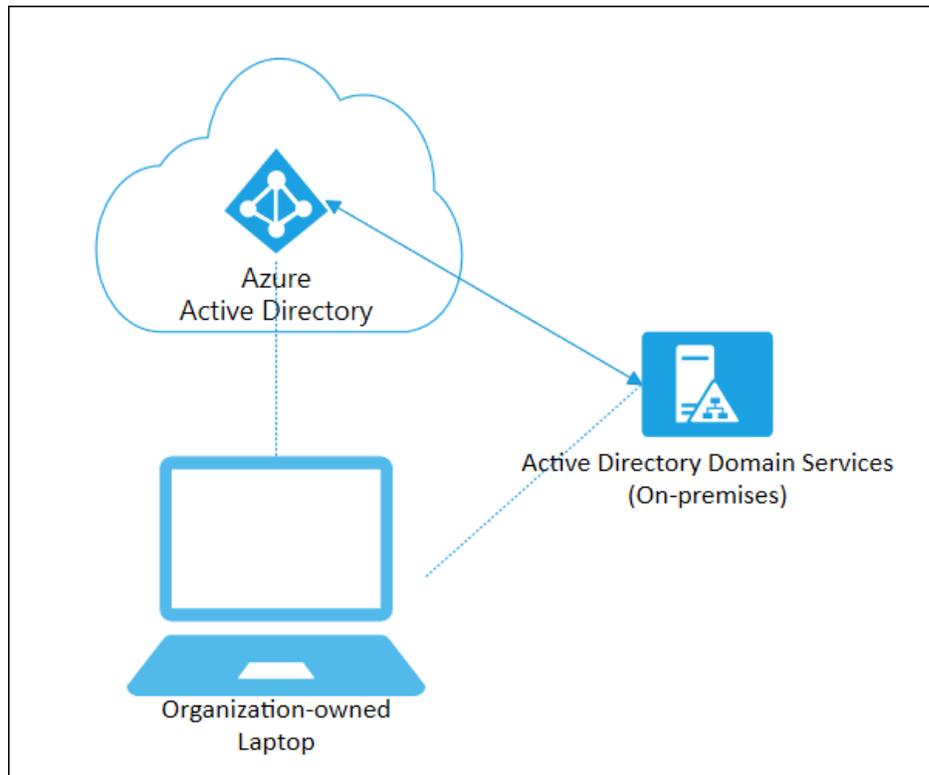


Figure 3.8 – Hybrid Azure AD Joined Device (docs.microsoft.com, 2019)

A Hybrid Azure AD device gives System Admins the rights to manage or secure the device itself from either cloud services such as Intune and Endpoint Manager, or on-premises infrastructure using Configuration Manager. For example, let us assume that the IT Department would like to push changes to endpoint devices using Group Policy, install software using Configuration Manager and the Cloud Management Gateway, but also like to remote wipe, restart, or lock the endpoint using Intune. A Hybrid Azure AD device allows for multiple management points as well as the IT Department to determine which workloads they want to manage through on-premises vs the cloud. Only devices

running Windows 10 can be configured as a Hybrid Azure AD device, and mobile phones are strictly managed using Intune. A Hybrid Azure AD joined device gives the IT Department full control of the information, configuration, as well as a choice in which platform to use when managing and securing their endpoint devices. For the purposes of this project the IT Department decided not to use a Hybrid join approach, and instead join devices using strictly Azure joined.

Co-Management

It is also important to mention Co-Management in this scenario. A device that is configured to work with Configuration Manager and Intune is referred to as a co-managed device. Originally many System Admins believed that co-management was a pathway towards taking all devices and migrating them to be managed with Intune. However, Bran Anderson (corporate Vice President of Microsoft's Commercial Management Experiences) is quoted saying that "Co-management isn't a bridge, it's a destination" (Anderson, 2019). This means that organizations can be perfectly fine with managing workloads through Configuration and Intune and stay there for as long as they wish, without worrying that Configuration Manager and their entire infrastructure is going away. An overview of the architecture in a co-managed environment can be seen in Figure 3.9.

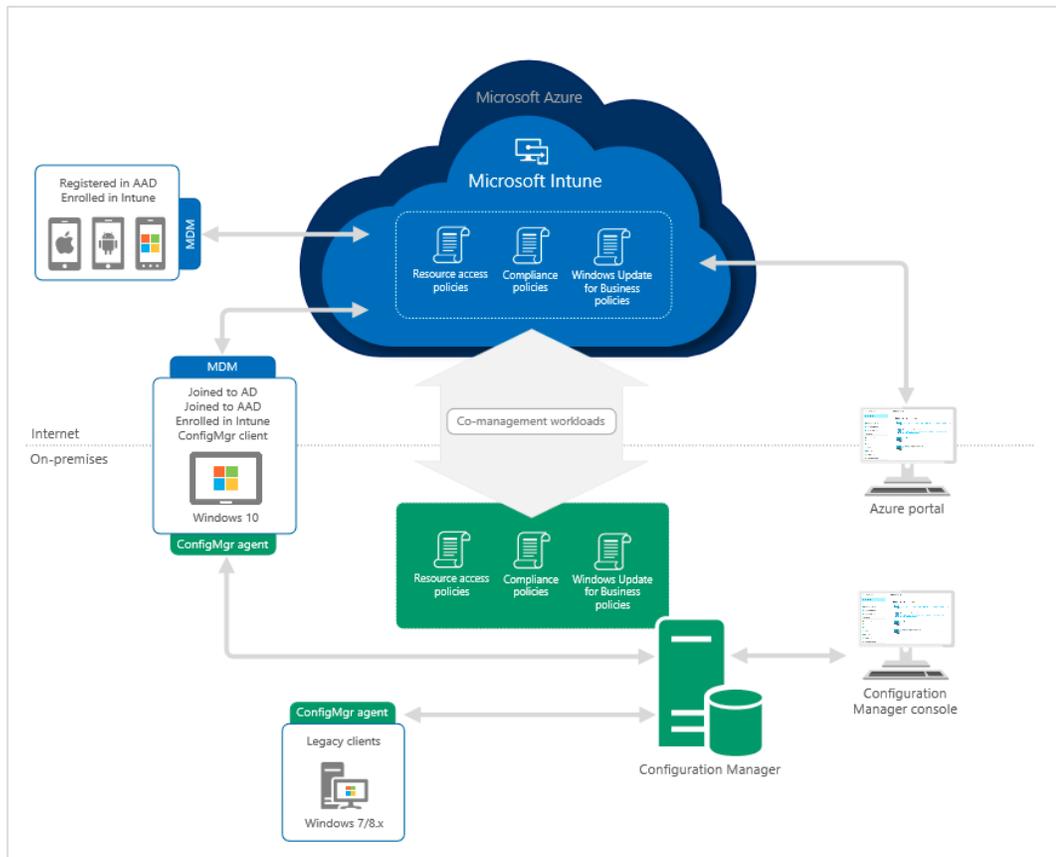


Figure 3.9 – Configuration Manager and Intune Co-Managed Architecture
(docs.microsoft.com, 2021)

In the previous Figure 3.9, endpoints can exist in a co-managed state where app and policy workloads can be handled by both Configuration Manager and Intune. We can also see that Mobile phones are handled solely by Intune, Legacy Windows 7 clients are handled solely by Configuration Manager, and an Azure AD Joined Windows 10 system is operating in a co-managed state receiving workloads from Intune and Configuration Manager. Essentially a co-managed state means that an endpoint may have some policies handled by

Intune from the cloud, whereas other policies will be handled by Configuration Manager. Ultimately both products can carry out the goals of managing devices and can serve as a solution for devices that still need to utilize on-premises resources from Configuration Manager.

Upon examination of the co-management requirements, the IT Department made the decision not to hybrid join systems and instead have complete separation of workloads between Intune and Configuration Manager. Because the IT Department was already having success managing on-premises endpoints with Configuration Manager, the workloads with Intune were strictly meant to be managing devices in a telework environment. If the IT Department were to utilize this scenario, they would have to implement the Cloud Management Gateway which was already previously decided against.

Configuring Cloud Services

The IT Department was also tasked with configuring additional services using their current infrastructure. This section will cover a brief overview of the steps needed to configure each cloud service. The three services that needed to be configured were Microsoft Intune, synchronizing Apple Business Manager with Intune, and Defender for Endpoint.

Microsoft Intune Configuration

The first service that the IT Department needed to configure was Microsoft Intune. Enabling Microsoft Intune is the first step towards successfully managing and securing endpoints in a telework environment. Once the tenant has been configured to allow for Intune, devices that leave the company network can then point towards the cloud for all the management capabilities. In short, the steps to configure Intune are as follows (docs.microsoft.com, 2020):

1. Sign in and create an Intune trial configuration – the licensing was already included in the Microsoft 365 E5 license
2. Configure a domain name – ex: H2Odistrict.com
3. Add users and groups to Intune to synchronize with Intune
4. Assign licenses to users or devices
5. Set up the MDM Authority
6. Add Apps to be installed automatically (optional).
7. Configure device profiles – such as email settings, VPN connection, WiFi, or App deployments (optional)
8. Customize the Company portal
9. Enable device enrollment by setting up the MDM authority and enabling specified OS platforms to be managed.
10. Configure App policies (optional)

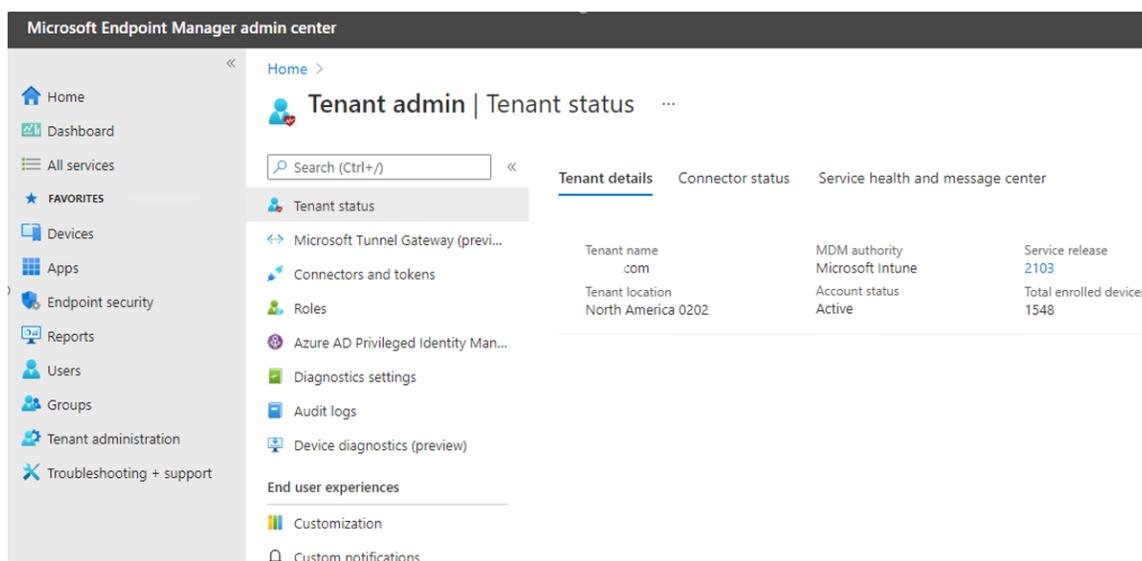


Figure 3.10 – Successful Intune Tenant Enabled

Once Intune has been set as the MDM authority and the device profiles have been created, devices can now be Azure AD Joined and will show up in Intune. Devices in Intune do not need to be connected to the same corporate network and can now exist in an employee's home, at a coffee shop, or even in another state. In other words, physical network location does not matter anymore because the management exists in the cloud and not behind corporate firewalls.

