Global Information Assurance Certification Paper

Fight or Flight: Moving Small and Medium Businesses into the Cloud During a Major Incident

GIAC (GCIH) Gold Certification

Author: Drew Hjelm, drew@vets.io
Advisor: *Clay Risenhoover*

Accepted: August 30, 2020

Abstract

Incident responders often aid small and medium businesses (SMB) during crippling cyberattacks that cause outages of critical systems. Most SMBs lack sufficient capacity to monitor and protect their on-premises IT infrastructure. Many of these SMBs are already using cloud platforms in a limited fashion. These organizations can use more cloud services to improve security visibility against future attacks and possibly speed up recovery time. This research examines the feasibility thereof and discusses the challenges that organizations may face with rapid cloud migration, including software compatibility and insurance requirements.

1. Introduction

Major cyber incidents compel large businesses and other entities to make massive investments in information security and change their organizations' security posture. For example, Target spent hundreds of millions of dollars on staffing and building a "cyber fusion center" for securing its stores after threat actors stole its data on 42 million customers in 2013 (Krebs, 2015). However, smaller organizations might not be able to make comparable changes as their larger retail counterparts. Ransomware impacts small and medium businesses (SMBs) disproportionately, with more than 70% of reported ransomware incidents affecting businesses under the $250 million revenue bracket (Aon, 2020). Many SMBs have already partially adopted cloud infrastructure. If SMBs adopted cloud-based services more fully, they might decrease the risk and severity of incidents like ransomware. This research examines whether incident responders can use cloud-based services to assist SMBs in recovering business operations more quickly. It also discusses the challenges organizations may face with rapid cloud migration, including software compatibility and insurance requirements.

2. Current State of SMB Networks and Incident Response

To discuss the viability of migrating SMBs to the cloud during a significant cyber incident like a ransomware attack, it is essential to understand the typical arrangement of SMB information technology architecture and the challenges presented by responding to a cyber incident in an organization.

2.1. The State of SMB Networks and Cloud Adoption

SMBs represent a large percentage of businesses in the United States and have small networks and staff who may be unable to respond to security incidents. According to the US Small Business Administration (SBA), SMBs with fewer than 500 employees constituted more than 99% of businesses in the United States, employing 47.5% of

employees in 2015 (SBA, 2018). The SBA (2018) found that there were 5.8 million businesses with fewer than 500 employees and 5.2 million businesses with 20 or fewer employees. A Spiceworks (2019) survey found that 62% of businesses with fewer than 100 employees did not have an IT security expert on staff. This lack of experience among many businesses represents an enormous vulnerability for a significant portion of businesses in the United States.

Meanwhile, most small data centers in small businesses in the United States had very few servers. Ganeshalingam, Shehabi, and Desroches (2017) found that among buildings with small data centers (server rooms and server closets with fewer than 25 servers), approximately 70% had only one server in the data center. They further note that these "represent a use case where operators need just one server for file sharing across an office or for email or web hosting" (Ganeshalingam, Shehabi, and Desroches, 2017). This research adds to earlier estimates showing that small businesses with 49 or fewer employees require one or fewer servers (Applied Computer Research, 2011). While SMBs typically have few servers in their data centers, they are still using other computing services.

2.2. Cloud Services and Adoption

Microsoft and Google are two major cloud service productivity software providers used by businesses. The Microsoft 365 Suite (formerly called "Office 365") includes hosted email, desktop and web productivity applications, endpoint security, identity management, and endpoint management features. Google Apps Suite also includes hosted email, web productivity applications, identity management, and endpoint management features. Microsoft and Google provide connections for on-premises infrastructure to synchronize identities to cloud platforms, allowing for hybrid cloud approaches. Microsoft offers Azure Active Directory (AD) Connect to allow organizations to replicate users and devices between on-premises Active Directory Domain Controllers and Microsoft Azure Active Directory (AAD). Users can log in to Microsoft 365 with the same credentials they use to log in to their endpoints. Google offers Google Cloud Directory Sync, which provides a similar function. Many

organizations are using these technologies for their hybrid clouds to connect on-premises identity management servers with cloud-based email.

A significant number of SMBs are using cloud-based offerings to handle various IT services for their organizations. Enlyft, a marketing data firm, found that 64% of the 1.2 million companies using Microsoft 365 have 50 or fewer employees (Enlyft, 2020b). In comparison, 72% of the 1.4 million companies using Google Apps Suite have 50 or fewer employees (Enlyft, 2020a). A Spiceworks (2020) survey conducted in 2019 found that 54% of organizations surveyed are solely using cloud services to manage their email, while only 5% of those organizations are using cloud identity management. 57% of organizations surveyed by Spiceworks are using on-premises identity management. Since it is possible to have a hybrid cloud adoption model, this explains why on-premises solutions and cloud solutions have different adoption rates.

2.3. On-Premises Servers Represent Vulnerability for SMB

Ransomware continues to be a significant problem disproportionately affecting SMBs, likely because of downtime caused by the incidents, lack of information security capacity, and smaller, less-sophisticated networks. In 2017, security software vendor Malwarebytes published a survey of SMBs finding that 1 in 6 ransomware incidents led to downtimes of greater than 25 hours (Malwarebytes, 2017). Aon, an insurance reseller, found that "72.4% of reported ransomware infections targeted businesses with revenues under $250 million" (Aon, 2020). Beazley, a cyber insurance underwriter, found, based on insurance claims, that the Remote Desktop Protocol is a primary method for threat actors to gain access to companies to deploy ransomware (Beazley, 2020). As discussed earlier, SMBs are more vulnerable to ransomware and other cyberattacks since they might host smaller data centers containing a single server serving all the organization's functions.

During many ransomware incidents, ransomware operators regularly move from workstation endpoints to DCs. These hosts are central for investigations and frequently require the most time to clean before allowing other endpoints to utilize services on those servers. For example, the Microsoft Threat Protection Intelligence Team (2020)

documented how the Ryuk ransomware family operators commonly deploy their malware from DC servers. Similarly, Gatlan (2020) reported that the REvil (sometimes called Sodinokibi) ransomware operators use DCs in retail point-of-sale attacks. Utilizing these vulnerable on-premises servers (whether targeted from other compromised endpoints or through exposed RDP) ultimately represents a potential single point of failure and a hindrance to restoring business operations during a catastrophic cyber incident like ransomware.

