2020



NIST Cybersecurity Framework with Microsoft 365 Business

BUSINESS CASE AND OVERVIEW

NICK ROSS, MICROSOFT CERTIFIED EXPERT ADMINISTRATOR

NIST CSF WITH MICROSOFT

Overview & Business Case

PURPOSE

This document is a guide for mapping Microsoft 365 Business solutions to the NIST Cybersecurity framework core. It is meant to help you sell the solution to your customer as a compliance offering and show how these solutions address each category in the NIST Core functions:

Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities

Protect– Develop and implement appropriate safeguards to ensure delivery of critical services

Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Respond– Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

AUDIENCE

This guide is was written for Managed Services Providers but could be used by other parties to assess the Microsoft 365 Business solution with NIST Cybersecurity Framework.

NIST CSF WITH MICROSOFT

Overview & Business Case

EXECUTIVE SUMMARY

Digital Transformation has reshaped the ways people work and the ways companies do business. Employees expect to work from anywhere, at any time, on any device. Third party SaaS applications are being onboarded at a rapid pace in efforts to enhance productivity. The security landscape has drastically changed. Users are likely to get breached outside of your network, exposing corporate data and potentially bringing an infected device back into your "trusted" perimeter. As an IT administrator, the more you lock down access to corporate resources, the more you get blamed for decreasing productivity and increasing frustrations around the organization. Companies need a solution that provides a "zero-trust" model without inhibiting productivity.

Microsoft 365 Business is a great solution for the shifting landscape. When exploring an upgrade from a legacy solution like Office365 Business Premium, it is best to start the conversation around compliance with your customer. Many businesses are required to conform to certain compliance regulations. Businesses that don't follow these regulations still need to follow cybersecurity best practices to avoid a breach or data loss. The NIST Cybersecurity Framework is a guide for organizations to manage and reduce cybersecurity risk. The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018). NIST's security standards serve as the foundation for FedRAMP. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services. By aligning your security practices with NIST CSF, you are giving yourself a foundation to achieve FedRAMP certification. In this guide, we show you how Microsoft 365 Business solutions map to the NIST CSF. Discovery questions are listed that you should be asking to help sell and implement this solution. Ultimately, the sale should be driven with the awareness around how the customer is exposed from a security and compliance standpoint.

A secondary objective is to encourage you to compare the suggestions given in this guide with your existing cybersecurity policies, risk management/mitigation policies, vulnerability assessments, and overall business practices. Whether you are just starting out as an MSP or have been in business for many years, we think it's always good to periodically review the policies and procedures that you have in place.

NIST CSF WITH MICROSOFT

Overview & Business Case

Disclaimer

The partner and customer action items provided in this guide are recommendations. It is up to you to evaluate the effectiveness of these recommendations in your respective regulatory environment prior to implementation. Recommendations should not be interpreted as a guarantee of compliance, but they are a good checklist to follow and compare against your existing policies.

Framework Core Overview:

The NIST framework core is a set of cybersecurity activities, desired outcomes and applicable references that are common across critical infrastructure sectors. The core consists of five concurrent and continuous functions. Each function contains categories with subcategories of guidelines.



Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Change Risk Management



Protect

- Identity Management and Access Control
- Awareness and Training
- Data Security
- Protective Technology
- Information Protection Processes and Procedures
- Maintenance



Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes



Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements



Recover

- Recovery Planning
- Improvements
- Communications

We will be covering each category in this guide and showing you what solution in the M365 Business stack addresses those categories and subcategories.

Overview & Business Case

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST CSF WITH MICROSOFT

Overview & Business Case



IDENTIFY

Description: “Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.”

Asset Management

Description: “The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed, consistent with their relative importance to business objectives and the organization’s risk strategy.”

Discovery Questions to Ask:

- *What applications or portals are you users accessing corporate data?*
- *What apps contain business critical data?*
- *Are users accessing corporate data from a personal device?*
- *If a user leaves, how do you know they don’t have corporate data stored on their personal device?*
- *Do users access email through their personal cell phone?*
- *Are there business-critical pieces of data that would leave you exposed if a personal device was compromised?*
- *What would be the cost to the company if this data was leaked?*
- *Are we compliant if data is leaked to unmanaged applications like a user’s personal Google Drive?*
- *Do you want your users to be able to access corporate data securely from anywhere at any time?*
- *Do employees have access to corporate apps after they leave the company? How do you know if they do?*

