Journal of Business Studies Quarterly
2022, Volume 12, Number 1
ISSN 2152-1034

Journal of Business Studies Quarterly jbsq.org

Moving Towards A Modern Desktop by Migrating Group Policy to Intune Policy

Matthew E. Hudson, Texas A&M University, United States
Ben Zoghi, Texas A&M University, United States

Abstract
Machines managed by on-prem technology are prohibited from existing primarily on the Internet. To manage these devices we must remove barriers, one such barrier is the management policy, Active Director Group Policy Objects (GPO). A mixed approach is utilized; quantitative data resulting from the Microsoft Intune telemetry was captured and reviewed, Policy Conflicts and Errors were reviewed against the organic growth of machines that consumed the policy; qualitative data from Global Service Desk, Onsite Admins, and users were collected to determine machine behavior issues. If a discrepancy from either method was detected actions were taken to understand and clarify the results. By moving towards a Modern Desktop, the company is able to achieve a portion of the Digital Transformation corporate objective. In addition, the eventual removal of Domain Controllers will result in $284.45 per month, per machine for the life of the device, the financial benefits will largely multiply, depending on the number of machines that implement changes. Through this new method and process, the Active Directory team now has a continual process to review and move policies to the Cloud. Other businesses and organizations could learn from the results of this project by reviewing their current policies and evaluating the potential benefits and risks before making a strategic move.

Keywords: GPO, Intune, Policy, Group Policy, Cost-saving.

1. Introduction

The Modern Desktop is a state describing a situation of a machine that exists anywhere and provides productivity to the user. Reprovisions, software updates, application deployments, and management of the machine are performed via the Internet.

During the COVID-19 pandemic of 2020, more than 80,000 workstations were moved outside the corporate network. Machines that would log in via the Internet were slow to reach a

stable Windows desktop as the GPOs were pulled from on-prem servers and were either lost or delayed in transmission. It is still necessary for the company to advance its Cloud presence while simultaneously causing zero impact to all business operations, onshore, offshore, joint ventures, company acquisitions, divestments, and while adhering to all trade compliance or export laws for each country.

Once reliance on Active Directory authentication and on-prem certificates the Active Directory servers can be decommissioned. Workstation machines will utilize Azure Active Directory singularly. A Work from Anywhere (WFA) environment has no reliance on Active Directory for policy, certificates, or authentication. These actions are replaced by Azure processes and performed over the Internet. Corporations, and the world, must work towards a Modern Workplace if they hope to remain relevant in a landscape where working via the Internet was as once pervasive as working inside the physical office. The problem and solution presented in this project will create a stronger End User Digital Experience for employees having never realized the change which occurred beneath them.

2. Literature Review

A. *The shift to remote work*

There have been many studies on the effects and usefulness of working from home, especially with the dramatic changes attributed to COVID-19. Looking back towards the second half of the 1940s when men were returning from World War II and women were told to return to the home after spending time away from the home in the workforce, women approved of the change and desired to remain in the workforce instead of heading back to the domicile. As many as "54% wish to continue working from home after the pandemic (Parker et al., 2020) "This can be attributed to an increase in work-life balance, spending less time in traffic, and the ability to work in a more comfortable environment. To attain this freedom Parker et al. (2021) state that, "about three-quarters or more say it has been easy to have the technology and equipment they need to do their job and to have an adequate workspace."

It is evident from the research that the younger the employees are more able to adopt and adapt to the new technology medium. While the ability to work outside the company is critical for many of the teleworkers, they are unaware of the technology on the backend infrastructure necessary to continue support for such a shift. Companies must learn to change or be left behind as the workforce abandons them.

Choudhury et. al. (2021) break down how geography affects the WFH and WFA scenario for various employees for the US Patent Office (USPTO) in their paper, "*Work-from-anywhere: The productivity effects of geographic flexibility*", "While traditional work-from-home (WFH) programs offer the worker temporal flexibility, work-from-anywhere (WFA) programs offer both temporal and geographic flexibility" (Choudhury et al., 2021) This means that many companies can offer temporary or full-time remote work options. Normally these infrastructures are implemented for the few, not the masses. They note that "workers are no longer required to live in the same geographic location as the firm and have greater flexibility to choose where to live."

While it offers greater flexibility, they fail to include research on how larger or global companies have multiple VPN points of presence across the world to support such an endeavor. Their largest distance described is 50 miles where he states, "those living more than 50 miles from the office for WFH" and "WFA examiners residing over 75 miles away", not taking into

account those that are on a different continent changes the dynamics of the research and behemoth undertaking to achieve such a shift (Choudhury et al., 2021). What is vital in this research is how much the environment is impacted by the commuting workforce. They state that USPTO "estimated that its remote workers avoided driving 84 million miles, thus reducing emissions by more than 44,000 tons" As sustainability and carbon footprint reduction become motivating factors for companies, continued research in this area is necessary (Choudhury et al., 2021).