Cloud platforms can provide significant monitoring and visibility improvements over on-premises servers. On-premises servers rotate logs frequently and may not be available during incidents if the organization has not configured centralized logging storage and retention. Azure AD logs, on the other hand, are retained for 30 days by default (Microsoft, 2020d), while Google Apps Suite retains logs for six months (Google, 2020). While sometimes on-premises servers may retain logs longer than cloud services, the on-premises logs can be deleted or wiped by threat actors deploying ransomware to hide their activities.

2.4. Cyber Insurance Considerations for Restoration

Organizations that face cyber incidents and have a cyber insurance policy may find that the policy does not cover losses or improvements to their infrastructure that are necessary for protection against future attacks. The Organization for Economic Co-operation and Development (OECD) reported that cyber insurance policies might not cover reputational losses or intellectual property losses (OECD, 2017). Dan Burke, writing for insurance carrier Woodruff Sawyer, stated that cyber insurance policies might not cover "the cost to improve internal technology systems, including any software or security upgrades after a cyber event" (Burke, 2019). In many cases, insurance will cover the remediation of the root causes of security incidents. Even with the root cause of the incident remediated, many SMBs still have inadequate access to expertise to secure on-premises servers. This can leave SMBs vulnerable to a future ransomware attack affecting the same infrastructure.

2.5. Considerations for Incident Restoration

After a significant ransomware incident, a victim organization may be able to restore their environment from backups; however, restoring from backups involves assuring they are viable and clean from malware or other persistence mechanisms. A frequent objective for threat actors deploying malware is to ensure that victims cannot restore their environment from backups to a state before the ransomware, which would likely deprive the threat actor of payment. Threat actors may delete backups, encrypt backups, or otherwise make the underlying storage unavailable by destroying RAID. Testing backups is a critical consideration for organizations attempting to restore from backups.

Even if backups are viable, the organization will need to ensure the backups are clean of malware or other forms of persistence the threat actor may have deployed to ensure they can get back into the organization. The backup software may have backed up the environment after a threat actor already deployed tools into the environment, meaning the environment could have a risk of reinfection after restoration.

Forensic efforts may also slow restoration to determine the extent of data compromise. Various compliance standards such as HIPAA and PCI-DSS require victim organizations to determine the extent to which a threat actor viewed, accessed, or exfiltrated data. Restoring from backups may destroy forensic data showing threat actor activity, which would leave legal questions unanswered. Using tools like FTK Imager, dd, or other imaging solutions can add hours to the restoration process for organizations by introducing lag time between finding an infection and restoring a server or endpoint from backups. Perry (2017) also found that the speed of copying large virtual disks can be limited by hardware and networks in virtualized environments.

With these considerations in mind, many SMBs relying upon a single server crippled by a ransomware attack or other cyber incident may be unable to resume business operations during evidence collection and restoration. Suppose the organization has a single internal server functioning as Domain Controller, DNS server, and file server (commonly found in small businesses). In that case, cleaned endpoints may be unable to

connect to essential services hosted externally if the DC server is not operational. Incident responders must balance collecting forensic evidence and ensuring the safe restoration of the network against resuming business operations as quickly as is reasonable, given the state of the environment.

3. Experimentation: Cloud Migration

The exercise in this paper will compare how quickly an incident responder can restore an SMB environment to an on-premises infrastructure versus a restoration to the cloud during an incident. The goal is to determine whether an SMB could resume operations faster by performing cloud migration instead of continuing to use on-premises infrastructure.

3.1. Lab Setup

To compare restoring a small business to traditional on-premises infrastructure against restoring to the cloud, the researcher created a virtualized test environment. The test environment is meant to be representative of small businesses regularly encountered by incident responders. The environment included a Windows 2012 R2 server containing the Active Directory Domain Controller, DNS, and File Server roles (collectively the DC server, or DC). The researcher constructed a domain, cloudmovers.biz, and built a Microsoft 365 Business Premium environment for the organization. The DC server also synchronized the organization's users to Microsoft 365 using the Azure AD Connect software Microsoft provides. The organization had ten Windows 10 endpoints and ten users. A pfSense firewall controlled central networking functions (DHCP, switching) for the organization.

The researcher also performed additional hardening steps for the Microsoft 365 environment. The researcher enabled multifactor authentication for all users and disabled legacy authentication (POP3/IMAP) for the users.

3.2. Control Scenario: Restore from Backup

The main scenario emulated in the research is a ransomware incident that encrypted the Domain Controller and several endpoints. In many circumstances, a small organization may be able to restore its server and endpoints from backups, assuming the threat actor did not delete or encrypt the backups while deploying ransomware. Ransomware or malware was not deployed in the environment, but instead the researcher simulated ransomware recovery operations.

Windows Server Backup (WSB) was used to back up and restore the lab environment in an idealized fashion. In this environment, WSB saved backups to an online disk attached to the DC of both the OS disk and the disk containing the organization's file share. When the outage was simulated, the DC was booted into the Windows Recovery Mode and restored the DC from saved backup. Restoring the server and its file share from the backup took approximately ten minutes for this small environment.

In practice, a ten-minute restoration of a DC after a significant ransomware incident is not likely. Depending on the incident response tools, the time to collect forensic evidence for determining the state of the DC will vary. Collecting triage evidence on a server, such as a DC, using tools like Brimor Live Evidence Collector or Kroll Artifact Parser and Extractor (KAPE) can take between 10 minutes and 30 minutes depending on the artifacts collected. The triage package and virtual disks may take several minutes or hours to transfer for analysis, depending on the location of the endpoint. Examining the triage package for evidence of persistent malware and root compromise can take several hours. Preparing the DC server to return to production in a secure fashion will take much longer than just the time it takes to restore the server from backups.

3.3. Experiment 1: Restore Domain from Scratch

If an organization cannot restore from backups, it may instead try to rebuild the environment using installation media. Rebuilding would require reinstalling the server

operating system, installing Windows updates, promoting the server to Domain Controller, re-creating user objects, and installing any required software. The researcher did not perform a complete rebuild during this project; however, the environment's initial build was used as a proxy for the rebuild. The researcher built the environment starting with a base Windows 2012 R2 image, installed upgrades, created the domain and ten virtual endpoints, and performed Active Directory synchronization with Microsoft 365 in three hours.

3.4. Experiment 2: Restore Company to Cloud

As an alternative to restoring from backups or reinstalling the environment from base images, the researcher also tried to restore the compromised organization by migrating operations to the cloud. Since the test organization adopted Microsoft 365, the researcher started work to migrate the management of endpoints from on-premises Active Directory to Azure Active Directory. A Cloud Migration checklist can be found in the Appendix: Azure AD Cloud Migration Checklist (Microsoft 365).