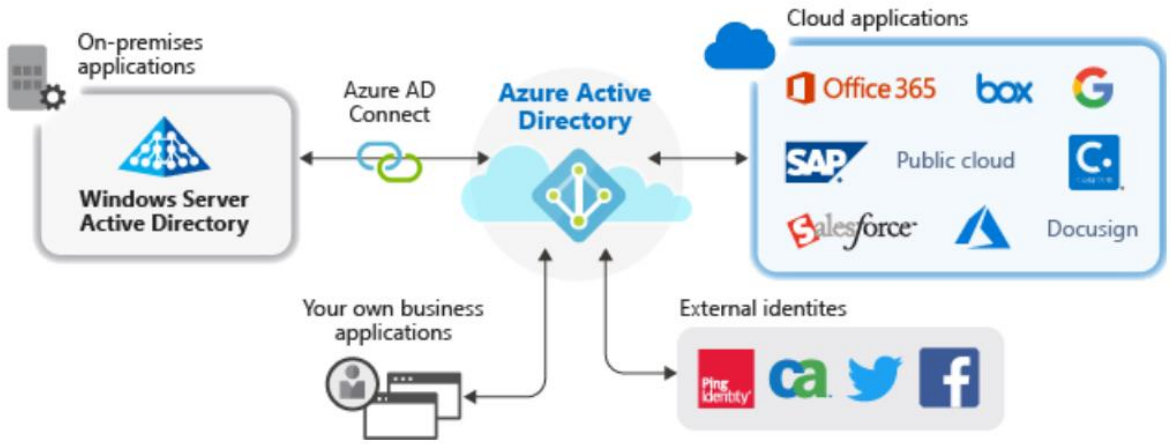
NIST CSF WITH MICROSOFT

Overview & Business Case

Microsoft 365 Solution: Azure AD, Intune

Managing and protecting key assets in a zero-trust model is a foundational component to M365 Business. The solution allows you to discover and grant access to resources based on user and device trust claims. Management of user identities, PCs, Macs, Mobile devices, and cloud applications can all be controlled at granular level on or off your trusted network.

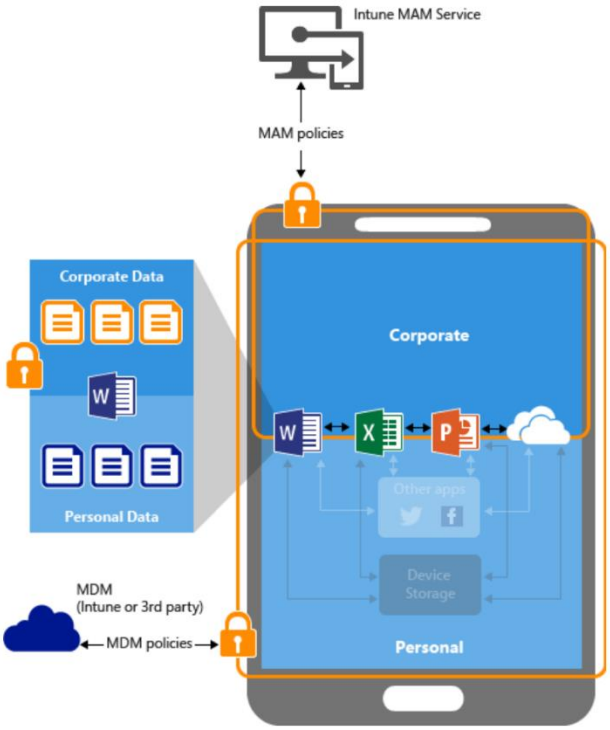
Azure Active Directory is the backbone of your solution. Policies can be scoped to users, groups, applications, and devices. Adding applications for single sign-on improves security because users do not have to store or transfer passwords. Access to applications can be granted as part of an AzureAD group so users can increase their productivity by not having to wait for new credentials. At the same time, when a user leaves the company, their access to all applications can be removed immediately. AzureAD Connect can be set up to connect your on-premise active directory to the cloud and extend your security perimeter.



NIST CSF WITH MICROSOFT

Overview & Business Case

Intune is both a Mobile Device Management (MDM) and Mobile Application Management (MAM) solution. You can enroll Windows, macOS, Android, and iOS devices into this MDM solution and control access to applications based on device health. We can create policies around applications that contain corporate data so that we protect this data even on unmanaged devices such as personal cell phones. This protection includes controls on restricting save as and cut/copy/paste permissions.



Business Case-

Ex. Intune MAM: A user accesses their email on their personal cell phone. They try to save a corporate document to their personal Google Drive. They are blocked from doing so with a message that states their corporate policy does not allow saving to unmanaged applications.

Ex. AzureAD: Change Management has always been a cumbersome process for Company XYZ and users often grow frustrated when they move across departments because they do not have the access to applications they need. Using AzureAD, you can add applications to the portal for single sign-on and grant access based on group membership. We now have an inventory of all applications the company uses and know who can access those applications.