These studies failed to consider the technology turmoil that must first occur in the background to allow the employees to be productive at home. Burrows, convincingly states in his article, "*VPN vs Cloud: The Case for Sunsetting the VPN*" that "Suddenly, everyone was working from home, and unless you could quickly get your hands on the on-premise hardware required to run traditional VPNs (known as VPN concentrators), companies were hard-pressed to keep workers supplied with secure, reliable connections." (Burrows, 2021). With the expansion of a mobile workforce Varco, in 2016, "moved more than a dozen of its VPN routers and moved to a cloud-based service that offered hundreds of access points around the globe." (Burrows, 2021). Meaning they are better poised to support a workforce that moved home during the pandemic. "Small businesses have fewer financial resources" forcing them to spend more money, forcing the office to require employees to enter the office or close the doors to the business according to Bolozdiņa, et al. (2020).

Microsoft saw the value in the ubiquitous of Cloud management and the need to abstract the machine from the employee layer. In an article written by Microsoft, they outline the benefits of moving management to the cloud for mobile employees, work from home, and how easily it could be used for WFA (Jain, 2020 Mar 31), They began by asking the question "when these devices are no longer on-premises and are not expected to "check in" to the corporate network for weeks, how do you ensure they remain managed and up-to-date?" The answer was Cloud management but how do you allow the company to maintain business continuity while providing for the future? Co-management was the answer that created a bridge or destination for the corporate back-end where workloads are slowly moved unbeknownst to the workforce.

B. *Active Directory past and present, is it secure?*

In 2002 AD was just a toddler in the sense it was slowly growing but not yet mature. At the time Bradbury states the benefit of having "one place [to manage] their access rights to multiple systems can save IT departments much time and energy, not to mention cost" similar to the conversations Cloud was in 5 years ago (Bradbury, 2002 September 12).

Within the article by Bradbury, a case study is presented with House of Fraser concluded that adopting the technology allowed for a small infrastructure that was "completely new to us and a bit scary," like any new technology. Adoption and trust are inherently slow. Active Directory was the standard to manage the Microsoft estate for policy and device management. Today Microsoft Intune has become the standard for management via the Cloud. Neither has escaped negative opinions. When Active Directory was released "IT managers complained about the training problems with the implementing such a large architecture." (Parker et al., 2020). Something that is echoed with today's IT admins when implementing Intune for Machine management." Bolozdiņa, et al. (2020). "An analysis of company size indicates that there is a relationship between the size of the company and IT infrastructure." As a company grows, so does the complexity of the IT systems. The same could be said about cloud-based management.

“Gartner does not, under most circumstances, recommend a wholesale migration to Windows 2000” (Morgan, 2000 January). This shows how little the technology community had faith in a Microsoft Architecture to manage machines. This is significant because in 2021 Gartner named Microsoft as the lead in device management, both cloud on on-premises. In his article, Wallent (2021 August 31) states that "[Cloud-based management] is foundational to enabling employee productivity in hybrid work environments. From remote to frontline workers and from large enterprises to small, Microsoft is recognized for its ability to execute and completeness of vision for Endpoint Manager.”

It is now time to move away from Active Directory in favor of a Cloud management solution such as Intune.

In July of 2021 a backdoor was discovered in the Printer spooler service, Print Nightmare, affecting machines and Domain Controllers in Active Directory. This is alluded to by Grillenmeir when the author states “In the worst case, the intruder could gain access to such a system and furthermore find that your domain controllers still have the printer service (spooler) running” (Grillenmeir, 2021 July). “In the case of the SolarWinds attack, the intruders were able to use this federation [Active Directory] to their advantage for stealthy access to the Orion source code hosted in the cloud by stealing the token signing certificate.” (Constantin, 2020) This points to the [necessity] to retire this on-prem model and move to Azure and Intune for management and the security of the devices.

This is also in regards to vulnerabilities found in Group Policy. Constantin describes a method to update a policy on the server and simply wait for the policy to propagate (Constantin, 2020). “The flaw is old and exists in all Windows versions for desktops and servers beginning with Windows Server 2008”. Because “updates are not instant by default and usually take time to propagate over a network.” “So, if you manage to find a bug in the Group Policy update process, you can trigger it yourself whenever you want to — making a potential attack easier.” (Constantin, 2020). These types of issues should propel companies to rethink their current state.

C. *Moving to Cloud*

Migrating machine management to the cloud contains many layers, one such layer is the policy layer. This is the compliance and control layer to which the machines must adhere. In *“IT-infrastructure Migration and Modernization”* the author explains how Active Directory infrastructure is reviewed and revised to create a more manageable environment for machine management (Ekholm, 2021 June 2).