Synchronize Intune with Apple Business Manager

The next step for the IT Department would be to connect their iOS devices with Intune so that Intune can be the new MDM server and they can setup the current 150 iPhones with the new MDM server. Future projects will include

migrating devices away from MaaS360. The steps to synchronize Intune with Apple Business Manager are the following:

1. In Endpoint Manager Navigate to Devices > MacOS Enrollment > Apple MDM Push certificate
2. Grant Microsoft permission to send user and device info to Apple
3. Download the Intune certificate signing request to create an Apple MDM push certificate
4. Login to Apple Business Manager, go to Settings, Device Management Settings, and click on Add MDM Server
5. Upload the Intune Certificate
6. Create an Apple MDM push certificate by clicking Download Token
7. Enter the Apple ID used to create the push certificate
8. Upload the Apple MDM push certificate to upload

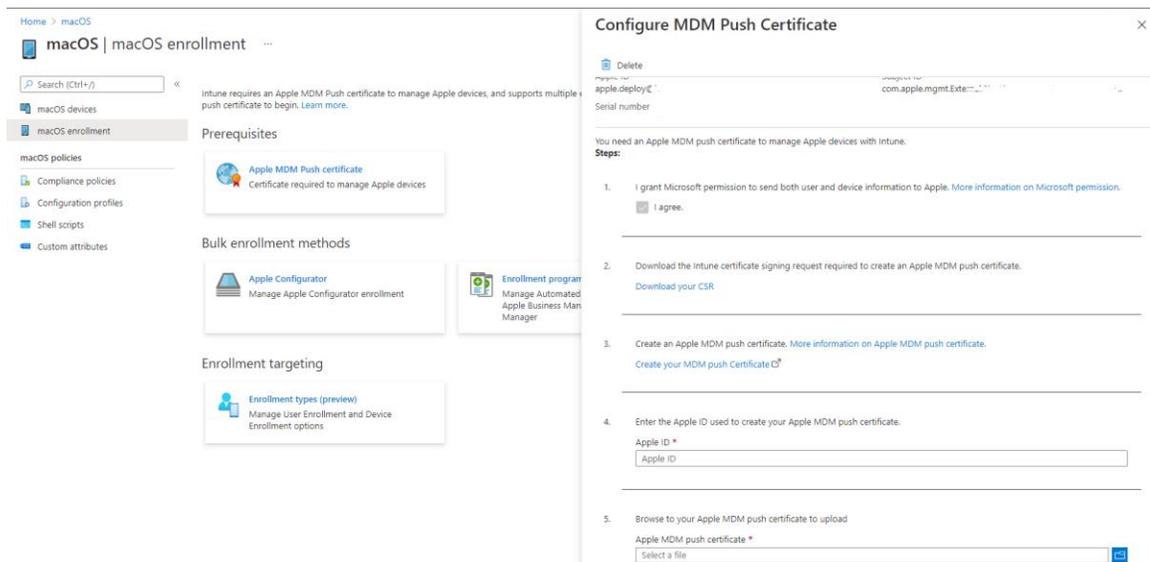


Figure 3.11 – Creating an Apple MDM Push Certificate from within Intune

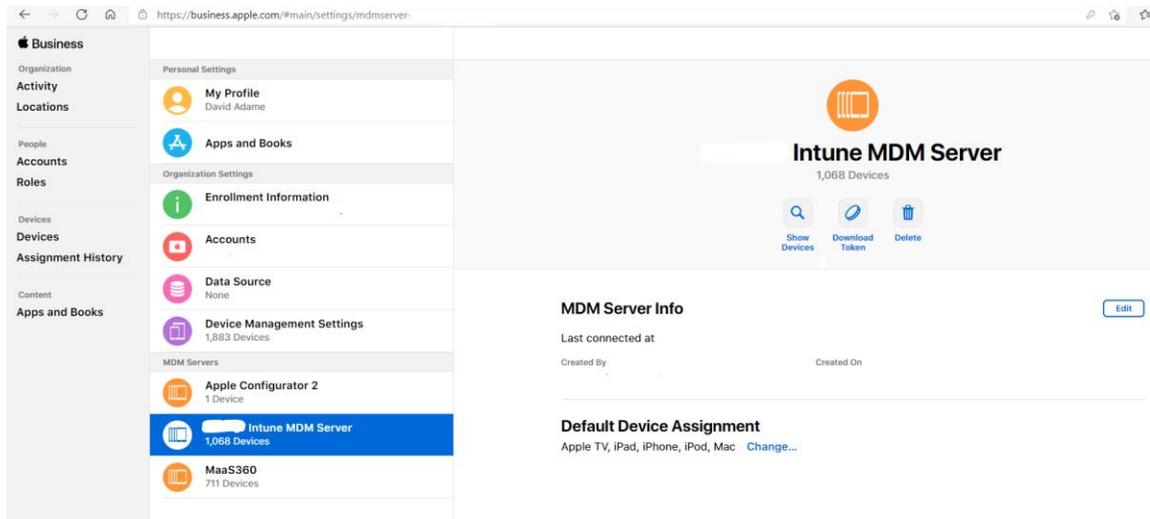


Figure 3.12 – Apple Business Manager Successfully Synced with Intune

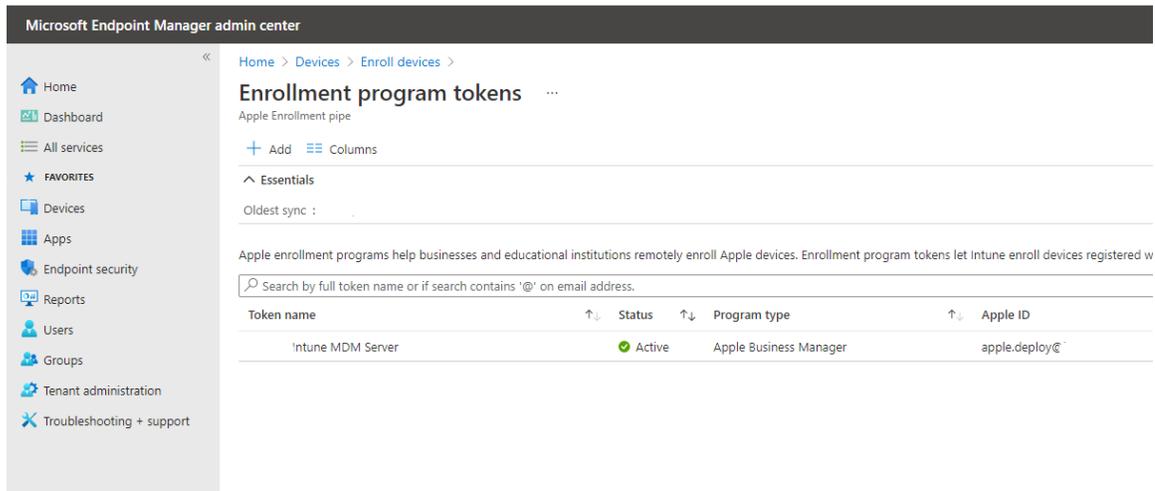


Figure 3.13 – Apple Enrollment Program Token Synced with Intune

Once Apple Business Manager and Intune have been synchronized then the next step would be to create an enrollment profile for each device. The enrollment profile will determine what the user see’s when they first enroll the device into Intune. The IT Department created an enrollment profile that allows the user to sign Company Portal and enroll the device into Intune. Once an iOS device has been successfully enrolled, all the compliance policies will download for the device and the IT Department will have the ability to manage and secure the device properly from within Endpoint Manager.

Microsoft Defender for Endpoint

After Intune and Apple Business Manager are synchronized, the next cloud service to configure would be to deploy Microsoft Defender for Endpoint. Deploying Defender for Endpoint will give the IT Department visibility into the

organization's security posture and ensure that each endpoint is feeding information back into Endpoint Manager. The steps to deploy Microsoft Defender for Endpoint are the following:

1. From Endpoint Manager, navigate to Endpoint Security > Microsoft Defender for Endpoint
2. Connect the Microsoft Defender for Endpoint to Microsoft Intune in the Microsoft 365 Security Center
3. Configure the Connector settings, which include the MDM Compliance Policy Settings, App Protection Settings, and Common Shared Settings
4. Create a Device Configuration profile for each OS platform – in this case Windows 10, and iOS
5. Assign the profile to the devices – in this instance it will be all users and groups that are enrolled in MDM through Intune.