Overview & Business Case

Action Items:

- *Gather an inventory of all applications across the organization and assign them a risk score*
- *Understand what devices types you will support from a Mobile Device Management standpoint*
- *Create a Compliance Policy for each Device type you defined above*
- *Enroll Devices into MDM*
- *Create an app protection policy for Windows, iOS, and Android devices for mobile application management*

***Category(s) Met**: ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-5, ID.AM-6*

Business Environment

Description: "The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions."

Discovery Questions to Ask (Internal to MSP):

- *Do you know the customer's business structure and mission statement?*

While similarities can be found in certain verticals, you really show your value as a managed service provider by tailoring your solutions to customer needs. Performing a discovery of workflows and stakeholders across the organization is key. Aligning your solution stack with the customers business objectives will set you up for success and strengthen the security solutions you implement.

**NOTE*We will not be touching on a Microsoft solution here as this is basic discovery.*

Overview & Business Case

Governance

Description: “The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.”

Discovery Questions to Ask (Internal to MSP):

- *Have you communicated your cybersecurity policies to the customer?*
- *Are cybersecurity roles defined internally and at the customer level?*
- *If this customer follows compliance requirements, do you have the necessary controls in place if they were to get audited?*
- *What policies and procedures have you implemented to govern and manage risk? Is this defined for every customer?*

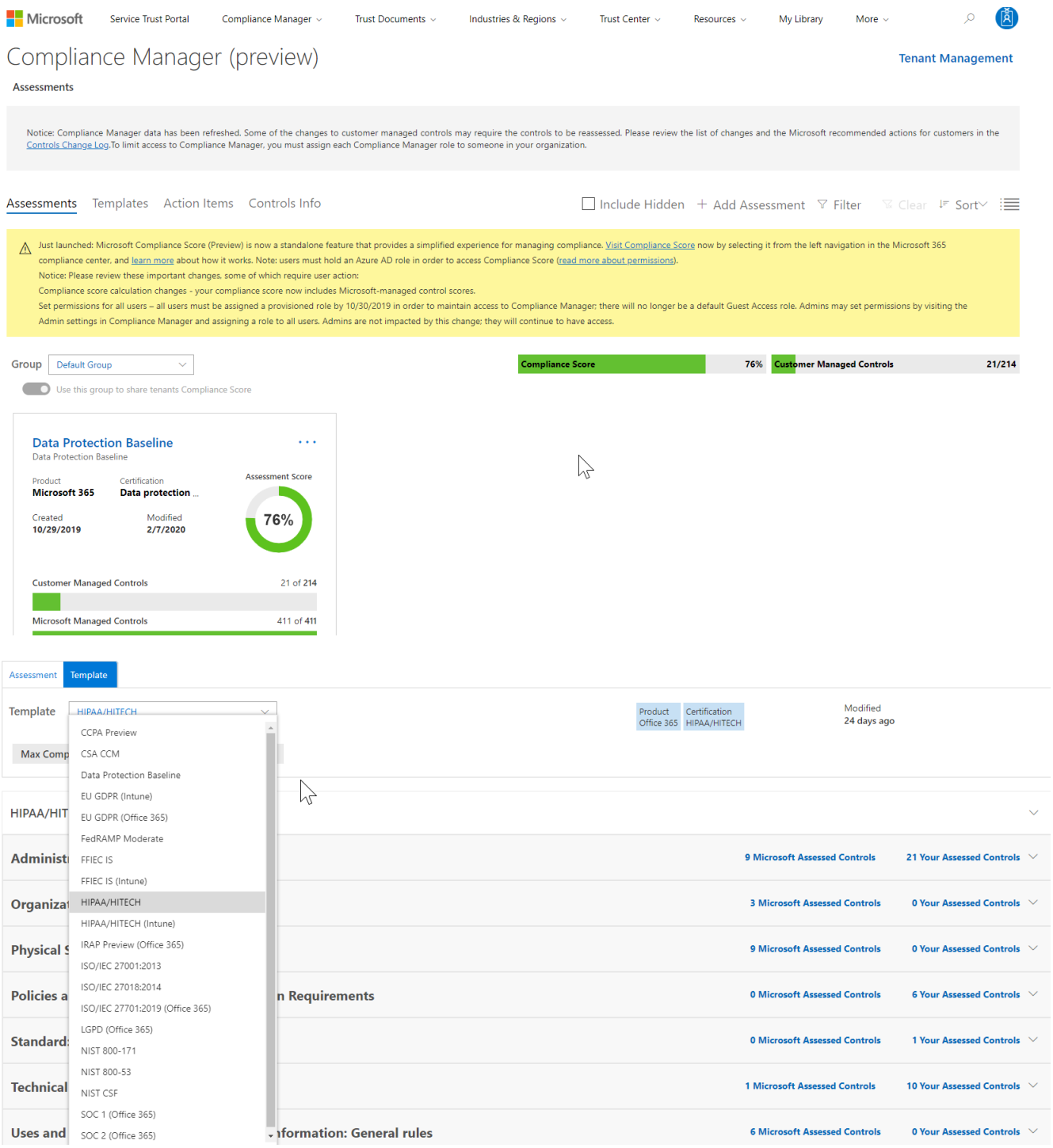
Microsoft 365 Solution: Service Trust Portal

Microsoft’s security stack includes many solutions for data classification and data loss prevention. You can create custom data loss prevention policies, retention tags, and encryption settings across your applications. Labels and policies can be automatically applied with the detection of certain sensitive information like PII.