3.4.1. Microsoft 365 and Azure Active Directory Preparation

There were several steps involved with migrating the organization to Azure Active Directory. First, the researcher disabled Azure AD Connect synchronization from Azure Active Directory using Microsoft PowerShell because there will no longer be an on-premises AD server to synchronize:

```
Install-Module MSOnline
Connect-MSOLService
Set-MsolDirSyncEnabled -EnableDirSync $false
```

After disabling Azure synchronization, the next step was to enable user password resets and force a password reset across the organization using Azure Active Directory console shown in Figure 1.

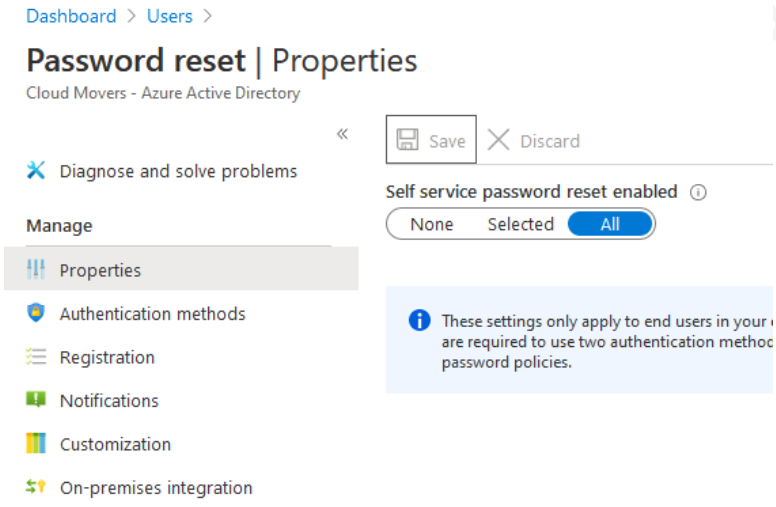

Figure 1: Self-Service Password Reset Options

After enabling password resets, the researcher confirmed that all users enabled multifactor authentication in Azure Active Directory.

The researcher also confirmed that Microsoft 365 was capturing audit logs for all activities, shown in Figure 2. Microsoft does not enable this feature by default for all organizations at the time of this writing. After enabling these logs, organizations may not see them in this console for up to 24 hours.

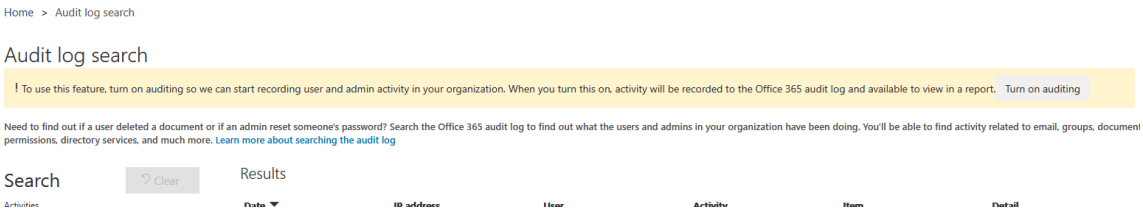

Figure 2: Enabling Audit Logs

There are several ways to join endpoints to Azure Active Directory. However, most do not apply to existing endpoints in-use during incident recovery. System administrators can join endpoints to AAD during the initial configuration. If an endpoint is already in use, the system administrator will need to use ADConnect to Hybrid Join the endpoint with both AAD and on-premises AD or disjoin the endpoint from a domain and then manually join the endpoint to AAD. In an incident where the DC is offline and will be removed (such as the scenario in this research), the only feasible option is to disjoin an endpoint from the domain, move to a workgroup, and then rejoin the endpoint to AAD.

Drew Hjelm

The first change to make for the cloud migration is to ensure networking no longer depends on the on-premises DC and DNS server. In the lab, the pfSense firewall assigned DHCP settings, including the DNS resolver address. To remove the DC, the researcher changed the DHCP setting for DNS to use the pfSense as a local DNS resolver, which would forward DNS queries to the public DNS recursive resolver Quad9. In an environment where endpoints have static IP and DNS assignments, a system administrator may have to reconfigure each endpoint manually.

3.4.2. Joining Endpoints to Azure Active Directory

After ensuring the endpoints were no longer using the DC, the researcher then disjoined them from the domain. To remove the computer from the domain, the researcher logged in to the endpoint as a local administrator account and opened `sysdm.cpl` to change computer names and domain memberships. When changing to a workgroup, the workgroup name cannot be the same as the domain name because this can lead to three-hour reboot times (Microsoft, 2020b). Once the computer is a part of the workgroup, the researcher rebooted and logged back in as a local administrator.

Next, the researcher performed the AAD domain join. This wizard is in the Start Menu Settings, as shown in Figures 3, 4, and 5. The researcher used a Microsoft 365 account in the Azure AD Global Administrator role. In practice, when prompted for an email address, the system administrator can choose to join the endpoint to Azure Active Directory with an Azure AD Device Administrator account or use the Microsoft 365 credentials for the user who will primarily use the endpoint. The primary security consideration is that using the endpoint user's credentials to join the endpoint to AAD makes the user a local administrator. To prevent users from becoming local administrators on their endpoints, system administrators should use an Azure AD account with the Azure AD Device Administrator role assigned to join endpoints to AAD.