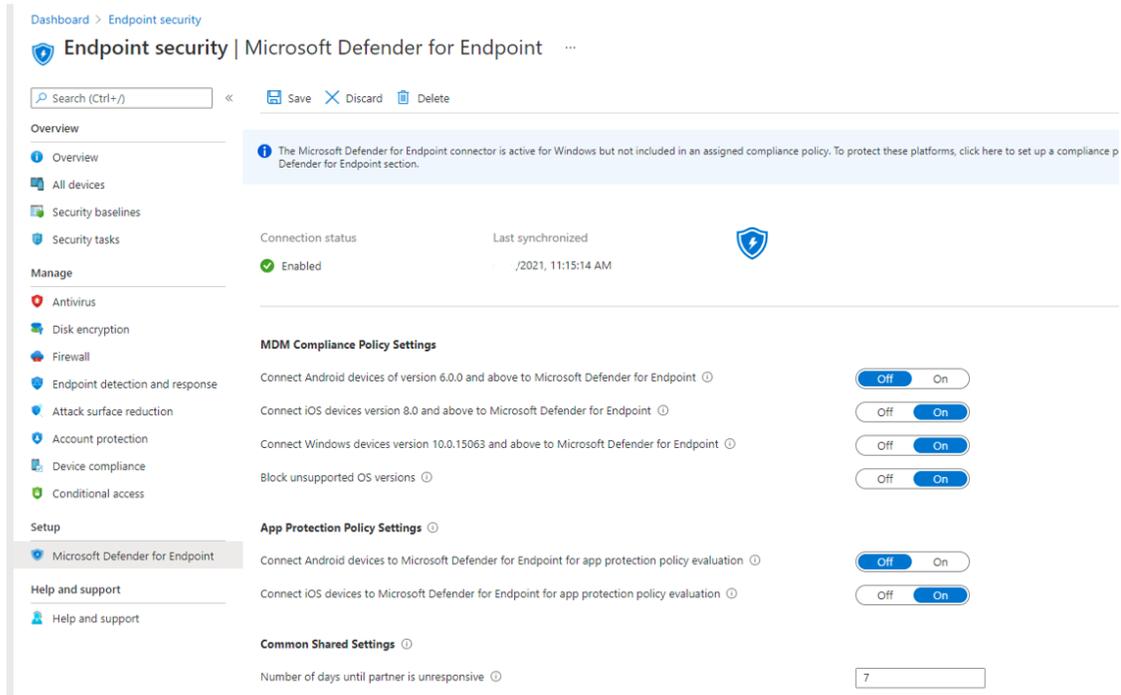


Figure 3.14 – Microsoft Defender for Endpoint Connected Successfully

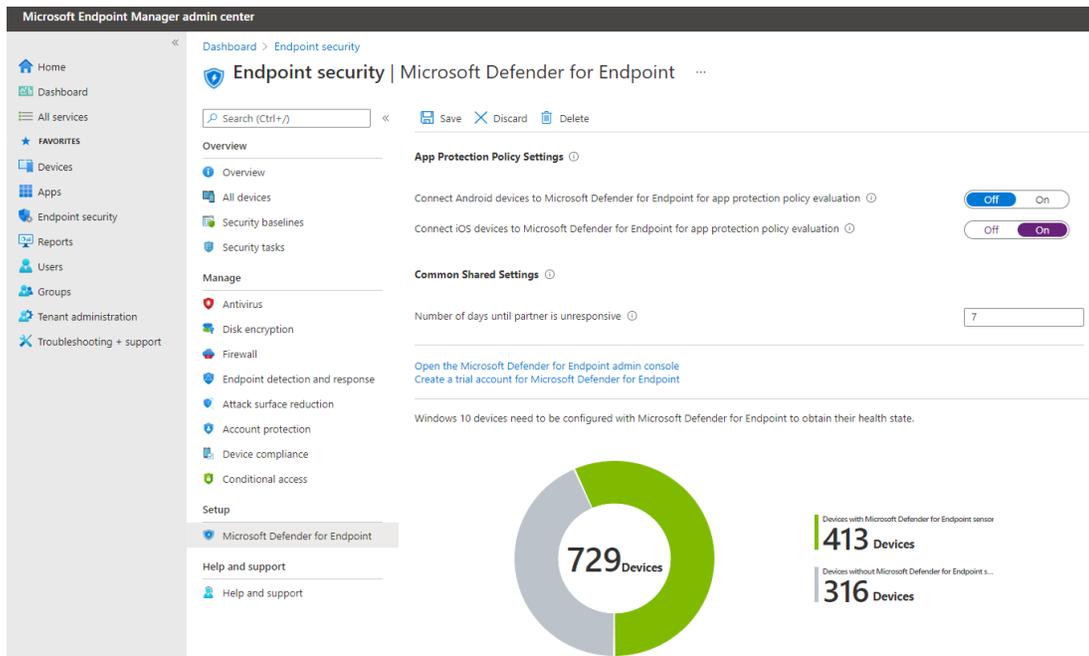


Figure 3.15 – Microsoft Defender for Endpoint Devices Onboarded

Getting Devices Into Intune

The IT Department's first task was to determine what needed to be configured to support the rapid increase of remote endpoints. The remote endpoints that were discovered included employee personal devices, company owned desktop PC's and laptops that employees will be using at home, as well as their current stock of over 150 iOS mobile phones that were going to replace existing iOS devices as part of an annual refresh. The next task was to configure the cloud services needed to support the remote endpoints. In this chapter we will discover the methods that the IT Department used to enroll the devices into Intune. Although there are numerous methods of enrolling devices into Intune, for the purposes of this project we will demonstrate some of the methods that the H2O district decided to implement.

BYOD Devices

H2O district had a policy in place that restricted an employee's access to apps such as Office 365 and email from personal devices – also known as BYOD. Access to data and applications from BYOD devices was restricted because the IT Department was unable to properly manage or secure the device. Instead, certain personnel that needed access to resources were only able to remote into their computer from home to access applications or use their corporate phone which was allowed access. However, given that H2O district is

now choosing to manage their devices in Intune, support for future enrollment into Intune is possible given that devices can be locked at an application layer, rather than the entire device. This capability also allows for the company's data and applications to be stored on a separate encrypted volume and be securely wiped in the event an employee leaves the organization or their phone is compromised.

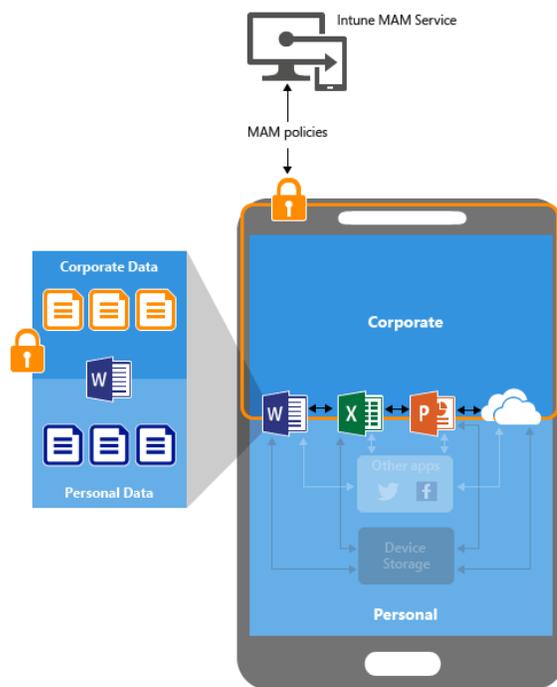


Figure 3.16 – Application Protection Policy for BYOD Devices
(docs.microsoft.com, 2021)

To implement support for BYOD, The IT Department needed to setup an App Protection Policy (APP) within Intune that allows for users to download

Microsoft's Company Portal app and register their personal device. The employee will login with their H2O district username which allows them to access to applications like Excel, Outlook, PowerPoint, Word, OneNote, OneDrive, and Teams. This immediately gave people access to their emails with their personal devices as well as Teams to communicate with their colleagues. In creating this policy, the IT Department can manage and protect their information at the application layer. There are still more policies that can be created such as ensuring that a device meets a specific iOS version, or that a device is active within a certain period, or even if a device has a PIN. However, in the beginning of the pandemic it was crucial to ensure that people were able to get access to information regardless of whether they were on a computer or mobile device.

Corporate Owned Desktops and Laptops

Due to the increase of employees that are working from home, the IT Department had to decide the best Azure Join method for company owned laptops and desktops. The original concern was that the IT Department was unable to manage or communicate with their endpoints in a telework environment. Previously, the IT Department was unable to support remote endpoints since they were not on the corporate network. However, now that the IT Department is using more cloud infrastructure, there are more remote support options available.

For company owned desktops and laptops that employees would use from home, it was decided to go with an Azure AD Joined approach. These devices would be strictly Azure AD Joined and receive their policies and application deployments from Intune. The desktops and laptops were setup with the IT Department's standard Windows 10 Image but not joined to the domain because the devices would not exist on the same corporate network.

Although there are many ways to add a device to Azure AD, the IT Department was forced to develop a quick solution in response to the increase of teleworkers. The IT Department created a group called 'Intune Auto-Enrolled Desktop' and 'Intune Auto-Enrolled Laptop' in Azure AD and configured a policy. This policy states that any Azure AD device that exists in the group will be automatically enrolled into Intune. After the IT Department deployed Windows 10 to a device, it be joined to Azure AD and are automatically enrolled in Intune by performing the following:

1. Logging into Windows as an administrator
2. Clicking Start > Settings > Accounts > and click Access work or school.
3. Entering an administrator's Azure AD credentials (which is typically their company email address)
4. Verifying the settings and clicking join, waiting for the All Set message and clicking Done.

5. After the device is joined, the system is restarted and then the IT personnel will add the device to the proper group in Azure AD.