Microsoft Compliance Manager is a dashboard and management tool that provides a summary of your data protection and compliance stature and recommendations to improve data protection and compliance. The customer actions provided in Compliance Manager are recommendations; it is up to you to evaluate the effectiveness of these recommendations in their respective regulatory environment prior to implementation. Recommendations found in Compliance Manager should not be interpreted as a guarantee of compliance, but they are a good checklist to follow. They have predefined templates for most compliance regulations, and they allow you to assign task to users in your organization. Microsoft has recently integrated these capabilities in the Security and compliance center, giving you a “Compliance Score” which action items you can take to help improve that score.

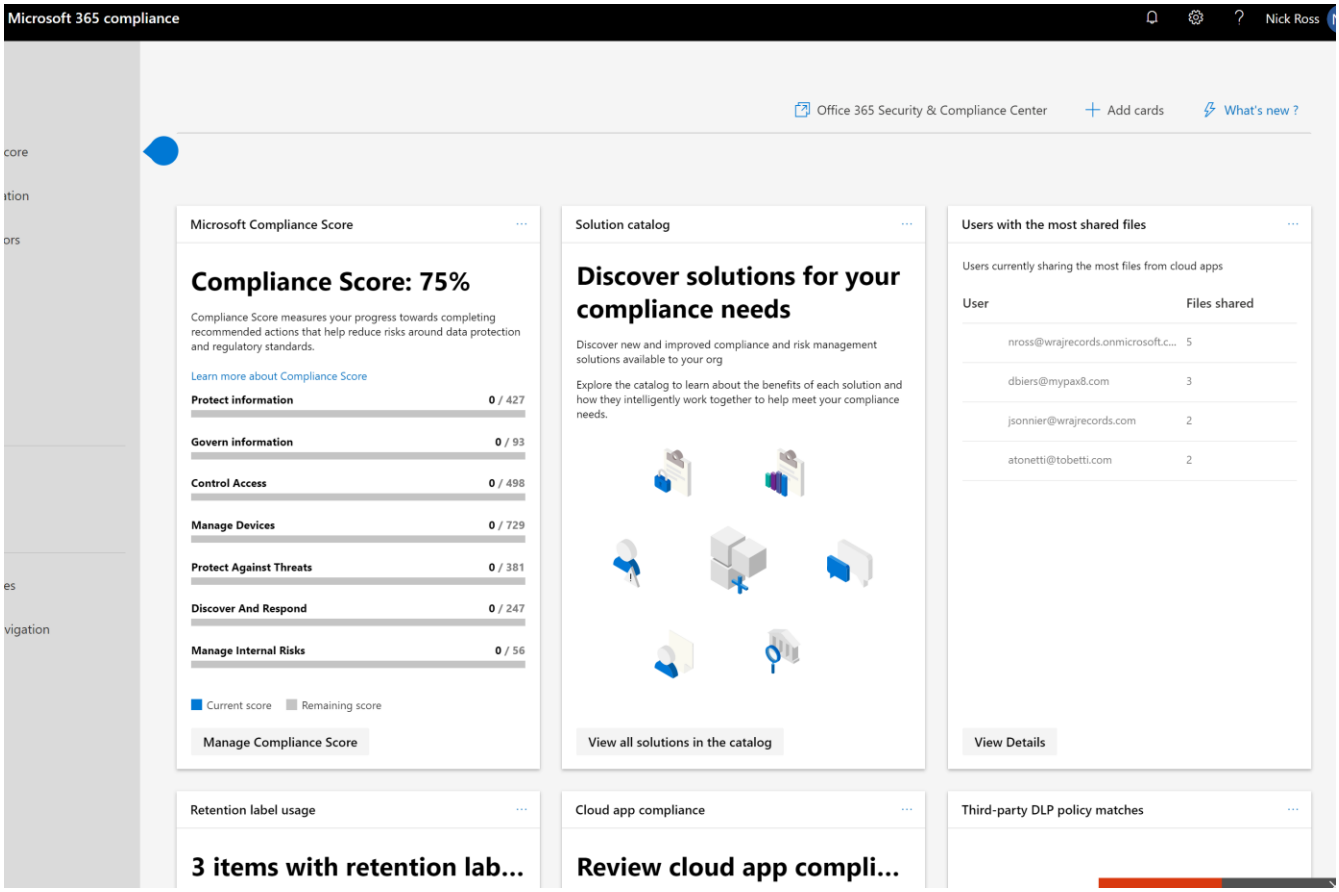
NIST CSF WITH MICROSOFT

Overview & Business Case



NIST CSF WITH MICROSOFT

Overview & Business Case



Business Case: *Using compliance manger, I can perform an assessment of HIPPA compliance with the recommended action they provide for each control to get to a more compliant state.*