This project stops short of the real need for cloud management and the need to migrate (GPO). They collapsed the Domain and adopted the portion of Cloud for Cloud Management Gateway (CMG). The CMG is capable of disseminating policy and application deployment from the Cloud. In a hybrid situation, as discussed in the article, the next prudent move will be to migrate GPO to Intune, removing 1 more reliance on the internal network.

Näsi (2020 October) writes the thesis about implementing Intune at Varala Sports College. It is worth noting that the author states “It is desirable to understand the current and future business needs of your organization and how they fit into the corporate strategy. If a deployment does not take into account the long-term approach to mobile management, it is possible that shorter-term solutions will not scale with organizational change and growth.” (Näsi, 2020 October). This is crucial because moving to the Cloud is not a simple process, it requires

critical planning for both the business and technology teams, and the move must create value for the company.

By 2022, Gartner states, “50% of company-owned Windows 10 PCs will be managed using EMM software or UEM tools. That this should help companies boost operational efficiency. The difficult part for many will be choosing whether to use something like Intune or cobble together a management ecosystem built on software from a number of third-party vendors (Finnegan & Marian, 2021 Aug 23). This article describes the use of Intune to manage devices. "Adame agrees that "it is designed to make it easier to manage a variety of devices in a way that protects corporate data while still allowing employees to do their jobs using both corporate and personal devices” (Adame, 2021 August).

In addition, “the software’s integration with Microsoft’s Azure AD and Azure Information Protection enables admins to classify (and optionally protect) documents and emails by applying access rules and conditions” (Finnegan & Marian, 2021 Aug 23). This is significant because it shows the policy is also integrated into Azure AD security principles, a growth from Active Directory and necessary for a Zero Trust initiative.

Adame continues with the importance of managing the machine via the cloud, previously 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..." This calls attention to the issue of managing machines once they leave the corporate network. This is a "solution to manage the devices outside the corporate network in a way similar to how it was previously performed inside the network as now part of a telecommuting environment "Those include keeping up with the growing trend in hybrid remote work, managing the flow of information, and establishing zero trust." "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" (Adame, 2021 August).

They concluded that moving to cloud management was the “most effective solution forward” and “prior to the project implementation the IT Department had no visibility or communications into their endpoints once they left the network.”

They promotingly state “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” (Adame, 2021 August).

This is the experience that all companies desire once their policy is managed via the Cloud.

3. Methodology

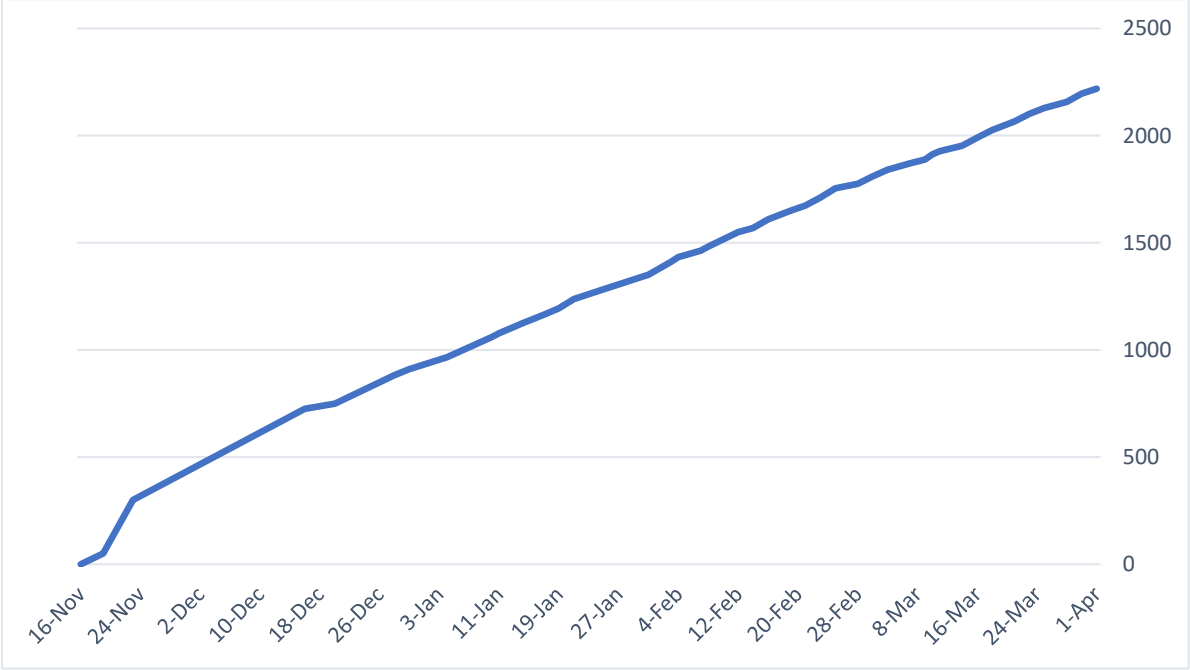
Participants

Machines

Only machines running Windows 10 21H2 Operating System and co-managed within the environment were targeted with the new policy. The Private Preview group, shown in Figure 1, consists of any machine in the environment that through their own actions or another, are upgraded to Windows 10 21H2. This group has grown at an organic rate since the initially

released date of the Operation System on November 16, 2021. The first release of policy to the Private Preview machines occurred on December 16, 2021.