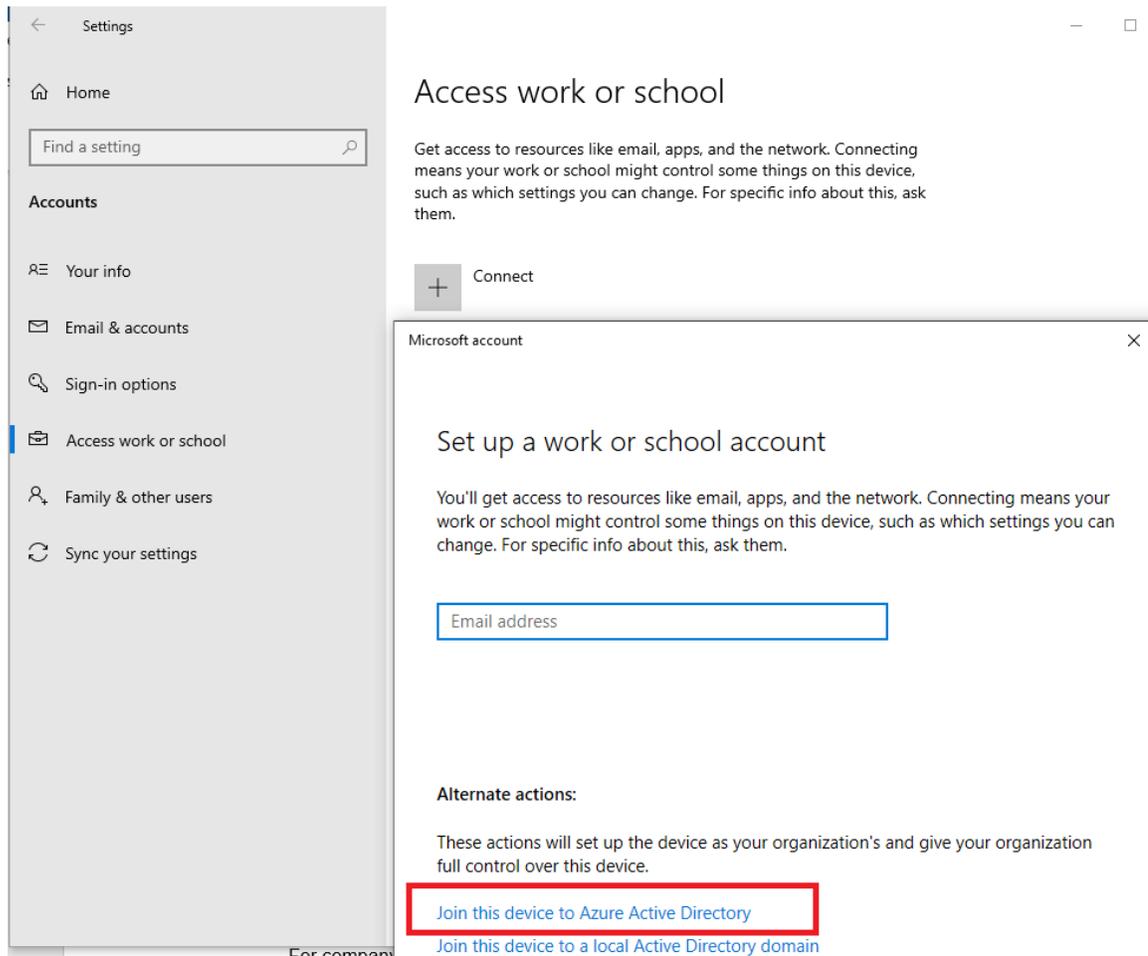


Figure 3.17 – Azure Active Directory Join from Settings Menu

The IT Department will also have to make a future decision to determine exactly how much of their on-premises infrastructure they would like to enroll and manage within Intune. Although there are many capabilities that exist for

managing devices Azure AD joined devices, the project did not call for the on-premises systems to be migrated into Intune.

Corporate Owned Mobile Phones

Prior to the pandemic, the IT Department was in the middle of a phone refresh and ordered 150 phones to be deployed to users. The IT Department previously setup an account with Apple Business Manager and was using it with IBM MaaS360 as the MDM solution. In the last section, the IT Department also configured the Intune MDM server to integrate Intune with Apple Business Manager in which the overview and working components are seen in Figure 3.18. The new solution allows for the IT Department to purchase devices, automatically report to Apple Business Manager, and automatically enroll into the Intune MDM server which can be seen in Figure 3.19. Additionally, a device enrollment profile was created in Figure 3.20 so that when the device arrives from the hardware vendor, it is ready to be delivered to the employee for Device Enrollment. When the employee walks through the setup process, the device automatically enrolls into Intune by simply logging in using their H2O district email and password. The IT Department configured each of the 150 new phones to be setup to use Intune as the MDM server, and that a future project will involve migrating the rest of the IBM MaaS360 devices into Intune.

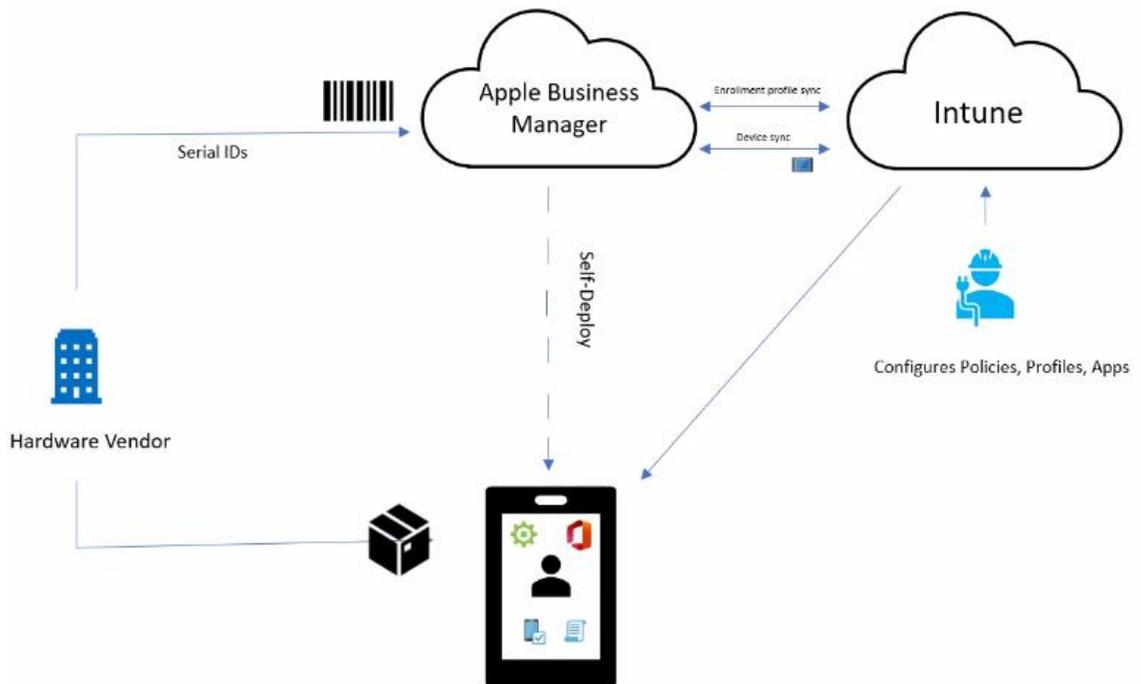


Figure 3.18 – Apple Business Manager and Intune Integration

Change Device Management

You are about to change device management for **iPhone XR**.

Assign to server:

Unassign

Cancel

Continue

Figure 3.19 – Assign Device to Intune in Apple Business Manager

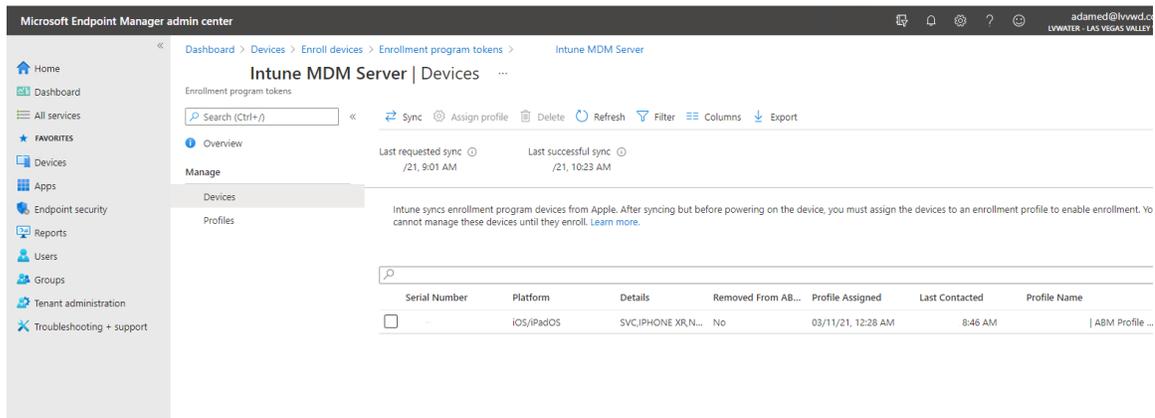


Figure 3.20 – iOS Device Enrolled in Intune with Enrollment Profile Assigned

Viewing Devices in Endpoint Manager Admin Center

As previously mentioned, Microsoft is now making a shift towards rebranding their products into a single console known as Endpoint Manager. Endpoint Manager consists of all the services and tools to manage and monitor all the endpoints throughout the enterprise including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot (Microsoft.com, 2021). As shown in Figure 3.21, System Admins can simply launch a web browser, navigate to endpoint.microsoft.com, and immediately gain visibility into their endpoints and begin to manage them. The IT Department has gained a significant ability to centralize their endpoints and effectively manage them through device profiles and compliance policies.

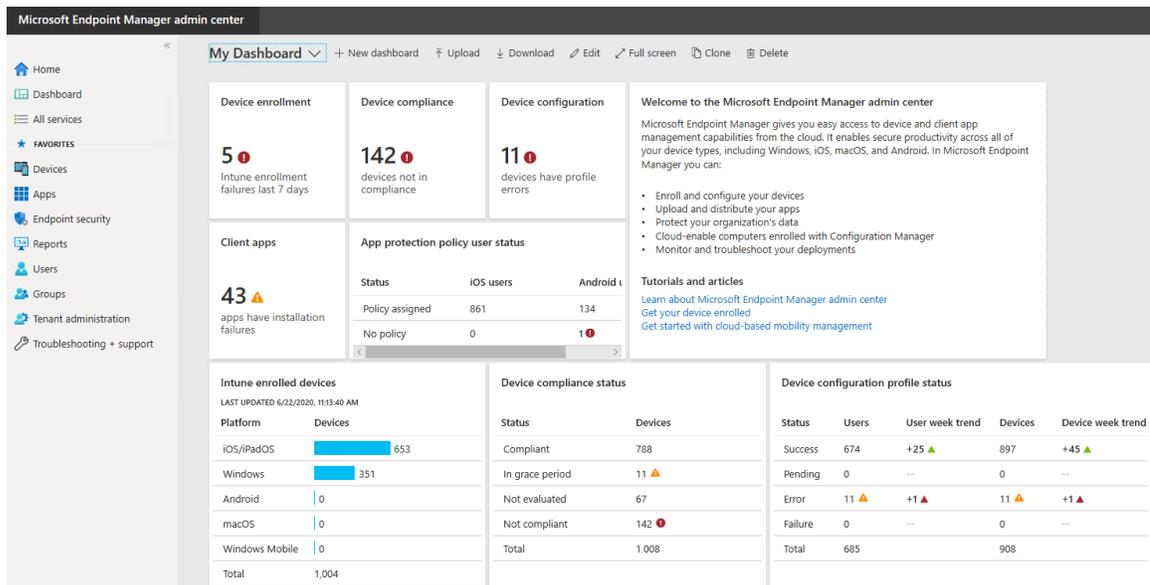


Figure 3.21 – Microsoft Endpoint Manager Admin Center

Viewing Devices in Microsoft 365 Security Center

As shown in Figure 3.22, a new tool that the IT Department gained was the ability to gain insight into the threats that not only exist at the endpoints, but across all their Microsoft products such as Defender for Office 365, and 365 Defender. System Admins can navigate to security.microsoft.com and instantly gain access to the Microsoft 365 Security Center to determine the types of threats that exist in their organization. All the data that is submitted from the Defender for Endpoint client is submitted back to the Microsoft 365 Security Center where more advanced analysis can be performed.