Action Items:

- *Define your cybersecurity policy (if not done already)*
- *Communicate cybersecurity roles with the customer (if not done already)*
- *Define your policies around the governance of risk in the organization (if not done already)*
- *Login to the Service Trust Center and go to the assessment page where you can access templates such as NIST, ISO, HIPPA and more to view what recommended actions to take*

Category(s) Met: ID.GV-3

Overview & Business Case

Risk Assessment

Description: "The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals."

Discovery Questions to Ask (Internal to MSP):

- *Are all asset vulnerabilities known at the customer site? I.e. If they are using a 3rd party app, what vulnerabilities exist?*
- *Are these vulnerabilities documented with a risk score?*
- *Is business impact identified if these assets were to get breached?*
- *Are risk responses identified and prioritized?*

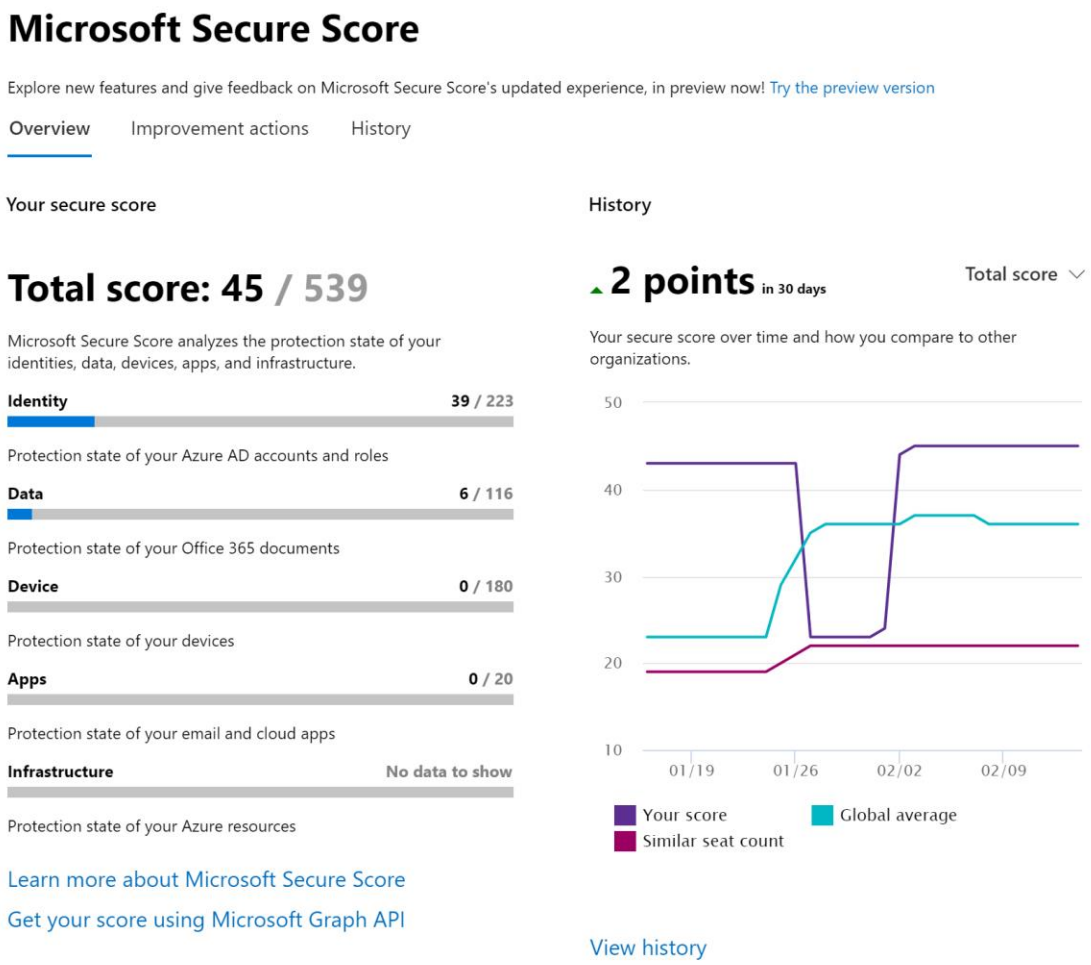
Microsoft 365 Solution: Secure Score, Intune, Azure AD

The solutions in Microsoft 365 Business provide a holistic platform to measure vulnerabilities across users, devices, cloud applications, and data. Role-based access can be implemented to provide a model of least-privilege to users in the tenant and you can identify what applications have the most critical business data. Intune allows you to manage device risk and know if a device is in a compromised state.