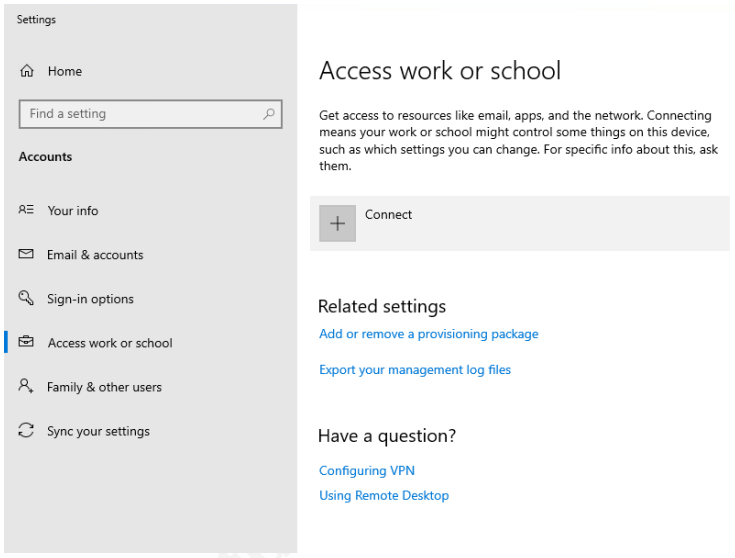

Figure 3:Access Work or School

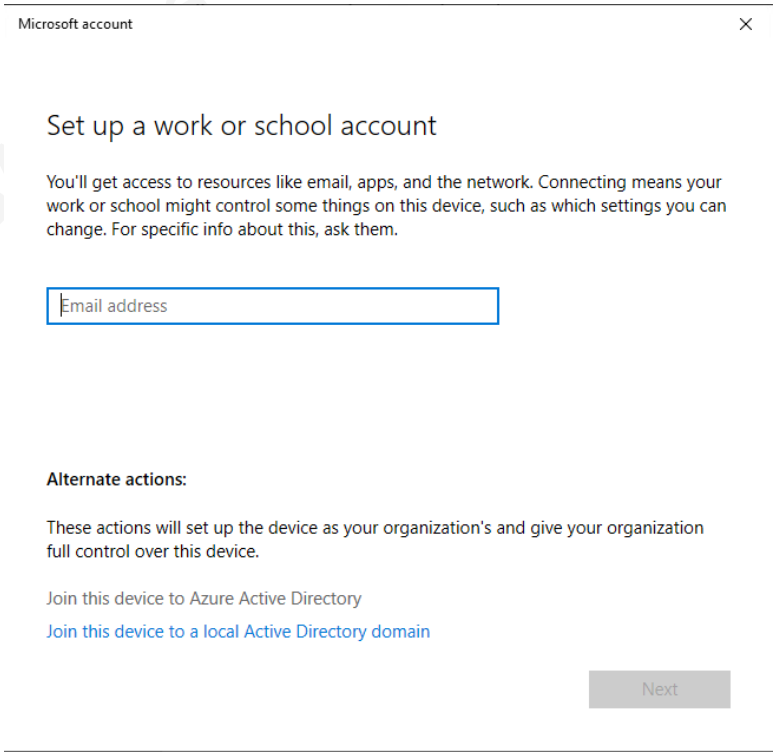

Figure 4: Join to Azure Active Directory

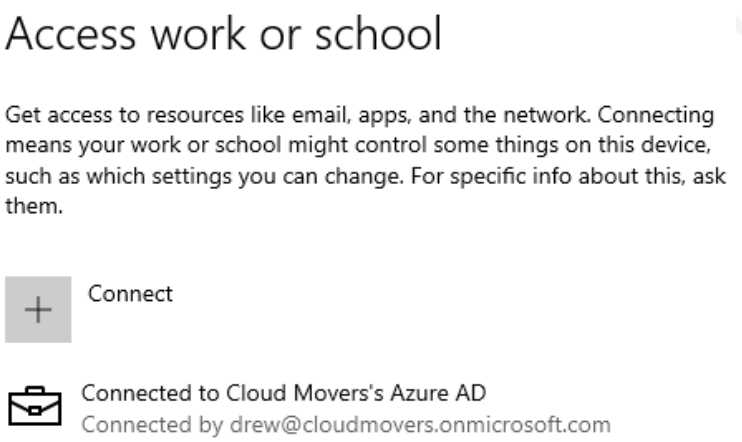

Figure 5: After AAD Join

After joining the endpoint to AAD, the researcher logged out of the local administrator account and logged in as a non-privileged user with Microsoft 365 account credentials (e.g., scott.lang@cloudmovers.biz). The Windows login workflow prompted for MFA credential (e.g., SMS code, One-Time Password, or Microsoft Authenticator App prompt) and then prompted to set a PIN for future logins.

In a real migration, the system administrator may need to assist the user with copying files manually after the user logs in to the endpoint with their Microsoft 365 credentials. There is no built-in method to migrate user profiles in Windows 10. The system administrator may need to copy files from the user's old home directory (e.g., C:\Users\scott.lang) to the user's new home directory (e.g., C:\Users\scott.lang.CLOUDMOVERS).

3.4.3. Migrating File Storage to SharePoint Online

The other major piece of migrating an organization to the cloud is ensuring its files are available for access. In Microsoft 365, this means uploading the file server to SharePoint Online. The researcher used the Microsoft SharePoint Migration Tool (SPMT) to move the lab organization's file server to SharePoint. ShareGate (2018), a publisher of a tool recommended by Microsoft to perform large and complex migrations, indicated that the SPMT is suitable for simple file migrations to SharePoint from file shares.

Organizations migrating to SharePoint during an incident should be ready to create a clean server or endpoint to perform the migration. The SPMT is a multi-threaded application that requires a significant amount of memory to operate efficiently. The organization may be able to use its existing hardware to create a server VM, or the incident responder may also be able to provide hardware for this purpose. An organization affected by malware should use a SharePoint migration server clean from malware and on a network segment isolated from other endpoints to prevent malware from spreading. Once the system administrator mounts the storage on the migration server, the migration can begin.

To prepare the file share for migration in the lab environment, the researcher created a new Server 2012 R2 virtual machine with 8 GB memory to perform the migration. In the lab environment, backups were restored from the file share to the new migration server. The SPMT is a straightforward wizard application that requires pointing at local storage, selecting a target, and inputting credentials. Once installed, the researcher selected “Start your first migration” and then "file share" when prompted (Figure 6), followed by the source location (Figure 7).

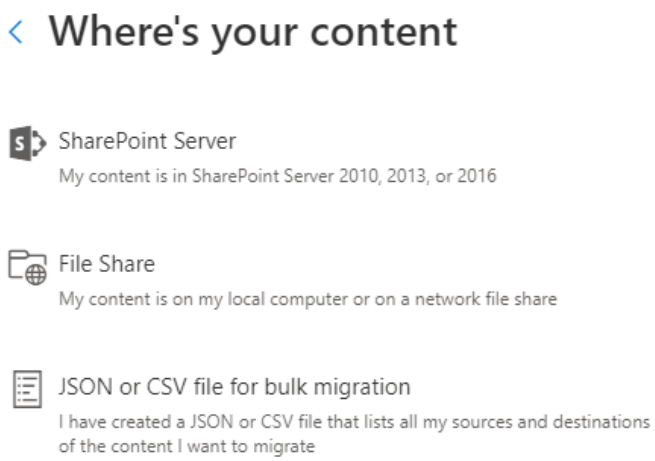

Figure 6: SPMT Content Selection

Figure 7: SPMT Source Selection

Next, the researcher selected to move the file share to a SharePoint site (Figure 8 and Figure 9). The application prompted Microsoft 365 credentials for the migration, and then the migration started. After completing the migration (Figure 10), all the lab files were accessible in SharePoint, as shown in Figure 11.