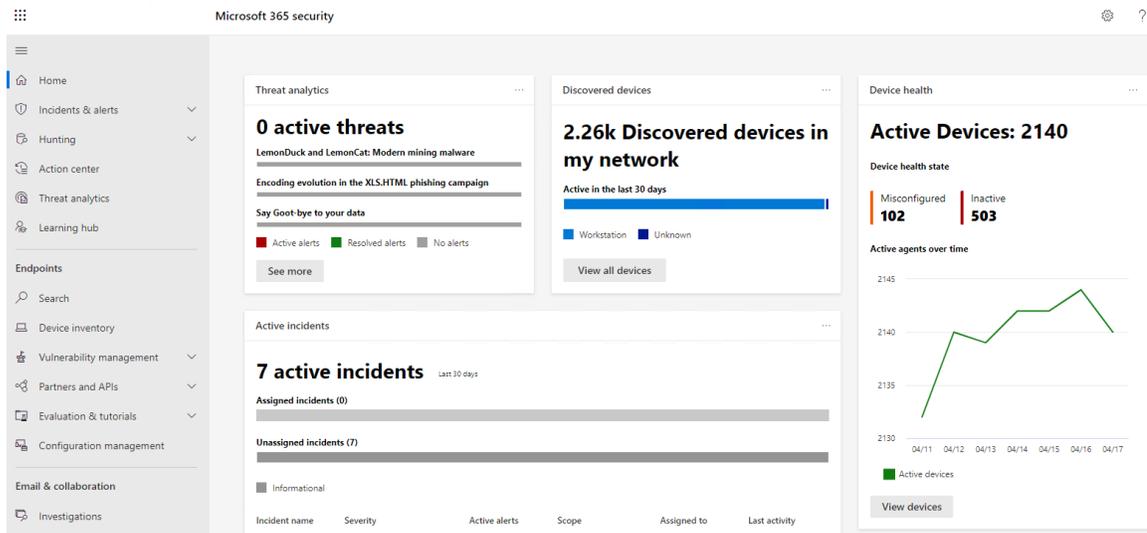


Figure 3.22 – Microsoft 365 Security Center

Summary

The solutions that were configured in this chapter enabled the IT Department to significantly increase the serviceable areas for their endpoints. As previously mentioned in Chapter 2, the IT Department was only able to service endpoints that were behind the corporate firewalls. Now with the services that were implemented in this chapter, the IT Department has gained the ability to manage endpoints regardless of they are physically located. Furthermore, the decision to utilize more cloud services will allow the IT Department to gain much more capabilities to provide better levels of service which will be highlighted in the next chapter.

CHAPTER FOUR

POST IMPLEMENTATION

Chapter Overview

In chapter two we outlined the current level of service that the IT Department can carry out on-premises, and how that same level of service needed to be considered in the strategy and implementation. Given that a significant effort was made in migrating much of H2O IT infrastructure into the cloud, the IT Department has gained some significant improvements in their ability to manage and secure endpoints. This chapter will cover how the IT Department is able to operate in the new environment, and some of the benefits they have gained.

New Endpoint Management Capabilities

As previously mentioned, the IT Department has the responsibility to provide endpoint management in the areas of Software Deployment and Updates, Operating System Support, and Remote Support. This section will cover how the IT Department is able to carry out each of those responsibilities in the new environment.

Software Deployment and Updates

The IT Department gained a significant improvement in their ability to deploy and update software to endpoints that leave the network. Previously the

only method the IT Department was able to deploy applications was through Configuration Manager, or through a manual installation process. Now the IT Department has the benefit of deploying applications through Microsoft Intune to remote endpoint devices as seen in Figure 4.1. Intune also gives the IT Department the ability to deploy apps to both iOS devices and MacOS devices should the Department choose to utilize this method. Another benefit in the new environment is that the endpoint does not have to exist on the same network to receive the deployments. Instead, endpoints can exist anywhere and now be completely serviceable by the Intune MDM service.

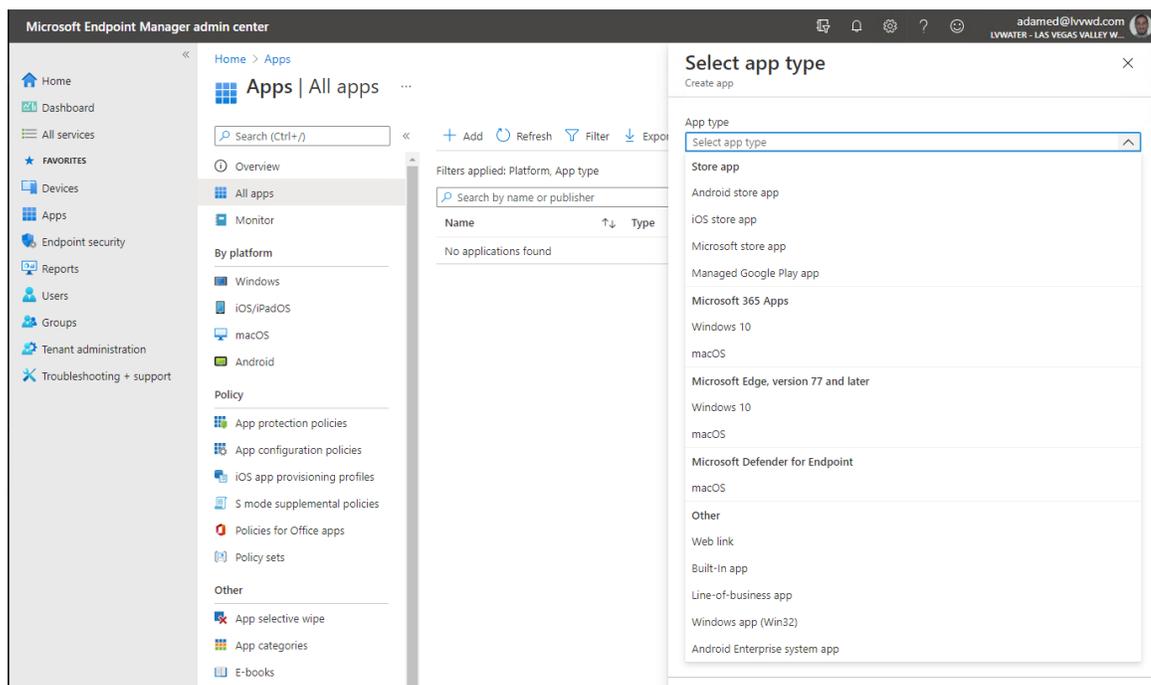


Figure 4.1 – Application Deployment Types in Endpoint Manager

Operating System Support

Operating System Support is where the IT Department has noticed dramatic improvement. In the past the IT Department has always focused on maintaining a Windows 10 image, which can often be a time-consuming task having to ensure that each image works for the device model. Maintaining an OS image typically allowed for more control of the configuration of Windows 10 operating system, however it requires timely hours from the IT Department just to maintain. In the past the IT Department has found that they were spending countless hours just maintaining the image every 6-months. With each iteration of Windows 10 the IT Department has encountered problems with previous iterations of the image that were incompatible, which often led to more frustration and troubleshooting. There was also an issue with remote endpoints being unable to utilize the Configuration Manager task sequence Image deployment method because they did not exist on the same corporate network. Prior to the migration, if a user's operating system becomes corrupted on their laptop, it would require them to bring in their laptop on premise and a technician manually reimage the device, often resulting in days of downtime.

With endpoint devices enrolled into Microsoft Intune, the IT Department can leverage the power of Windows Autopilot for operating system support as seen in Figure 4.2. Windows Autopilot takes the grueling task of having to maintain an operating system image. Instead, Autopilot allows for IT to configure

devices before they arrive onsite – like how iOS devices can be preconfigured before arrival. In short, a deployment profile is created in Intune prior to the device's arrival. Instead of deploying Windows to the device when it arrives, the IT Department can configure all the applications and services on the back end and have the user log into the device right away. In essence, the IT Department now has the possibility of no longer having to maintain an image, but instead leveraging the power of Windows AutoPilot to reset devices directly from the Endpoint Manager console, regardless of where they physically exist.

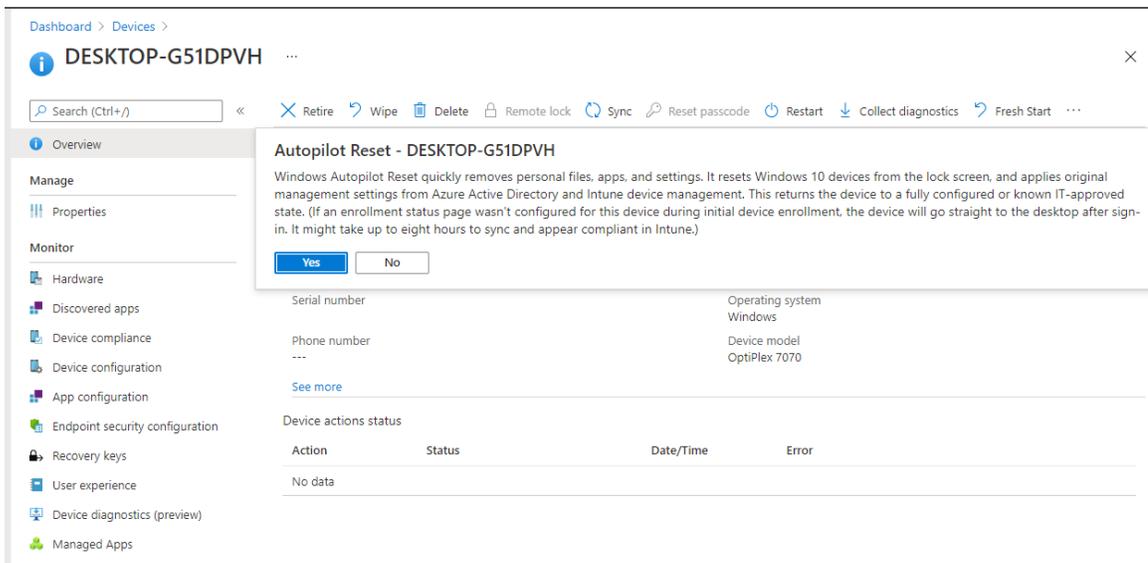


Figure 4.2 – Autopilot Reset within Endpoint Manager

Additionally, the IT Department gained a significant advantage in their ability to deploy Operating System updates to their Windows 10 Devices.