Figure 1: Machine Enrollment



Users

Procedure

Core Windows 10 policies were identified from the current set of Group Policy Objects (GPOs). This consisted of over 26 GPOs housing more than 900 settings to manage the core devices of the company. Each setting was reviewed by the service owner, to determine validity, relevance, and if any changes were required. Once confirmed, the setting was implemented in Intune, either in the Configuration Service Provider (CSP) or Settings Catalog.

Upon creation, they were tested in labs for two weeks. Policies passing validation were released to the Private Preview group every four weeks in accordance with standard Change Management procedures. If a problem was detected in either the lab or the Private Preview, it was removed for review.

Data Analysis

The Active Directory team will compile their own procedure based on their experiences, then create a continual process to move all Group Policies to Intune.

Quantitative results

From several GPOs that support Windows 10, settings were reviewed for continued relevance and if they only existed for on-prem management. From this review process, 65 settings were selected; 6 were excluded for on-prem management while 5 Settings were not found in Intune and thus pending until Microsoft adds them.

Microsoft's active blog site of "Known Intune Issues" is continually updated with the latest issues affecting the Intune infrastructure and clients (Helenclu and dsindona88, 2022 March 18). Once an issue has been resolved, it will be removed from this page. It is critical to review this page on a continual basis to become aware of any current problems that might affect this project

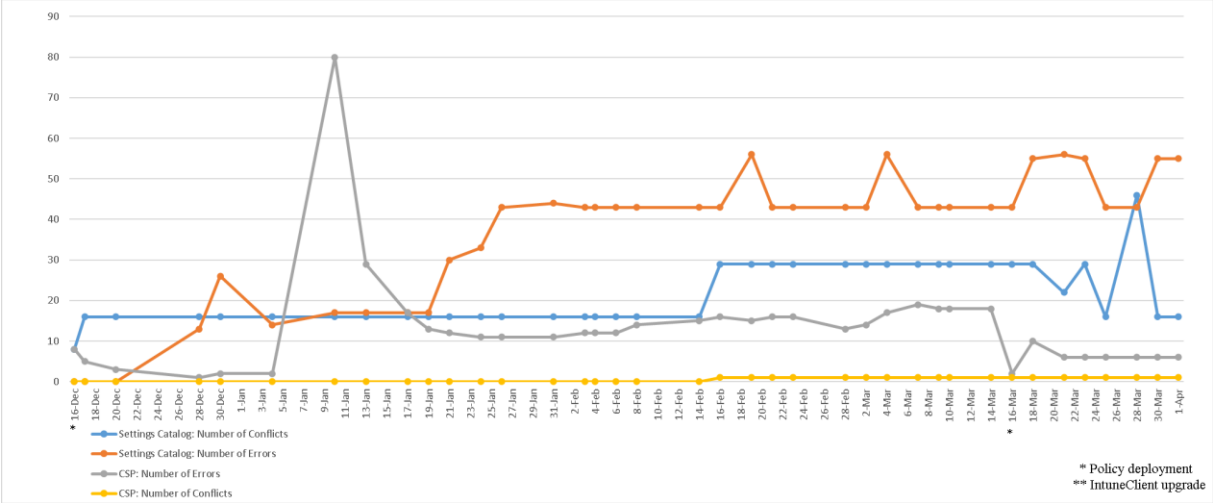
Policy sets deployed via Intune are represented by 19 CSPs and 46 Setting Catalogs. As machines consumed policy, they send telemetry to Intune regarding:

- Conflict – Two policies with different settings are applied to the same machine
- Error – The machine is not able to correctly apply the policy
- Not Applicable – This policy doesn't apply to this machine

This data is then aggregated into Intune reports as shown in Figure 2. This data was then exported and combined to form a single data point per day to indicate the number of machines exhibiting such behavior.