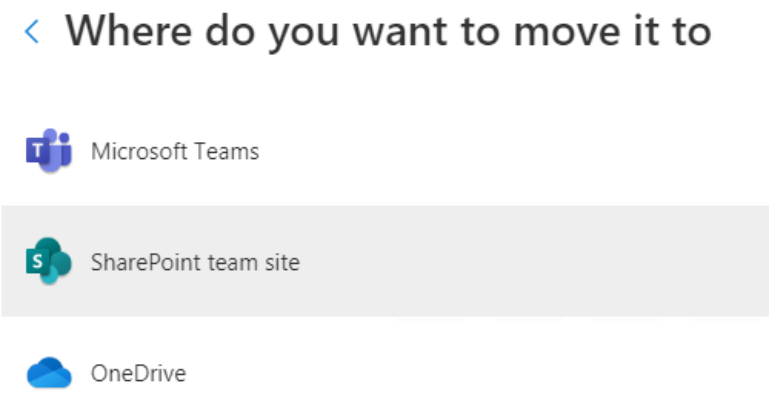

Figure 8: SharePoint Selection

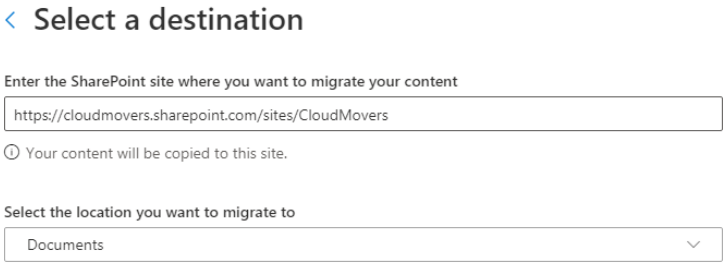

Figure 9: Target Destination

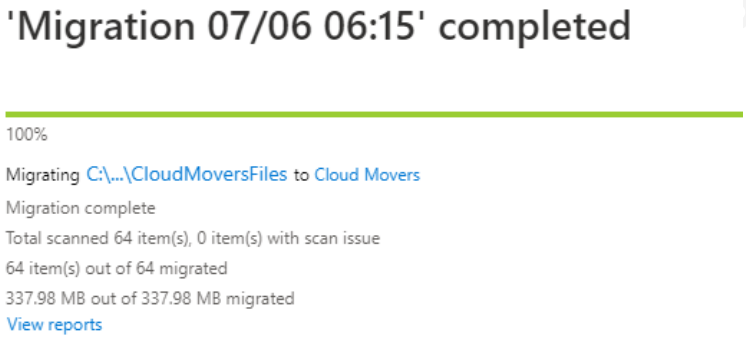

Figure 10: Migration complete

In a production environment, system administrators can manage access to folder permissions in Microsoft 365 to ensure that users without proper authentication can access files they need for their roles. Users on Windows 10 PCs can "sync" SharePoint folders to their local computers to make the transition from traditional file shares to SharePoint easier and edit documents in desktop applications.

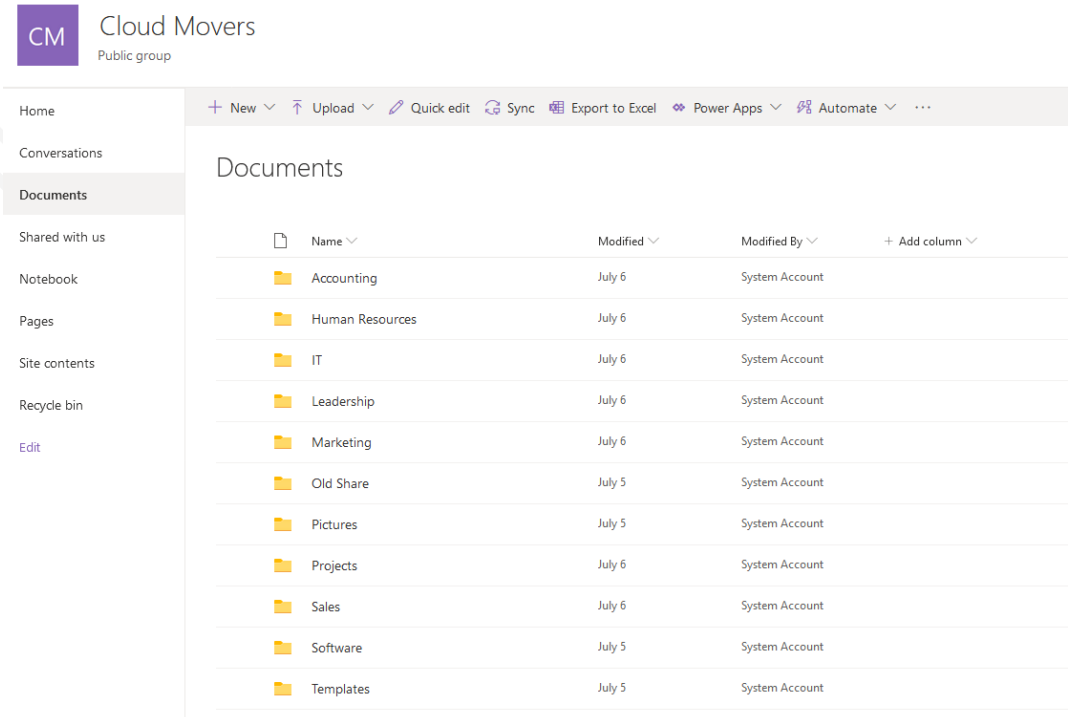

Figure 11: SharePoint with folders migrated

3.5. Cloud Migration Results

The researcher was able to disjoin an endpoint from the on-premises domain and rejoin to AAD in approximately five minutes. In practice, a user could be up and working more quickly than having to wait for internal servers to be available, assuming the endpoint is clear of malware and not subject to further investigation by the incident response team. An Endpoint Detection and Response agent that performs deep scanning and analyzes behavior may aid the incident response team in clearing an endpoint for use more quickly.

Migrating the lab file share to SharePoint only took a few minutes, but that was because it included a limited set of files. In practice, SMBs could likely upload their file shares from restored backups within several hours, depending on the size of the shares and the speed of their network. Speeds for uploading to SharePoint can depend on many factors, including local computing resources, network speed, and whether Microsoft is throttling an account. Isaac Stith (2016) reported uploads of up to one terabyte per day to SharePoint.