Previously, the IT Department was directing customers to plug in their laptops to

the network so that they can be serviced properly. However, end users would often leave their devices powered off or would fail to plug in, often leading to non-compliant devices. Using Intune, the IT Department was able to define an update ring – as seen in Figure 4.3 - and target their remote Windows 10 devices. This feature allowed for devices to look directly to Microsoft for their Windows Update rather than on premise, hence leading to greater compliance for OS updates.

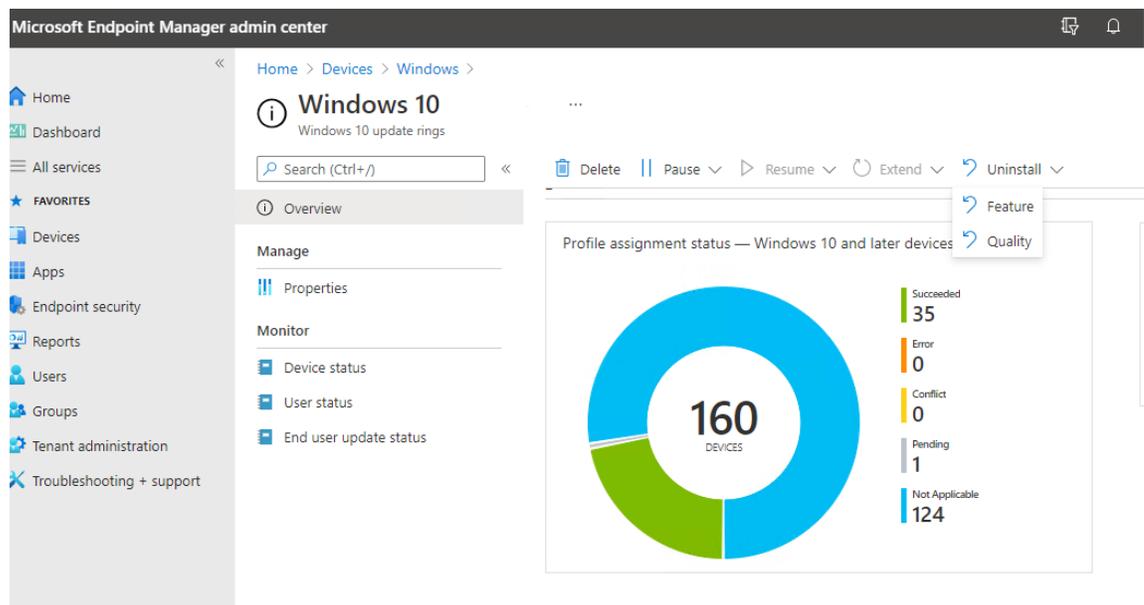


Figure 4.3 – Windows 10 Update Ring Defined

Remote Support and Troubleshooting

Remote support and troubleshooting for endpoints can be improved dramatically, especially for laptops and mobile phones which prior to cloud migration, did not have any ability for remote support. The platform that can now

be discovered as a possibility is direct Integration with TeamViewer. TeamViewer is a “comprehensive remote access, remote control, and remote support solution that works with almost every desktop and mobile platform, including Windows, macOS, Android, and iOS” (Teamviewer.com, n.d). Now that Intune is properly configured, the IT Department can now connect and directly integrate with the built-in TeamViewer Connector as seen in Figure 4.4. Helpdesk technicians will be able to click on a user’s endpoint regardless of where it is and initiate a New Remote Assistance Session with any device as seen in Figure 4.5. It is important to note that the figures do not show the proper configuration of the TeamViewer connector because at the time of the project the licensing costs were being determined. However, a plan in the near future for the TeamViewer integration is certainly being considered.

Microsoft Endpoint Manager admin center

Home > Tenant admin > Connectors and tokens

Connectors and tokens | TeamViewer connector

Search (Ctrl+/) << Connect Refresh

Windows	Connection status	Last connection	Connection request expires
Microsoft Store for Business	Requires setup	--	--

Windows

- Microsoft Store for Business
- Windows enterprise certificate
- Windows Symantec certificate
- Windows side loading keys
- Microsoft Endpoint Configuratio...

Apple

- Apple VPP Tokens

Android

- Managed Google Play

Cross platform

- Microsoft Defender for Endpoint
- Mobile Threat Defense
- Partner device management
- Partner compliance management
- TeamViewer connector**
- Certificate connectors
- Telecom expense management
- Derived Credentials

Information: New connection requests expire after 15 minutes. If the Connection status is not Active within 15 minutes, click Connect to start a new request.

The TeamViewer service allows users of Intune-managed devices to get remote assistance from their IT administrator. Create TeamViewer sessions by first associating Intune with your TeamViewer account and then authorizing it to work with Intune. If you don't yet have a TeamViewer account you will need to create one.

[Log in to TeamViewer to authorize](#)

Figure 4.4 – TeamViewer Connector for Intune

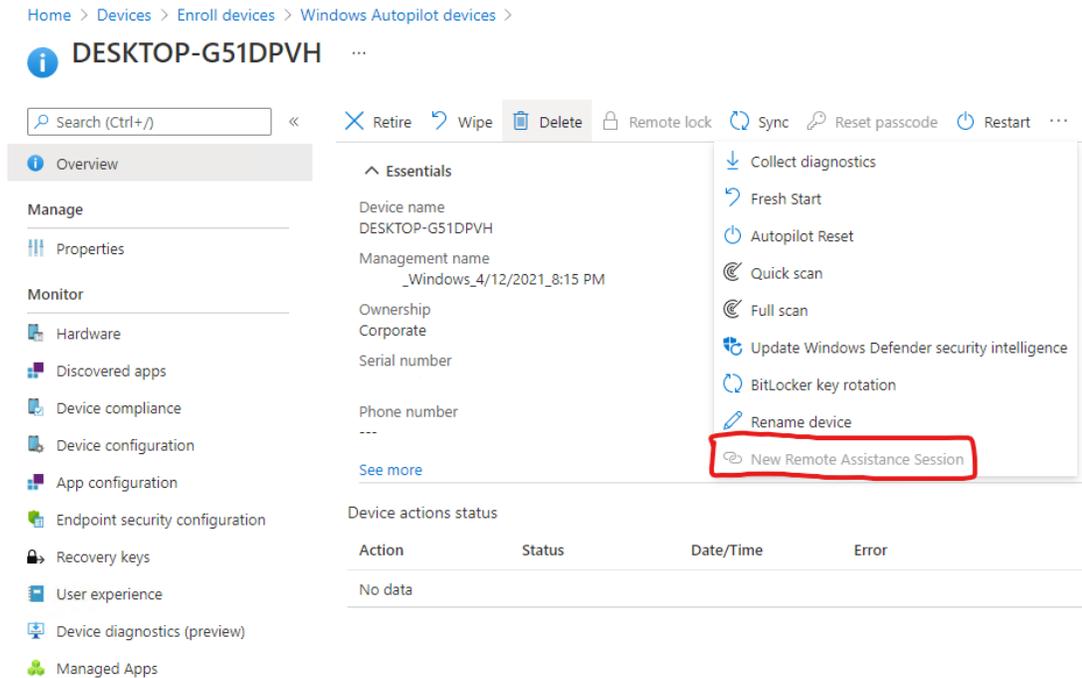


Figure 4.5 – Remote Assistance Session Capability for Endpoint

New Endpoint Security Capabilities

As previously mentioned, the IT Department is responsible for providing endpoint security in the areas of Device Compliance and Threat Protection. This section will cover how the IT Department is able to carry out each of those responsibilities in the new environment.

Device Compliance

After configuring each of the cloud services, and onboarding endpoints, the IT Department gained a significant advantage in their ability to view device compliance. Endpoint Manager allows for the IT Department to view and manage

all their devices compliance in a single area. Compliance policies can ensure a system has adequate threat protection installed, or bit locker drive encryption enabled, or even be a specific OS version. Actions can be taken for devices that are not in compliance as well such as indicating a message for a user to initiate an update, or even heavier actions such as removing corporate data and not allowing access to corporate resources. When browsing through Endpoint Manager an icon is displayed to indicate whether the endpoint is compliant as seen in Figure 4.6.

Device name	Managed by	Ownership	Compliance	OS	OS version
iPhone SE	Intune	Corporate	Compliant	iOS/iPadOS	14.4.2
Administrator's iPhone	Intune	Corporate	Not Compliant	iOS/iPadOS	13.4.1
BRENT's iPhone	Intune	Corporate	Compliant	iOS/iPadOS	14.4.2
Bauller iPad 8thGEN 4145	Intune	Corporate	Compliant	iOS/iPadOS	14.4.2
	Intune	Personal	Not Compliant	Windows	10.0.18362.657
DESKTOP-6PQFDHV	Intune	Personal	Compliant	Windows	10.0.19041.928
DESKTOP-9JLK37L	Intune	Personal	Not Compliant	Windows	10.0.19041.928
DESKTOP-GS1DPVH	Intune	Corporate	Compliant	Windows	10.0.18363.476
DESKTOP-HOFTGIQ	Intune	Personal	Not Compliant	Windows	10.0.19041.867
DESKTOP-HNRA70S	Intune	Personal	Not Compliant	Windows	10.0.19042.867

Figure 4.6 – Device Compliance in Endpoint Manager

Threat Protection

Perhaps one of the greater benefits the IT Department has gained during the project is the benefit that comes with Microsoft Defender for Endpoint. The amount of information provided in the Microsoft 365 Security Center portal is far

more than the IT Department's previous solution with Trend Micro Smart Protection for Endpoint. The IT Department can respond to threats more quickly as well as drill down deeper into investigations using the new Defender for Endpoint service. Furthermore, the centralized dashboard for alerts allows for the Information Security team to be able to quickly identify which endpoints are impacted and begin to investigate as seen in Figure 4.7

The screenshot shows the Microsoft 365 Security Center Alerts dashboard. The left sidebar contains navigation options: Home, Incidents & alerts (with sub-items Incidents and Alerts), Hunting (with sub-items Advanced hunting and Custom detection rules), Action center, Threat analytics, Learning hub, and Endpoints (with sub-items Search and Device inventory). The main content area is titled 'Alerts' and includes an 'Export' button, a '30 Days' filter, and a 'Manage alerts' link. Below this, there are filter options for 'Status: New +1'. The alert list table is as follows:

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity
'Conteban' malware was prevented		Informational	Terminated by system	New	Malware	Antivirus		Apr 11, 2021 2:41 AI
'Conteban' malware was prevented		Informational	Terminated by system	New	Malware	Antivirus		Apr 11, 2021 2:36 AI
'Conteban' malware was prevented		Informational	Terminated by system	New	Malware	Antivirus		Apr 11, 2021 2:36 AI
'Conteban' malware was prevented		Informational	Terminated by system	New	Malware	Antivirus		Apr 11, 2021 2:34 AI
'Conteban' malware was prevented		Informational	Terminated by system	New	Malware	Antivirus		Apr 11, 2021 2:32 AI
'Conteban' malware was prevented		Informational	Terminated by system	New	Malware	Antivirus		Apr 11, 2021 2:27 AI
Artifact was blocked based on malicious beh...		Informational		New	Malware	Antivirus		Mar 24, 2021 11:28 I

Figure 4.7 – Microsoft 365 Security Center Alerts

Another added benefit of Defender for Endpoint is a feature found in the Threat and Vulnerability Management dashboard as shown in Figure 4.8. The dashboard allows the IT Department to see their overall vulnerability from an exposure score. A low score will indicate a lower risk of exposure, whereas a higher score indicates a higher risk of exposure. The IT Department is also able to see Top security recommendations from Microsoft that will directly assist with reducing the H2O districts overall vulnerability. Although there are many

capabilities of Microsoft Defender for Endpoint, these tools directly assist the IT Department with being able to assess their overall security posture against active threats and turn them into action items.