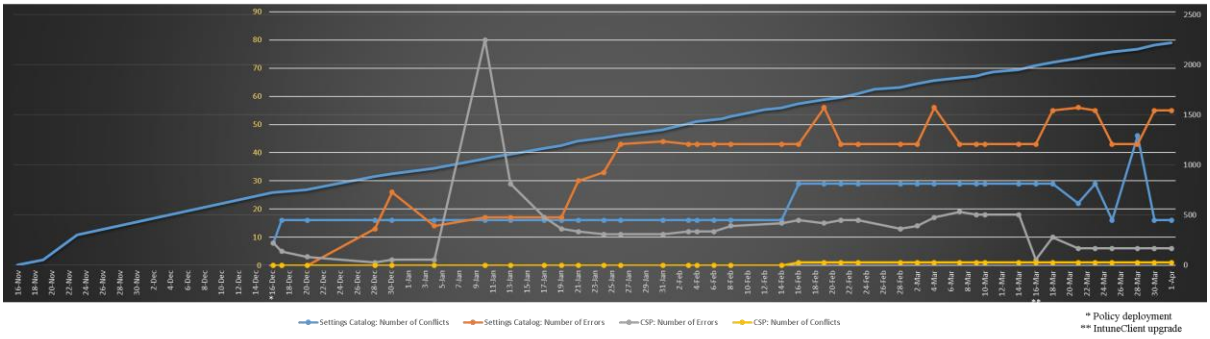
Errors

Figure 2: Settings Catalog and CSP Errors Over Time



Each Settings Catalog and CSP error were investigated to understand the source of the error and why it appeared on the machine. Figure 2 illustrates the Microsoft policy telemetry returned from the machine. Each error was reviewed to determine if machines exhibited an error for the same setting, if the setting was applied to the machine, and if the machine had any other issues that would have caused the error to occur. Overlaying the number of errors over the population sample, as seen in Figure 3, shows the number of errors remained stable as the population increased, negating the Microsoft error exhibited on January 4th and recently anomaly on January 19th.

Figure 3: Sample population with errors overlayed



Behavior Anomalies

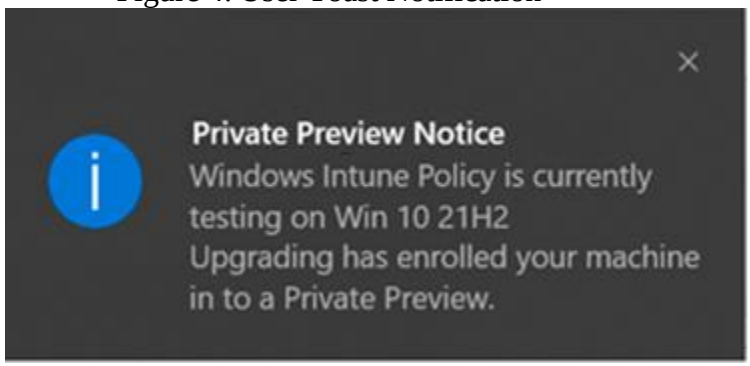
Polices were tested in a lab environment prior to the push to the private preview machines. During one such push of settings, it was observed that machines in the pilot group behaved erratically. Machines would not allow the login prompt to appear, if such an attempt was possible, the machine would engage the screensaver after three seconds of inactivity. One machine was fraught with a 100% CPU utilization making it very difficult to troubleshoot. After one day the machine began to crash and reboot every hour, while other machines continued to have the screensaver issue. This test machine was reimaged while the investigation of the screensaver continued on other pilot machines.

All policies were removed from the lab to stabilize them and to investigate the issue. One by one, the policy was added back to pilot machines; it was monitored for one hour, forcing Intune policy refresh, rebooting, and login/logoff actions. As each policy passed, a new policy was added until the offending policy was determined. The problem was traced to a Settings Catalog policy. Microsoft moves policies from CSP to Settings Catalog at irregular intervals, inferring the stability of the policy. Reverting this setting to the original CSP revealed a proved a successful policy deployment and stable pilot group. This issue was reported to Microsoft which in turn responded that other companies were experiencing the same issue and that reverting to the CSP will resolve the issue until Microsoft can fix the root cause. Deploying such a broken policy to a production environment would have caused disastrous results.

Qualitative results

Zero Tickets were generated for Windows 10 21H2 issues. Global Service Desk (GSD) and Onsite IT Administrators reported no issues or queries from users other than the PowerShell Toast notification as shown in Figure 4.

Figure 4: User Toast Notification



Discussions with several random users indicated they were not aware of the change on their machine. A companywide Yammer post regarding this project for which the users were directed to read had been overlooked. While telemetry noted errors or conflicts on machines, users were both unaware and unaffected by the Intune Policy. As more users adopted Windows 10 21H2, they discussed the features and Operating System with colleagues triggering other enrollments into the private preview.

Due to the various policy settings and behaviors, all policies should continue to move through a controlled process to prevent any issues resulting in non-productive time and impacting the business process of the company.

The data collection, monitoring, and troubleshooting will continue until the conclusion of this project. The production environment will require continual monitoring to ensure proper application of the Intune Policy.

D. *Risk Management Process*

Risks have been identified and assessed as to the nature and degree to which the impact will occur. The risk level is determined by multiplying the Likelihood and Severity based on the perceived level of risk. Utilizing a Risk Register and mitigation plan, potential severity will be lowered. See details in Appendix A.