3.6. Comparison of Restoration Methods

The table in Figure 12 shows the results of the various restoration methods. For some activities, the researcher used estimates of times. For example, Perry (2017) found average VMware transfer speed over a network was 60-95 MB/s, compared to 400 MB/s for USB3. These speeds are equivalent to 480-760 Mb/s and 3200 Mb/s, respectively. Tools like EWFAcquire can write at 108 MiB/s (equivalent to 113 MB/s or 904 Mb/s) to USB3 drives. Using the SharePoint transfer estimate of 1 TB/day (Stith, 2016), the researcher estimated 6 hours to transfer 250 GB to SharePoint. The summarized results show the estimated restoration time when analyzing and reimaging all endpoints in an SMB network or a subset of 2 endpoints and the DC. The results do not include the lag time that may occur due to physically moving collection hardware between endpoints or other unforeseen work.

Method	All endpoints (hours)	Two endpoints and DC (hours)
Restore DC from Backup	121	33
Complete Rebuild	122	34
Migrate to AAD/M365	128	40

Figure 12: Estimated restoration times

The total estimated project time to restore SMB may be longer to migrate identity and device management to Microsoft 365 and Azure Active Directory for all tasks. However, removing the on-premises DC shortens the time to allow endpoints back on the network by removing the cleaning tasks related to the DC server from the critical path of incident recovery. Figure 13 shows the critical path of recovery requiring forensic imaging and analysis of the DC server before allowing endpoints back onto the network. Figure 14 shows the critical path of recovery dependent on recovering the endpoints themselves. By shortening the critical path to getting endpoints back onto the network and allowing end-users to perform their work, the cloud restoration method improves the recovery time of business operations instead of forcing users to wait for investigation and restoration of servers.

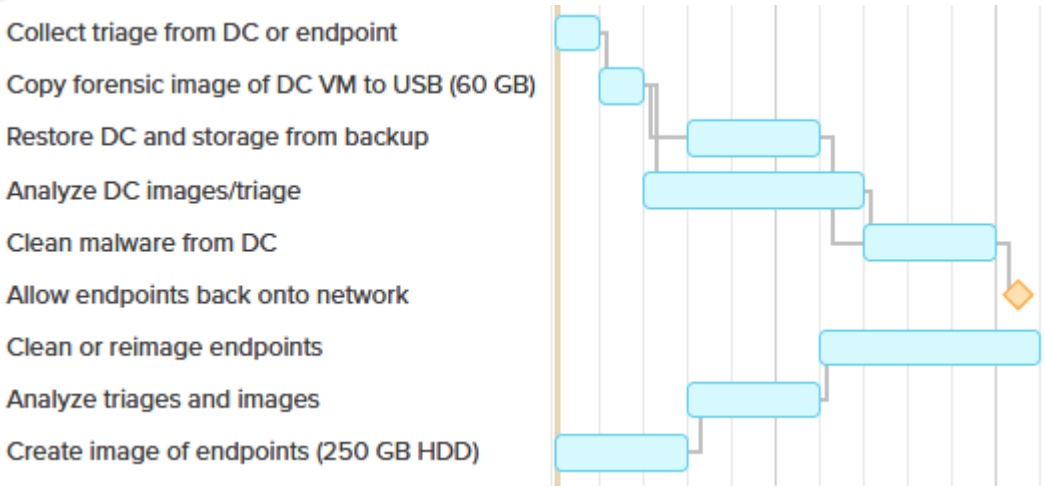

Figure 13: Restoring SMB with DC

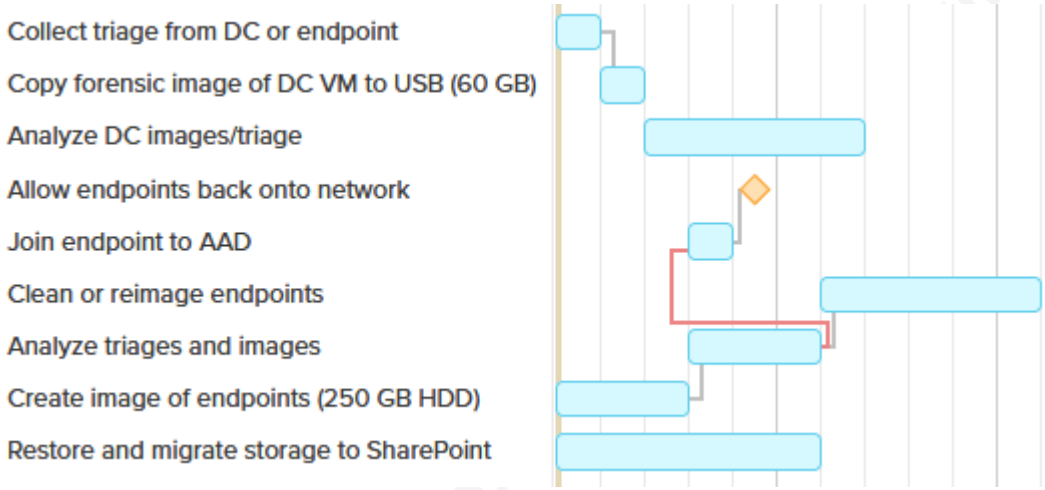

Figure 14: Restoring SMB to AAD/M365

4. Findings and Discussion

The experiment suggests that migrating endpoints from on-premises DC servers to AAD can reduce significant bottlenecks in restoring an SMB from a catastrophic outage like a ransomware incident. The single point of failure for many SMB networks is the server operating critical services like Active Directory, DNS, and file shares. Bypassing the server and restoring operations for end-users may improve the time required to resume business operations. However, there are other topics for these organizations to consider before moving straight to the cloud.

4.1. Difficulties Migrating Endpoints and Users to Cloud

Users may experience changes to workflows when migrating from on-premises file shares to the cloud, which may require further training during the incident. For example, users who were accustomed to accessing files on a file share may require assistance with navigating SharePoint to their files. SharePoint offers the ability to sync folders from the cloud storage to a local endpoint, which will have a similar user experience as the previously accessed file server.

Another challenge was migrating files from locally stored domain profiles to an Azure Active Directory profile. Since on-premises domains and Azure Active Directory are different, the profiles of users stored on devices are not compatible. When a user logs in with a Microsoft 365 account, they may no longer have access to their domain user profile and files. After disjoining from the domain, the endpoint sees domain user pepper.potts as different from the Microsoft 365 user pepper.potts@cloudmovers.biz since they have different security identifiers. In a situation where ransomware has not encrypted a user's endpoint, a system administrator may assist the user with moving files from their old location to a new location on the endpoint that can also synchronize to OneDrive cloud storage.