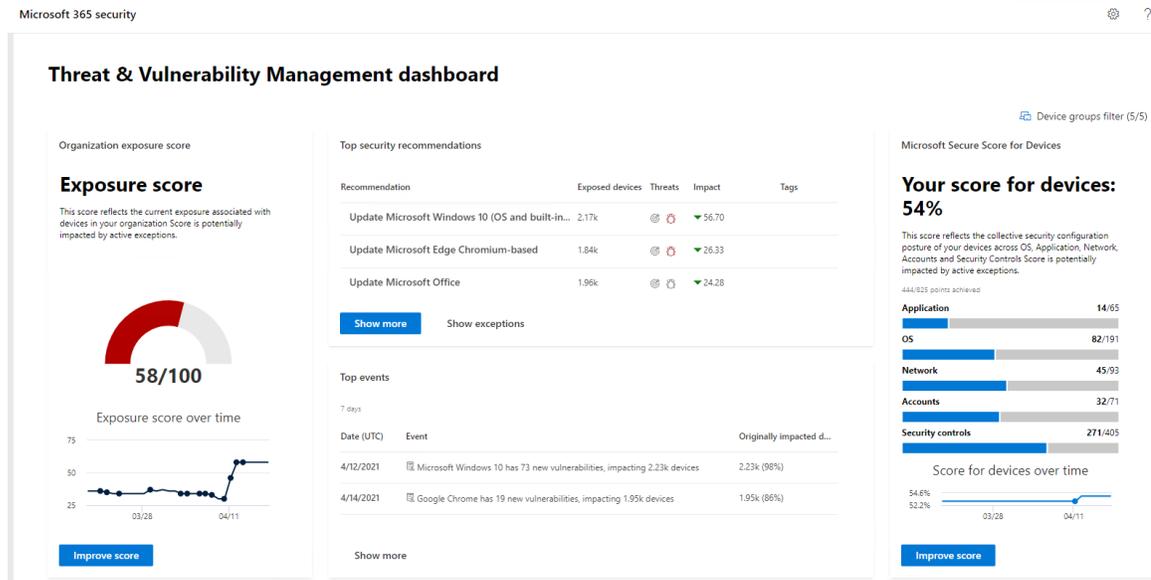


Figure 4.8 – Threat and Vulnerability Management Dashboard

CHAPTER FIVE

CONCLUSION

Chapter Overview

This chapter will conclude by unveiling some of the new opportunities as well as challenges that H2O District and other organizations in a similar situation will face. Determining a way to effectively manage and secure endpoint devices was just one of the many challenges brought forth by the COVID-19 pandemic. Fortunately, the foundation has been laid for the H2O District to be able to cope with the forthcoming issues as the organization continues to evolve during these uncertain times. The chapter will conclude by offering a summary of the new solution, and some of the future tasks ahead for the IT Department.

New Opportunities and Challenges

Growing Trend in Hybrid Remote Work

There is no doubt that the COVID-19 pandemic impacted the way IT Departments support organizations. Evidence of the rapid shift in the workforce can be seen by examining some of the key players in the teleconferencing industry such as Zoom, Cisco Webex and Microsoft Teams. In December of 2019 Zoom had 10 million daily participants, but fast-forward to October 2020 and the platform had 300 million users who were logging into the platform (Arif, 2021). In March of 2020 Cisco Webex recorded 324 million participants, only to have merely doubled to 600 million on October of 2020 (Mukherjee & Nellis,

2020). In March 2020 Microsoft reported 32 million daily active users - one month later in April 2020 that number jumped to 75 million daily active users, and 6 months in October 2020 later the number grew to 115 million (Spataro, 2020). Furthermore, as the world continues to open, there is a growing trend of workers now beginning to have a hybrid work schedule, meaning that they will be working partially at home as well as in-person on premise. In a survey conducted by Microsoft in March 2021 it was discovered that 73% of workers wanted flexible remote work options, while 67% of workers were craving more in-person time with their teams (Microsoft, pg. 5, 2021). These numbers accurately reflect the sentiment among the employees at the H2O district. There are already projects being initiated and such as the redesigning of conference rooms, temporary locations to perform work while onsite, as well as migrating internal applications to be accessible from home locations. As many organizations throughout the world have proven that work tasks can be performed from home, IT leaders will be faced with providing options for the remote workforce while at the same time being able to properly manage and secure each endpoint.

As the hybrid workforce is touted to become the next disruption, IT Departments across the world must be able to adapt and respond to such demands. Operational procedures such as providing or servicing equipment in people's homes will have to be properly planned and considered. Better insight and visibility into endpoints must be solidified and properly understood. Training of personnel to become familiar with the current cloud-technologies must become

a priority. Additionally, growing cybersecurity concerns such as phishing attacks, security patching, vulnerable home environments, and employee error must be addressed (Caserella, 2021). It is undeniable that a hybrid workforce will introduce new challenges, pose new threats, and warrant conversations between leaders on how to respond to such impacts. Ultimately, it is important for IT leaders to recognize the growing concerns of the hybrid workforce and be able to implement technological solutions that resolve the forthcoming business impacts associated with a change in the workforce.

Managing the Flow of Information

As the growing trend of remote workers and remote endpoints continues so will the growing trend in data existing outside of the network. Data is one of the most critical components of any organization and is proven to be costly in the event an incident occurs that involves a data breach. In an annual study released by IBM it was determined that the average cost of a breach totaled \$3.86 million dollars (IBM, pg.5, 2020). Given that data breaches can be quite costly, organizations typically find it valuable to classify data and govern how it is managed. Some of the common forms of data breach can typically include customer or employee personally identifiable information (PII), names and dates of birth, social security numbers, tax IDs, financial account information, medical records, payment card data, usernames and passwords, and the list goes on and

on (Palo Alto Networks, 2020). Given the significant cost of a data breach and the type of data that is proven valuable, it is important to identify what type data exists in an organization, where it exists, and how to properly safeguard that information as it travels to and from the network. Fortunately, Microsoft has developed products to assist with the classification and management of information through an organization.

The H2O District and organizations across the world will need to plan out accordingly on how they will wish to classify and govern the flow of their data as it leaves the network. In the Forrester study consisting of 157 IT security decision-makers, 57% of leaders mentioned that identifying sensitive and at-risk data would make their endpoint management more effective (Forrester, pg.5, 2021). Properly managing and securing an endpoint is just one piece of the puzzle when it comes to protecting information. IT leaders will still need to determine. Microsoft recommends discovering data wherever it is created or lives, classifying data with labels, protecting data with policies, and monitoring data to prevent misuse (Microsoft, 2018). Now that the endpoints are properly managed and enrolled into Intune, H2O district can begin looking at products such as Office 365 Advanced Data Governance to help assist with classifying data or discovering what type of information exists within their environment. Or perhaps IT leaders can utilize Office 365 data loss prevention (DLP) to assist with identifying and protecting information as it flows across the network onto specific devices. Furthermore, the organization can leverage Azure Information

Protection which assists with managing information across cloud services by allowing them to provide protection to their data such as encryption across each of their endpoints. Indeed, managing the information and data as it flows across networks, cloud services, and onto each endpoint would be the next step of the journey towards safeguarding an organization's information.

Establishing Zero Trust

Perhaps one of the more crucial conversations to be had for any organization is adopting a Zero Trust strategy. In a world where people, endpoints, and information leave the network, it is important to be able to extend security beyond the traditional internal networks and ensure that an organization can withstand the threats associated with having no boundaries. Zero Trust is a term defined by the National Institute of Standards and Technology (NIST) as “an evolving set of cybersecurity paradigms that moves defenses from a static, network-based perimeters to focus on users, assets, and resources” (Rose et al. pg. ii, 2020). As previously mentioned, the former philosophy on fortifying defenses and creating a perimeter is no longer useful in a post COVID-19 pandemic world. In 2020 a study was conducted by Okta – a worldwide leader in providing identity and authentication services – indicating that there was a 275% increase in a single year for organizations in North America to have a plan for a for zero trust in the next 12-18 months, and that 60% of organizations in North America were actively working on zero trust projects (okta, p.4, 2020). It would

certainly be advantageous for any organization to start planning to adopt a strategy that ensures that security can be extended beyond the traditional network infrastructure. Indeed, one of the critical components of establishing Zero Trust is being able to properly manage and secure and gain visibility into endpoints as they access information and resources from both inside and outside the network. Ultimately every Zero Trust strategy will be different for organizations, but now more than ever would be the time for IT leaders to adopt Zero Trust into their overall strategy.

Microsoft applies a Zero Trust into many of their products and uses it as a guideline to the services they deliver. Microsoft's slogan is to "Never Trust, Always Verify," and the guiding principles to obtaining Zero Trust is to verify explicitly all data points, use least privileged access using just-in-time or just-enough-access risk-based adaptive policies, and always Assume breach by segmenting access by network, user, devices, and app awareness (Microsoft, p.2, 2020). By laying down the foundation with the Microsoft services in this project, organizations will have the ability to transition smoothly towards a strategy that will closely align them with a Zero Trust security model. Defender for Endpoint is a clear example of how an organization will assume breach on all their devices by using analytics to gain visibility and minimize the damage that can be incurred by preventing lateral movement by isolating a device in the event of an incident. Furthermore, Intune can assist with establishing the identity of a device once it is enrolled and granting access to resources. Given that the

endpoints are now effectively onboarded into Endpoint Manager, the next part of the conversation is to IT leaders to determine their Zero Trust strategy for their organization.