4. Return on Investment

Cost Recovery

Before a company can remove a domain controller, user groups, user accounts, group policies, and authentication methods must first be migrated. When Group Policy is migrated to Intune it does not necessarily negate the need for Domain Controller decommissioning. Through natural progression, this server infrastructure is removed in favor of a modern approach once all the previous needs are transferred.

The company's Domain Controllers infrastructure grows and shrinks as the company expands and contracts. This infrastructure is located in data centers across the world, with costs varying according to the location, employee pay scale, server age, depreciation costs, local exchange rates, and warranty life. Datacenter contracts can vary per quarter, machine, and year. Data below, Table 1, is a representation of the sample environment as an aggregate across the management plane.

Table 1: Cost of Ownership

Company investment	Unit per month	Cost of Ownership	Cost Per machine/month
Data Center Hosting	1 Month @ 90 DCs	$25,000	$277.78
Engineering maintenance	$60 per hour @ 10 hours	$600	$6.67
Total			**$284.45**

As a domain controller is no longer necessary the cost of ownership will drop on-premise at a rate of $284.45 per machine per month with an offset occurring with Cloud data egress. The need for the Domain Controller after the policy is moved will continue until other enterprise needs are transferred. The beginning of this process could be two years in the future.

Corporate Objectives

Cost recovery is considered secondary to the main objective of ubiquitous management of users, devices, and resources no matter the location of the device. Companies are determined to adopt a modern approach utilizing cloud technologies, and real-time reporting with graphical data that can be sliced as needed to deliver appropriate management-level reports.

1. Digital Transformation

Digital Transformation is a process by which a company utilizes technology to create new business opportunities within the business and within the marketplace. Consider Henry Ford's introduction of the mechanized assembly line or the introduction of the transistor and microchip. This does not need to be a disruptive technology. Cloud computing was developed as companies improved the distributed computing models of servers to support their businesses.

This company is embarking upon Digital Transformation is a corporate objective from the top down. As each segment, business line, or business group adopts the Digital Transformation model the company as a whole reaps the benefits. Migrating the management of devices from an on-prem technology to a Cloud-based technology allows the company to remain in contact with a device as long as there is an Internet connection.

2. Modern Workplace

The Modern Workplace is characterized by the ability to use the latest technology to manage devices and users in a manner that removes the traditional boundaries and inhibitors. The Modern Workplace is a small portion of the Digital Transformation movement. Active Directory administrators have zero feedback with regards to their machine settings, now they are able to determine conflicts, errors, or applicability from a Web-based reporting model. Through this endeavor, the company will provision, deliver, and manage the user devices no matter the connection method, location of the devices, or the virtual device type.

5. Recommendations and Conclusion

Through this project, the company has moved further into the Modern Workplace area. The Active Directory team has learned how to test and deploy Intune policy as well as how to convert the current GPO Settings to either the Settings Catalog or a CSP. Telemetry has proven the benefit of understanding the machine state and changes. Furthermore, there are recommendations that should be undertaken.

Silo Breakdown

Effective teams can improve functionality and streamline behavior due to close working relations developed over time. When working with other teams this trust has not yet been created and can be quickly eroded due to conflict. As a company moves to adopt more Digital Transformation initiatives, it will be necessary for teams to work together for the betterment of the company and for the projects held between them. For a single policy, the Active Directory must work with any number of policy owners, the Endpoint Security team, and the Desktop Engineering team. This company must promote an environment of collaboration between silos if they expect this progress to continue. Failure between teams will result in project complications, delays, and sabotage.

Modern Desktop

Management profiles, applications, software updates, and Operating System upgrades will be delivered from one or more solutions regardless of user job duties. This is the direction for adopting a Modern Desktop. To reach this level of action machines will have their policy managed via Microsoft Intune. These machines are also not limited to physical devices. Virtual devices housed in the cloud that match physical hardware with both performance and Operating System platforms allow the business to provide a solution no matter where or how the user is connected to the corporation. The company must continue to adopt Modern Desktop initiatives begun with this project. The next step to prove the viability of Intune Policy will be to deploy an Azure Active Directory machine with zero reliance on the corporate infrastructure.

Group Policy Analytics

The company must continue to utilize Group Policy Analytics (GPA) as Microsoft continues to improve the platform. The platform was introduced in late 2020 and moved to General Availability in early 2022. GPA is still in its infancy. Improvements will allow it and other companies, to correctly identify Group Policies that can move to the cloud. Given the limited number of Group Policy areas available within GPA, Microsoft needs to place more effort behind the project to create a smoother migration to the Cloud

Future updates should include the notification to the IT professional when a CSP is available in the Settings Catalog and assist with the moving of the policy between Device Configuration Profiles.