4.2. Difficulties Migrating Applications to Cloud

Organizations that depend on server-based applications may find migrating to the cloud during an incident especially challenging because the on-premises infrastructure they depend on is no longer available. If an organization is dependent on on-premises server software (such as an accounting program like QuickBooks), they may have to forego cloud migration. For some applications, there may be other methods to make the application act like a cloud-based application, such as QBox for QuickBooks. Some applications may have cloud-native counterparts that the organization can migrate. The organization can also look at using Azure Active Directory Domain Services to connect to Azure Virtual Machines running their applications. Future research should cover how to quickly migrate on-premises hosted applications to Azure Virtual Machines.

4.3. Difficulty with Understanding Cloud Services

Cloud-based identity management solutions like Google Apps and Microsoft 365 (Azure Active Directory) may be less familiar to stakeholders than their on-premises counterparts. System administrators have been managing endpoints and users with Microsoft Active Directory since Microsoft Windows 2000. They will have tools and practices that focus on managing Active Directory that they may not have for managing newer technologies. In contrast to the age of and familiarity with Active Directory,

Google announced its endpoint management feature in October 2019 (Google, 2019). Organizations adopting cloud device management should ensure they apply configurations to their devices that address the risk posed by the organization. Microsoft Intune provides security baselines to apply to endpoints enrolled in device management (Microsoft, 2020c). Similar capabilities exist with Google Fundamental Device Management.

5. Recommendations and Implications

5.1. Prepare Cloud Migrations Before Incidents

In many cases, an SMB may not experience significant issues with migrating to the cloud during an incident; however, making significant infrastructure changes during an incident can add stress to an already fraught time. SMBs already using some cloud-based services (such as Microsoft 365 or Google Apps) should work to move on-premises services to the cloud before a security incident occurs to prevent added organizational stress caused by change during the incident. Microsoft provides a Cloud Adoption Framework to help organizations plan a cloud migration if they have time to migrate, however, this research is focused on scenarios when organizations do not have much time to invest in planning their cloud migration. A checklist for SMBs to follow to migrate remaining on-premises services to Microsoft 365 is in the Appendix of this paper.

5.2. Cyber Insurance Should Cover Improvements

If an organization has experienced an incident due to a flaw in software that can be remediated without making significant changes, the organization should fix the vulnerability. However, if the organization has an on-premises infrastructure that it can remove to make the organization more secure in the long run by decreasing maintenance (e.g., patching and allowing RDP/VPN traffic inbound), the organization should consider making these changes. Cyber insurance carriers who do not cover this sort of migration

should reconsider their coverage guidelines to reduce business losses during a significant incident such as ransomware.

5.3. Other Security Considerations for Cloud

Microsoft 365 (Azure Active Directory and Intune) and Google Fundamental Device Management offer device management policies. Organizations should implement these policies based on risk to the organization, adherence to regulations and standards, and other best practices. These organizations should also be using Endpoint Detection and Response agents who are able to detect modern threats to the endpoint. Future research on the topic of migrating to the cloud could identify appropriate policies for organizations to implement while using these cloud management tools instead of traditional on-premises Active Directory.

Cloud platform logging capabilities may be more robust than on-premises infrastructure. However, organizations still need to ensure they are actively looking for cloud-based threats to their endpoints and users. Scot Berner, Senior Security Consultant with Trusted Sec, documented how attackers can abuse trust relationships between applications established with OAuth, a protocol heavily used by Microsoft 365 (Berner, 2020). Lee Kagan, Director of Adversarial Collaboration at Lares, documented additional AAD application abuse scenarios that may use OAuth and how to detect them (Kagan, 2020). Dirk-jan Mollema (2020b), Principal Security Expert at Fox-IT, documented how to exploit single-sign-on using Azure AD. More recently, Mollema (2020a) demonstrated a proof-of-concept for generating forged Microsoft 365 Primary Refresh Tokens (PRT) for AAD-joined devices using the Mimikatz credential-stealing tool. These cloud-based attacks require organizations using cloud services to monitor for threats such as:

- New OAuth application registrations, to ensure applications that users permit to access services on their behalf are legitimate (Kagan, 2020).
- Geographically improbable logins, such as when a user or device logs in to view documents from two or more locations too far from each other for the user to have traveled between them legitimately.

- Unusual user agents or application IDs, such as a user typically accessing services with a Chrome browser on Mac OS who then starts accessing services using PowerShell on Windows (Mollema, 2020b).

Ensuring organizations migrating to the cloud are taking advantage of all available logging and monitoring should be the top priority of those assisting these organizations. Future research could document best practices for logging and alerting on these types of cloud-based threats.

6. Conclusion

Small and medium businesses affected by significant cybersecurity incidents like ransomware should consider direct migration to the cloud of their remaining on-premises services if their on-premises infrastructure cannot be restored in a timely fashion to meet business operations goals. Cloud infrastructure can decrease risks from ransomware threats facing SMBs. Many organizations are already paying for Google or Microsoft cloud services that can replace on-premises infrastructure.

References

Aon. (2020, May). *Cyber insights for insurers*. https://thoughtleadership.aonbenfield.com//Documents/202005-cyber-insights-insurers.pdf

Applied Computer Research, Inc. (2011). *Identifying IT markets and market size by number of servers*. Mission Critical Magazine. https://www.missioncriticalmagazine.com/ext/resources/MC/Home/Files/PDFs/WP_ACR-IT-Server-Market.pdf

Beazley Insurance. (2020). *2020 breach briefing*. https://www.beazley.com/Documents/2020/beazley-breach-briefing-2020.pdf

Berner, S. (2020, May 13). Practical OAuth abuse for offensive operations – Part 1. *TrustedSec*. https://www.trustedsec.com/blog/practical-oauth-abuse-for-offensive-operations-part-1/

Burke, D. (2019, October 7). Cyber insurance 101: What cyber insurance covers, 2020. *Woodruff Sawyer*. https://woodruffsawyer.com/cyber-liability/cyber-101-insurance-coverage-2020/

Enlyft. (2020). *Companies using Google Apps*. Retrieved July 26, 2020, from https://enlyft.com/tech/products/google-apps

Enlyft. (2020). *Companies using Microsoft Office 365*. Retrieved July 26, 2020, from https://enlyft.com/tech/products/microsoft-office-365