Conclusion

The overall purpose of this project was to provide a solution for the H2O District that will allow the IT Department to effectively manage and secure their endpoints in a telework environment. Given the circumstances brought on by the COVID-19 pandemic, the IT Department was forced to assess their current environment and determine the best path forward that would allow them to continue to fulfill their core responsibilities. For managing endpoints, the IT Department needed a solution that would help them maintain their ability to provide software deployments and updates, operating system support, as well as remote support or troubleshooting. For securing endpoints, the IT Department needed a solution that would allow them to ensure device compliance and threat protection. It was determined that the most effective solution forward was to leverage the cloud services provided from their Microsoft 365 E5 license. This solution allowed the IT Department to utilize a combination of cloud services such as Azure, Intune, Defender for Endpoint, and Endpoint Manager.

The solution provided in this project proved to meet the needs of the IT Department. The IT Department is now able to effectively manage and secure H2O District endpoints in a telework environment. Prior to the project implementation the IT Department had no visibility or communications into their

endpoints once they left the network. Additionally, the IT Department did not have the infrastructure or necessary configurations to support endpoint devices as given their current configuration. Now the IT Department can deploy applications to all their endpoints from Intune regardless of location. Furthermore, the IT Department can carry out common tasks such as deploying software updates, patching vulnerabilities, responding to lost mobile devices, ensuring device compliance, and detecting or responding to incidents in real time. The project significantly aided in the H2O district's ability to resume their operations and meet the technical demands during a worldwide pandemic.

The IT Department certainly has quite a few goals on the agenda in the upcoming future. The foundation for managing and securing endpoints has been set forth and now the IT Department will need to prepare for future goals. Defining appropriate compliance policies and baselines will need to be determined to satisfy information security concerns. Determining the best ways to support a remote workforce will need to be addressed across all divisional units including Human Resources. Establishing a path towards Zero Trust and managing the flow of information will need to be properly strategized. Without a doubt the IT Department will have a never-ending list of growing responsibilities and challenges to overcome. Fortunately, the solution described in this project has proven to be resilient in allowing the IT Department to meet H2O District's goals to adapt, effectively manage, and secure their endpoints regardless of

where they exist and regardless of what challenges may present themselves in the future.

APPENDIX A
ACRONYMS AND ABBREVIATIONS

ABM	Apple Business Manager
AD	Active Directory
AD-DS	Active Directory Domain Services
APP	App Protection Policy
BYOD	Bring Your Own Device
CMG	Cloud Management Gateway
DLP	Data Loss Prevention
IoT	Internet of Things
IT	Information Technology
ITCS	Information Technology Customer Support
MECM	Microsoft Endpoint Configuration Manager
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PC	Personal Computer
SCCM	Microsoft System Center Configuration Manager
OS	Operating System
MDM	Mobile Device Management
SSO	Single-Sign On
VPN	Virtual Private Network

BIBLIOGRAPHY

- Anderson, Brad. (2019, November 4). *Use the Power of Cloud Intelligence to Simplify and Accelerate IT and the Move to a Modern Workplace*. Microsoft. Retrieved March 3, 2021, from <https://www.microsoft.com/en-us/microsoft-365/blog/2019/11/04/use-the-power-of-cloud-intelligence-to-simplify-and-accelerate-it-and-the-move-to-a-modern-workplace/>
- Apple (2019, October). *Getting Started Guide – Apple Business Manager*. Retrieved March 03, 2021, from https://www.apple.com/business/docs/Site/Apple_Business_Manager_Getting_Started_Guide.pdf
- Arif, R. (2021, February 26). *In The Post COVID-19 World, Zoom Is Here to Stay*. Forbes. Retrieved March 24, 2021, from <https://www.forbes.com/sites/raufarif/2021/02/26/in-the-post-covid-19-world-zoom-is-here-to-stay/?sh=b04a9ba55b58>
- Bromiley, M. (2021, March 15). *SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey*. Retrieved March 19, 2021, from <https://www.sans.org/Reading-room/whitepapers/analyst/membership/40200>
- Casarella, D. (2021, March 01). *Cybersecurity Tips for a Remote or Hybrid Workforce*. Retrieved March 24, 2021, from <https://www.uschamber.com/co/run/technology/hybrid-workforce-cybersecurity>
- Fields, A. (2019, June 17). *Updated Licensing Graphics*. ITPromotor. <https://www.itpromotor.com/updated-licensing-graphics/>.

- Foley, M. (2018, October 26). *Microsoft Launched Azure 10 Years Ago and lots (but not Everything) has Changed*. Retrieved March 10, 2021, from <https://www.zdnet.com/article/microsoft-launched-azure-10-years-ago-and-lots-but-not-everything-has-changed/>
- Forrester Consulting. (2021, March). *Take A Proactive Approach to Endpoint Security*. Retrieved April 1, 2021, from <https://www.absolute.com/go/study/proactive-approach-endpoint-security-forrester-study/>
- Goodwin, S. (2021, March 10). *Remote Workforce Impact on Threat Defenses*. SANS. Retrieved March 19, 2021, from <https://www.sans.org/reading-room/whitepapers/telecommunting/remote-workforce-impact-threat-defenses-40180>
- IBM. (2020). *Cost of a Data Breach Study 2020*. Retrieved March 17, 2021, from <https://www.ibm.com/security/data-breach>
- Kirsch, C. (2016, March 31). *IDC: 70% of Successful Breaches Originate on the Endpoint*. Retrieved March 12, 2021, from <https://www.rapid7.com/blog/post/2016/03/31/idc-says-70-of-successful-breaches-originate-on-the-endpoint/>
- Lardinois, Frederic. (2019, November 4). *Microsoft Launched Endpoint Manager to Modernize Device Management*. TechCrunch. Retrieved March 18, 2021 from <https://techcrunch.com/2019/11/04/microsoft-launched-endpoint-manager-to-modernize-device-management/>

- Lueth, K. L. (2020, November 19). *State of the IoT 2020: 12 billion IoT Connections, Surpassing Non-IoT for the First Time*. Retrieved March 17, 2021, from <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/>
- Mearian, L. (2019, December 4). *Microsoft's Intune is Now Endpoint Manager: What is it, and How Well Does the UEM Tool Work?* Computerworld. <https://www.computerworld.com/article/3304583/what-is-microsofts-intune-and-how-well-does-it-really-work.html>.
- Microsoft. (n.d.). *App Protection Policies Overview*. Microsoft. Retrieved March 20, 2021, from <https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy>
- Microsoft. (n.d.). *Compare Microsoft 365 Enterprise Plans*. Microsoft. Retrieved March 03, 2021, from <https://www.microsoft.com/en-us/microsoft-365/compare-microsoft-365-enterprise-plans>
- Microsoft. (n.d.). *Microsoft Defender For Endpoint*. Microsoft. Retrieved March 02, 2021, from <https://www.microsoft.com/en-us/microsoft-365/security/endpoint-defender>
- Microsoft. (2020, May 21). *Microsoft Endpoint Manager Overview*. Microsoft. Retrieved March 5, 2021, from <https://docs.microsoft.com/en-us/mem/endpoint-manager-overview>
- Microsoft. (2021, April 4). *Plan for the Cloud Management Gateway in Configuration Manager*. Microsoft. Retrieved March 2, 2021, from

<https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmng/plan-cloud-management-gateway>

Microsoft (2018). *Trusted Information Protection*. Microsoft. Retrieved March 12, 2021, from <https://microsoft.com/en-us/security/business/information-protection>

Microsoft. (n.d.). *What is Co-Management?* Microsoft. Retrieved March 6, 2021, from <https://docs.microsoft.com/enus/mem/configmgr/comanage/overview>

Microsoft. (n.d.). *Windows 7 support ended on January 14, 2020*. Microsoft. Retrieved March 03, 2021, from <https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962>

Microsoft (n.d.). *Zero Trust Maturity Model*. Microsoft. Retrieved March 12, 2021, from <https://www.microsoft.com/en-us/security/business/zero-trust>

Microsoft (2021, March 22) *The Next Great Disruption Is Hybrid Work – Are we Ready?* 2021 Work Trend Index: Annual Report. https://ms-worklab.azureedge.net/files/reports/hybridWork/pdf/2021_Microsoft_WTI_Report_March.pdf

Mukherjee, S., & Nellis, S. (2020, October 23). *Cisco's Webex Participants Near 600 Million as Pandemic Flares Again*. Reuters. Retrieved March 24, 2021, from <https://www.reuters.com/article/us-cisco-systems-webex/ciscos-webex-participants-near-600-million-as-pandemic-flares-again-idUSKBN278018>

- Okta. (2020). *The State of Zero Trust Security in Global Organizations*. Retrieved March 17, 2021, from <https://www.okta.com/resources/reports/state-of-zero-trust-security-in-global-organizations/>
- Palo Alto Networks (2020). *2020 Incident Response and Data Breach Report*. Retrieved March 13, 2021 from <https://start.paloaltonetworks.com/cybersecurity-threat-report.html>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August). *Zero Trust Architecture*. National Institute of Standards and Technology. <https://doi.org/10.6028/nist.sp.800-207>
- Spataro, J. (2020, October 30). *Microsoft Teams Reaches 115 Million DAU-plus, A New Daily collaboration Minutes Metric for Microsoft 365*. Retrieved March 18, 2021, from <https://www.microsoft.com/en-us/microsoft-365/blog/2020/10/28/microsoft-teams-reaches-115-million-dau-plus-a-new-daily-collaboration-minutes-metric-for-microsoft-365/>
- Sumologic. (n.d.). *What is Software Development?* Retrieved March 06, 2021, from <https://www.sumologic.com/glossary/software-deployment/>
- Swoyer, S., & Magoulas, R. (2020, May 19). *Cloud Adoption in 2020*. Retrieved March 20, 2021, from <https://www.oreilly.com/radar/cloud-adoption-in-2020/>
- TeamViewer. (n.d.). *What is TeamViewer?* TeamViewer. Retrieved March 05, 2021, from <https://www.teamviewer.com/en-us/products/teamviewer/>

Verizon. (2020). 2020 Data Breach Investigations Report. Retrieved March 12, 2021, from <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>