Continual Process

This company and other companies will need to adopt a continual process to review Group Policy to determine, first, if available in Intune, and second, the format, CSP, or Settings Catalog. Policies presented in CSP format should be reviewed quarterly to determine if they exist in the Settings Catalog. Perform a pilot and the migration from CSP to Settings Catalog.

The selected company is well prepared for a modern approach to systems management. This is simply one stage in a multi-stage effort. While this project focused on the Core Windows

10 policies the formulated method and process can be put forth for all remaining Windows 10 policies as well as Windows 11 policies. Policies that do not yet exist in Intune or are deprecated and will not be available in Intune must be reviewed by the stakeholders to correctly determine a course of action beneficial to the company and its objectives.

6. Reference

Adame, D. (2021 August), Managing and Securing Endpoints: A solution for a telework environment, M.S Thesis, *Information and Decision Sciences, Cal State University*. [Online]. Retrieved from https://scholarworks.lib.csusb.edu/etd/1316/ [Accessed: Oct 11, 2021]

Bolozdiņa, D., Pirta-Dreimane, R., & Romānovs, A. (2020). Cloud Strategy Development for Medium and Small Business. *Information Technology & Management Science (RTU Publishing House)*, Vol. 23, pp. 45-54

Bradbury, D. (2002 September 12), Feeling the cosmic pull of active Directory, *ComputerWeekly.com*. [Online]. Retrieved from https://www.computerweekly.com/feature/Feeling-the-cosmic-pull-of-Active-Directory.[Accessed: Oct 12, 2021]

Burrows, P. (2021), *VPN vs Cloud: The Case for Sunsetting the VPN | Endpoint, Tanium Endpoint*. [Online]. Retrieved from: https://endpoint.tanium.com/vpn-vs-cloud-the-case-for-sunsetting-the-vpn/.[Accessed Oct 10, 2021]

Choudhury, P. R., Foroughi, C., & Larson, B. (2021 April) "Work-from-anywhere: The Productivity Effects of Geographic Flexibility," *Strategic Management Journal*, Vol. 42, No. 4, pp. 655–683. [Online]. Available: DOI: 10.1002/smj.3251

Constantin, L. (2020). Attackers can use Group Policy flaw to take over enterprise Windows systems. *ARNNET*. [Online]. Retrieved from: https://www.arnnet.com.au/article/680404/attackers-can-use-group-policy-flaw-take-over-enterprise-windows-systems/ [Accessed: October 9, 2021]

Ekholm, J. (2021 June 2), IT-infrastructure Migration and Modernization, M.S. Thesis, *Information Technology, Metropolia University of Applied Sciences*. [Online] Available: https://www.theseus.fi/handle/10024/501538 [Accessed: Oct 12, 2021]

Finnegan, M. and Marian, L. (2021 Aug 23), Microsoft Endpoint manager: What Intune's successor does and how it works, *Computerworld*. [Online]. Retrieved from https://www.computerworld.com/article/3304583/27icrosoft-endpoint-manager-what-intunes-successor-does-how-it-works.html. [Accessed: Oct 13, 2021]

Grillenmeir, G. (2021 July), Now's the time to rethink Active Directory security, *Semperis*. [Online]. Retrieved from https://securityboulevard.com/2021/08/nows-the-time-to-rethink-active-directory-security/ [Accessed: Oct 12, 2021]

Helenclu and dsindona88 (2022 March 18), Known Intune issues, *Microsoft Docs*. [Online]. Retrieved from https://docs.microsoft.com/en-us/troubleshoot/mem/intune/known-issues. [Accessed February 5, 2022]

Jain, M. (2020 Mar 31), Manage work devices at home during Covid-19 using Configuration Manager, *Techcommunity.microsoft.com*. [Online]. Retrieved from https://techcommunity.microsoft.com/t5/27icrosoft-endpoint-manager-blog/manage-

work-devices-at-home-during-covid-19-using-configuration/ba-p/1262052. [Accessed October 12, 2021].

Morgan, C. (2000, January), Active directory: For now, try to live without it, *Computerworld.* [Online]. Retrieved from https://www.computerworld.com/article/2594125/active-directory—for-now—try-to-live-without-it.html. [Accessed: Oct 12, 2021]

Näsi, A. (2020 October), Microsoft Intune mobiilihallin-nan ymmärtäminen ja käyttöön-otto, [Understanding and deploying Microsoft Intune mobile management], M.S. Thesis, *Data Processing Information Networks*, *Tampere University of Applied Sciences.* [Online]. Retrieved from https://www.theseus.fi/bitstream/handle/10024/353112/Nasi_Axel.pdf [Accessed Oct 13, 2021]

Parker, K., Horowitz, J. M., & Minkin, R. (2020). How the coronavirus outbreak has—and hasn't—changed the way Americans work, *Pew Research Center*. [Online]. Retrieved from https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasn't-changed-the-way-americans-work/. [Accessed: Oct 12, 2021].