Secure Score is like a credit score for a tenant's security. It provides you with better visibility to vulnerabilities in the organization and recommends settings you can configure to improve your score. If you are acquiring a new customer or trying to win a customer, accessing a tenant and reviewing their secure score is a great way to see where they have vulnerabilities present.

NIST CSF WITH MICROSOFT

Overview & Business Case



Business Case: *Using Secure score, I can view security actions to take in the tenant to get to a more secure state and see where vulnerabilities exist. I could see that the Global Admin Role is assigned to 5 users in the company who do not need that level of access. I can also see devices that are in an uncompliant state and drill down to see how that device is potentially compromised.*

NIST CSF WITH MICROSOFT

Overview & Business Case

Action Items:

- *Define and document all asset vulnerabilities at the customer site*
- *Define a risk score for all vulnerabilities. Threats, vulnerabilities, likelihoods, and business impact are used to define risk.*
- *After defining risk score, document risk responses and SLA's you want to meet for each*
- *Login to the Security Center of Microsoft and review a customer's secure score data. Project Manage task to delegate to your team to improve the security posture of the tenant.*

Category(s) Met: ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4

Risk Management Strategy

"The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions."

Discovery Questions to Ask:

- *Where does business-critical intellectual property live within the organization?*
- *Who has access to business-critical information?*
- *What are the most business-critical assets?*

Align with the executives at the company on a risk management strategy. If you understand the organization's risk tolerance, you can understand how restrictive you want to get with policies that you roll out to the organization. You want to follow a model of least to most restrictive. For example, for a firm that has a low risk tolerance, you may want to implement policies that are minimally restrictive to bring awareness and then slowly move into a more trestrictive version in a phased rollout.

**NOTE* We will not be touching on a Microsoft solution here as this is basic discovery. The strategy and risk tolerance that is defined will decide what solutions we implement and how restrictive we make policies.*

Overview & Business Case

Supply Chain Risk Management

Description: "The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks."

Discovery Questions to Ask Customer:

- *How often do you interact with users outside your organization?*
- *What is the primary method of communication? (email, phone, chat, etc.)*
- *How do you share documents with external users?*
- *Do you ever work on projects with outside contractors? Do you have language in those contracts that speaks to the data you will be giving access to?*
- *How do you know employees are using best security practices when sharing company data?*

Microsoft 365 Solution: AzureAD (B2B), Conditional Access, Data Loss Prevention, Azure Information Protection

How internal employees interact and share documentation with external users is often done in an insecure manner. Microsoft has implemented many security features across it's entire solution stack to provide a solution to this risk, while not inhibiting productivity. Controls can be put into place to protect the company in the case of human error as well. Often, many of these controls should be considered mandatory when dealing with firms that fall under compliance regulations.

Azure business-to-business, or Azure B2B, enables organizations to work securely with other organizations even if they are not using AzureAD. You can invite external users to your organization to access certain pieces of data. Using Conditional Access, you can scope what applications those users have access to and require them to use multi-factor authentication.

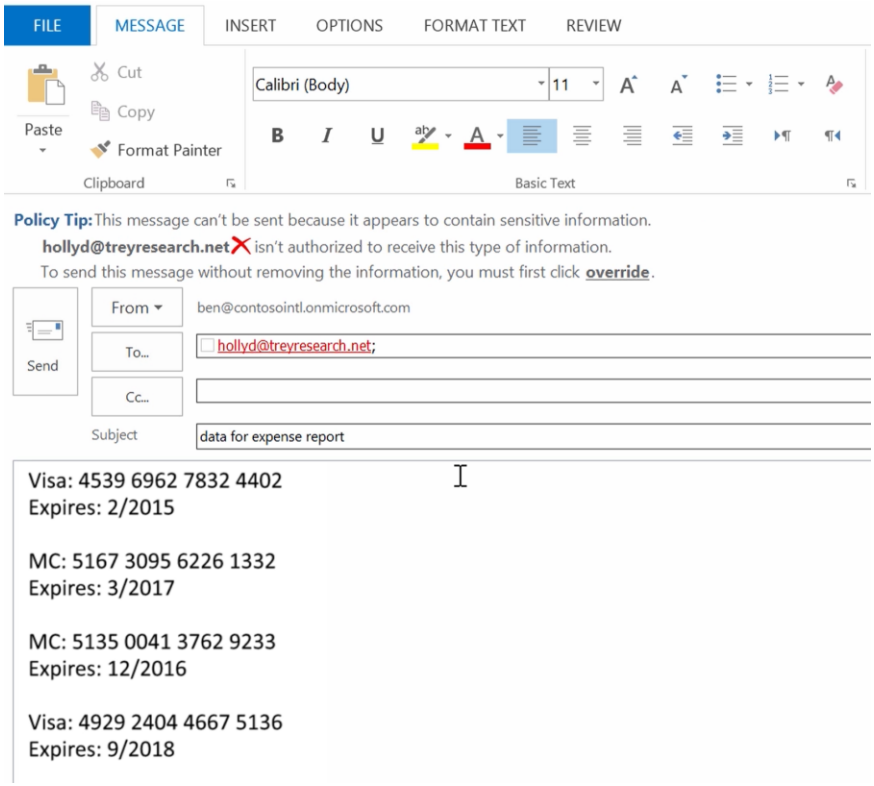
To prevent data loss, you can set up data loss prevention policies to automatically take action when documents containing certain sensitive data are trying to be shared outside your organization (or even internally between departments). These actions include notifying users with policy tips or blocking then from sending altogether. Additionally, with Azure Information Protection, you can classify documents and apply specific controls to that classification such as requiring encryption or preventing a user from sending outside the organization.