Ganeshalingam, M., Shehabi, A., & Desroches, L. (2017). *Shining a light on small data centers in the US* (o. DE-AC02-05CH1131). US Department of Energy, Lawrence Berkeley National Laboratory. https://eta.lbl.gov/sites/default/files/publications/lbnl-2001025.pdf

Gatlan, S. (2020, June 23). REvil ransomware scans victim's network for point of sale systems. BleepingComputer. https://www.bleepingcomputer.com/news/security/revil-ransomware-scans-victims-network-for-point-of-sale-systems/

Google. (2020). *Data retention and lag times*. https://support.google.com/a/answer/7061566

Kagan, L. (2020, June). Malicious AzureAD application registrations. *Pwntario Team Blog*. https://blog.pwntario.com/team-posts/lees-posts/malicious-azuread-app-registrations

Krebs, B. (2015, September 21). Inside Target Corp., days after 2013 breach. Krebs on Security. https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Malwarebytes. (2017). *The state of ransomware among SMBs*. https://www.malwarebytes.com/pdf/infographics/Malwarebytes_The_State_Of_Ransomware_Among_SMBs.pdf

Microsoft Threat Protection Intelligence Team. (2020, March 5). *Human-operated ransomware attacks: A preventable disaster*. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Microsoft. (2020, July 21). *Azure active directory joined computers experience a three hours delay during boot*. Retrieved July 26, 2020, from https://support.microsoft.com/en-us/help/4565997/aad-joined-computers-experience-a-3-hour-delay-during-boot-if-the-work

Microsoft. (2020, July 17). *Use security baselines in Microsoft Intune - Azure*. Retrieved July 26, 2020, from https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

Drew Hjelm

Microsoft. (2020, March 24). *How long does Azure AD store reporting data?* Microsoft Docs. Retrieved August 3, 2020, from https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention

Mollema, D. [_dirkjan]. (2020, August 3). *Been a long day but thanks to @gentilkiwi 's awesome new Mimikatz CloudAP support we managed to put together tooling that can sign arbitrary PRT cookies!* [Tweet]. Twitter. https://twitter.com/_dirkjan/status/1290397176561119233

Mollema, D. (2020, July 21). Abusing Azure AD SSO with the primary refresh token. *dirkjanm.io*. https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/

Nagarajan, V., & Meador, B. (2019, October 29). Help secure your organization with new endpoint management, intelligent access controls. *Google Cloud Blog*. https://cloud.google.com/blog/products/g-suite/help-secure-your-organization-with-new-endpoint-management-intelligent-access-controls

OECD. (2017, May). *Supporting an effective cyber insurance market*. https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf

Pelland, S. (2018, December 12). *Our take on Microsoft's free SharePoint Migration Tool (SPMT)*. ShareGate. Retrieved July 26, 2020, from https://sharegate.com/blog/our-take-microsoft-free-sharepoint-migration-tool

Perry, S. (2017, November 17). Exploring the effectiveness of approaches to discovering and acquiring virtualized servers on ESXi. SANS Reading Room.

Drew Hjelm

https://www.sans.org/reading-room/whitepapers/bestprac/exploring-effectiveness-approaches-discovering-acquiring-virtualized-servers-esxi-38155

Spiceworks. (2019, July). *The Future of Network and Endpoint Security*. https://3upg5n1ajpdonqkkp34tcif1-wpengine.netdna-ssl.com/marketing/wp-content/uploads/sites/2/2019/07/MS5_NetworkEndpointSecurity_WhitePaper-jul23-v3-1.pdf

Spiceworks. (2019, September 23). *2020 state of IT: Tech budgets, trends, and purchase drivers*. https://www.spiceworks.com/marketing/state-of-it/report/

Stith, I. (2016, April 4). *How fast can you go: Migrating to SharePoint Online with the high speed migration service*. SharePoint Evolved. https://www.sharepointevolved.com/2016/04/04/fast-can-go-1-terabyte-migration-sharepoint-online/

US Small Business Administration (SBA). (2018). *United States small business profile*. https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

Appendix: Azure AD Cloud Migration Checklist (Microsoft 365)

Prerequisites:

- The organization has one on-premises server providing Active Directory, DNS, and file server roles
- The organization is using cloud-hosted SaaS applications no longer requiring on-premises servers
- The organization is using Microsoft 365 for email delivery with Active Directory Sync (ADConnect) enabled
- The organization has Business Premium or higher Microsoft 365 subscription
  - https://portal.office.com/adminportal/home#/subscriptions
- Organization endpoints are all running Windows 10 or newer.
- Incident Responder or Organization has access to a server with at least 8GB memory for SharePoint migration.

Migration Steps

- Disable Active Directory sync in Microsoft 365 using PowerShell

```
Install-Module MSOnline
Connect-MSOLService
Set-MsolDirSyncEnabled -EnableDirSync $false
```

- Ensure users change passwords in Microsoft 365 and enable Self-Service Password Reset
  - https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/PasswordReset
- Ensure Azure Security Defaults are Enabled
  - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
- Verify users have configured Multifactor Authentication

Drew Hjelm

    - https://account.activedirectory.windowsazure.com/usermanagement/multifactorverification.aspx
- Ensure audit logging enabled in Microsoft 365
    - https://protection.office.com/unifiedauditlog
- Assign a Microsoft Intune Security Baseline to Device Groups
    - https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines#create-the-profile
    - https://endpoint.microsoft.com/?ref=AdminCenter#blade/Microsoft_Intune_Workflows/SecurityManagementMenu/securityBaselines
- Reconfigure networking for endpoints to use a firewall for DNS resolution. These steps vary depending on how the organization has configured their networking. The simplest way to handle this is to configure DHCP to set the DNS resolver to be the firewall rather than the DC.
- Ensure workstations are cleared of malware, possibly requiring forensic analysis, forensic imaging, or workstation reimaging.
- Disjoin workstations from on-premises Active Directory Domain using `sysdm.cpl`
- Join Workstations to Azure Active Directory
    - Start Menu > Settings > Accounts > Access Work or School
    - When on the "Set up work or school" screen, click "Join this device to Azure Active Directory."
    - To prevent end-users from becoming local administrators on their endpoints, system administrators should use an Azure AD account with the Azure AD Device Administrator role assigned to join endpoints to AAD.
- Migrate local files from old user folder to new user folder and allow sync to OneDrive
- Migrate files from a file server to SharePoint Online

- https://docs.microsoft.com/en-us/sharepointmigration/introducing-the-sharepoint-migration-tool