Wallent, M. (2021 August 31), Microsoft a leader in 2021 Gartner® Magic Quadrant™ for unified endpoint management tools, *Microsoft Security Blog*. [Online]. Retrieved from https://www.microsoft.com/security/blog/2021/08/31/28icrosoft-a-leader-in-2021-gartner-magic-quadrant-for-unified-endpoint-management-tools/. [Accessed: Oct 12, 2021]

Appendix A. Risk Register

Hazard Analysis and Risk Control Record

Doc ref:		**Task/Process Assessed:**	Group Policy to Intune Migration
Revision:	Version 1.001	**Location:**	College Station, TX
Date:	November 19, 2021 0659	**Assessment Team:**	Desktop Engineering
Operation:	Tesing of Intune management	**Final Approved by:**	Dave Petty

	HAZARD		POTENTIAL RISK			CONTROL MEASURES		RESIDUAL RISK		
Activity Steps	**Hazard Description and Worst Case Consequences with no Prevention or Mitigation Measures in Place**	**Loss Category/ Population Affected**	**Likelihood**	**Severity**	**Risk Level**	**List all Current and Planned Control Measures, taking into Account all Contributing and Escalating Factors** **Current and Planned Prevention Measures to reduce Likelihood**	**Current and Planned Mitigation Measures to reduce Severity**	**Likelihood**	**Severity**	**Risk Level**
Personnel										
Employee doesn't wish to be in the Private Preview (PP)	User must submit a Ticket to GSD then to SysMgmt-L3 for review	Validity	VL (1)	L (-1)	**I (-1)**	Company wide, IT, Desktop Services Yammer post and email notification to Geo IT mangers	N/A	VL (1)	L (-1)	**I (-1)**
Team fails to review /migrate policy (Desktop Engineering, Security, Active Directory)	Project falls behind, deadline not met, the business doesn't move to Intune policy in an appropriate amount of time	Productivity, Team Image	M (3)	M (-3)	**M (-9)**	Weekly meetings to discuss poilicy move progress	Provide continue training and contact with team. Assist in moving policy as a training method	L (2)	L (-2)	**L (-4)**
Employees critical to the success are moved to a new postion	Corporate knolwedge is lost, project will not move forward at current pace	Productivity	M (3)	C (-4)	**H (-12)**	Team members should, if known, inform about potential promotions	N/A	L (2)	S (-2)	**L (-4)**

Policy										
Policy conflict with other Intune Policy	Machine fails to apply security or useability policy to the machine	Productivity	L (2)	M (-3)	**M (-6)**	Review policy policy before adding setting	Push policy to test group prior to the larger population	VL (1)	L (-1)	**I (-1)**
Not in Intune	Required security policy is not applied to machines	Objective / Company Wide	H (4)	M (-3)	**H (-12)**	Any policy now found in Intune will be moved to the end of the project. Microsoft adds policies each month	Use PowerShell script from Intune to deploy the Registry settings.	M (3)	S (-2)	**M (-6)**
Intune Policy setting is different from orignal GPO	Machine will have a differnet behavior than the original policy	Productivty / Company Wide	L (2)	M (-3)	**M (-6)**	Understand the change and how it will affect the company.	Review with the policy owner to undertand how /if the change will affect the machine/user	VL (1)	S (-2)	**L (-2)**
Business Operations										
Critical business machine is inadvertently added to the PP group	Business operation could be impacted. Procedure on an rig is interrupted	Profit / Company wide	L (2)	C (-4)	**M (-8)**	GeoIT Unit managers inform usres of potention impact of upgrading. Periodic review of machines	Add popup to machines notifying users that their machine is in a Priviate Preview	VL (1)	S (-2)	**L (-2)**
Machine behavior adversely affected.	Machine is not in a stable state.	Productivty / Company Wide	L (2)	C (-4)	**M (-6)**	Testing policies will stay in pilot for 2 weeks before moving to Private Preview	Review machines to determine if policy is at fault and remove it from Production	L (2)	S (-2)	**L (-4)**

Legend	
Risk Level	I - Insignificant, L - Low ,M - Medium,H - High,E - Extreme
Likelihood	VL - Very Low ,L - Low ,M - Medium,H - High,VH - Very High
Severity	L - Light,S - Serious,M - Major,C - Catastrophic,MC - Multi Catastrophic

		SEVERITY	Very Low	Low	Medium	High	Very High
			1	2	3	4	5
			LIKELIHOOD →				
Light	-1		-1	-2	-3	-4	-5
Serious	-2		-2	-4	-6	-8	-10
Major	-3		-3	-6	-9	-12	-15
Catastrophic	-4		-4	-8	-12	-16	-20
Multi-Catastrophic	-5	↓	-5	-10	-15	-20	-25