NIST CSF WITH MICROSOFT

Overview & Business Case

Business Case: *A user has a document containing PII (SSN) and attaches it in an email to send to a user of an external domain. With DLP policies in place, that user will get a policy tip making sure they understand they are sending to a user outside the company (you could restrict so far to not allow them to send at all) and it will also encrypt the document automatically.*

Ex.



Action Items:

- *Ensure that the contracts the customer has with suppliers or outside contractors contains language for the data they are willing to share.*
- *Make sure there are policies in place to meet these contractual obligations (Enforce the least privileged model)*
- *Configure DLP policies, AIP Labels, Conditional Access Policies, and external sharing settings to meet the company's requirements in a secure manner*

Category Controls Met: ID.SC-2, ID.SC-3

NIST CSF WITH MICROSOFT

Overview & Business Case



PROTECT

Description: Develop and implement appropriate safeguards to ensure delivery of critical services.

Identity Management and Access Control

Description: "Access to assets and associated facilities is limited to authorized users, processes, and devices, and to authorized activities and transactions."

Discovery Questions to Ask:

- *Are you using a model of least privilege for applications across the company?*
- *How are employees storing credentials across the organization?*
- *What applications or portals are users accessing corporate data?*
- *What apps contain business critical data?*
- *Are users accessing corporate data from a personal device?*
- *If a user leaves, how do you know they don't have corporate data stored on their personal device?*
- *Do users access email through their personal cell phone?*
- *Are their business-critical pieces of data that would leave you exposed if a personal device was compromised?*
- *What would be the cost to the company if this data was leaked?*
- *Are we compliant if data is leaked to unmanaged applications?*
- *Do you want your users to be able to access work data securely from anywhere at any time?*
- *Do employees have access to corporate apps after they leave the company? How do you know if they do?*

Overview & Business Case

Microsoft 365 Solution: Conditional Access, Azure AD, Intune

With Conditional access you can create policies based on a set of conditions that include:

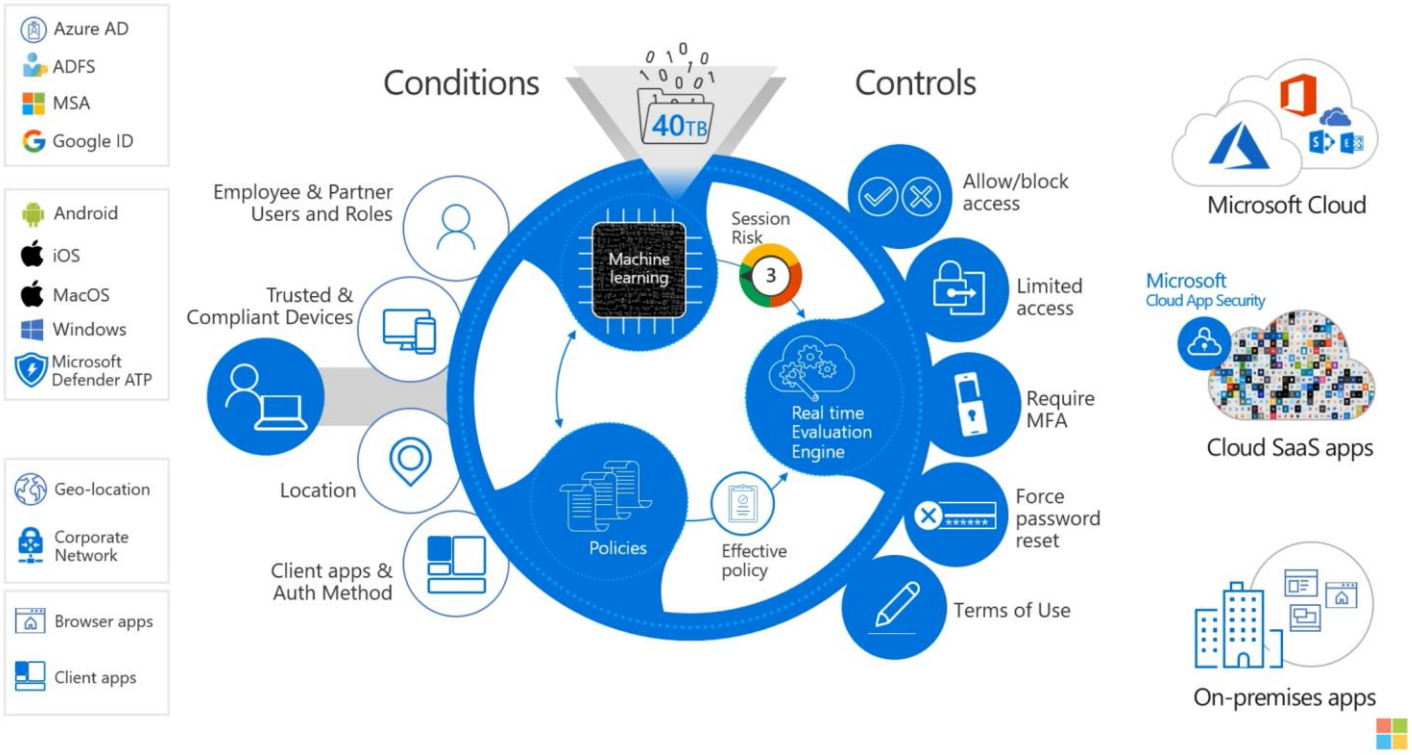
- Users/Groups: Who do you want to scope this policy to? Is there anyone you want to exclude?
- Applications: What applications does this policy apply to? Think of the apps that have the most sensitive data
- Devices: Are there certain device platforms you want apply this policy to? Do you not want to grant access on a device that isn't enrolled into Intune?
- Locations: Is this user on my network?

Whenever a user meets the conditions defined, you can then apply a variety of controls:

Examples-

- Let users access the applications unimpeded. This would be in low risk scenarios such as the user being on your network
- Prompt the user for additional security with MFA
- Require the device to be enrolled in Intune and in a healthy state
- Block access completely (App is too critical to be accessed off network, a user's device is comprised, app uses legacy authentication, MFA prompt failed, etc.)

Overview & Business Case



Business Case: *A customer has a financial document with critical business data. If that document was to be compromised the financial toll to the company would be huge. You want to give access to the document to certain employees if they are off your network, but you do not want them to download the document to an unmanaged device. You set up a conditional access policy scoped to the necessary users that says if this user is not on my network and not on a device managed by Intune, I want to allow them to access the document in a browser, require MFA, and prevent download.*

Action Items:

- *Take your asset inventory you garnered earlier in this document with the list of apps and their risk score. Create a Conditional Access Policy for the applications that have more restrictive controls with higher risk scores.*
- *Create a conditional access policy to require MFA for all users if they are not on your network*

Category(s) Met: PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7

Overview & Business Case

Awareness and Training

"The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities, consistent with related policies, procedures, and agreements."

Discovery Questions to Ask (Internal to MSP):

- *Do we provide security awareness training to end users?*
- *Do users with elevated privileges understand importance around continual security training?*

STACK IT UP

Microsoft's Office 365 ATP comes with an attack threat simulator with Enterprise plans but not with M365 Business. Here is a good opportunity to stack another security training tool like Breach Secure Now to train end users.

NIST CSF WITH MICROSOFT

Overview & Business Case

Data Security

"Information and records (data) are managed, consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information."

Discovery Questions to Ask:

- *Can a user access corporate data on their personal device?*
- *Can a user save corporate data to their personal storage?*
- *How do you prevent data leakage on a lost or stolen device?*
- *How do you prevent data loss when an employee leaves the company or is fired?*
- *Do users send documents and emails with sensitive company info to external users without you knowing?*
- *How do you know if data is being accessed on a device with malware?*
- *Are there certain sensitive documents you would not want shared between internal departments or groups?*

Microsoft 365 Solution: BitLocker, Azure Information Protection, App Protection Policies, Data Loss Prevention Policies

With Microsoft 365 Business, data is protected in the cloud, on physical devices, in rest, and in transit. There are many solutions part of the stack to help secure corporate data.

BitLocker Encryption: Device encryption for Windows 10 devices. Devices enrolled in Intune can have device compliance policies that require Bitlocker and device profiles that automatically configure Bitlocker without IT intervention.

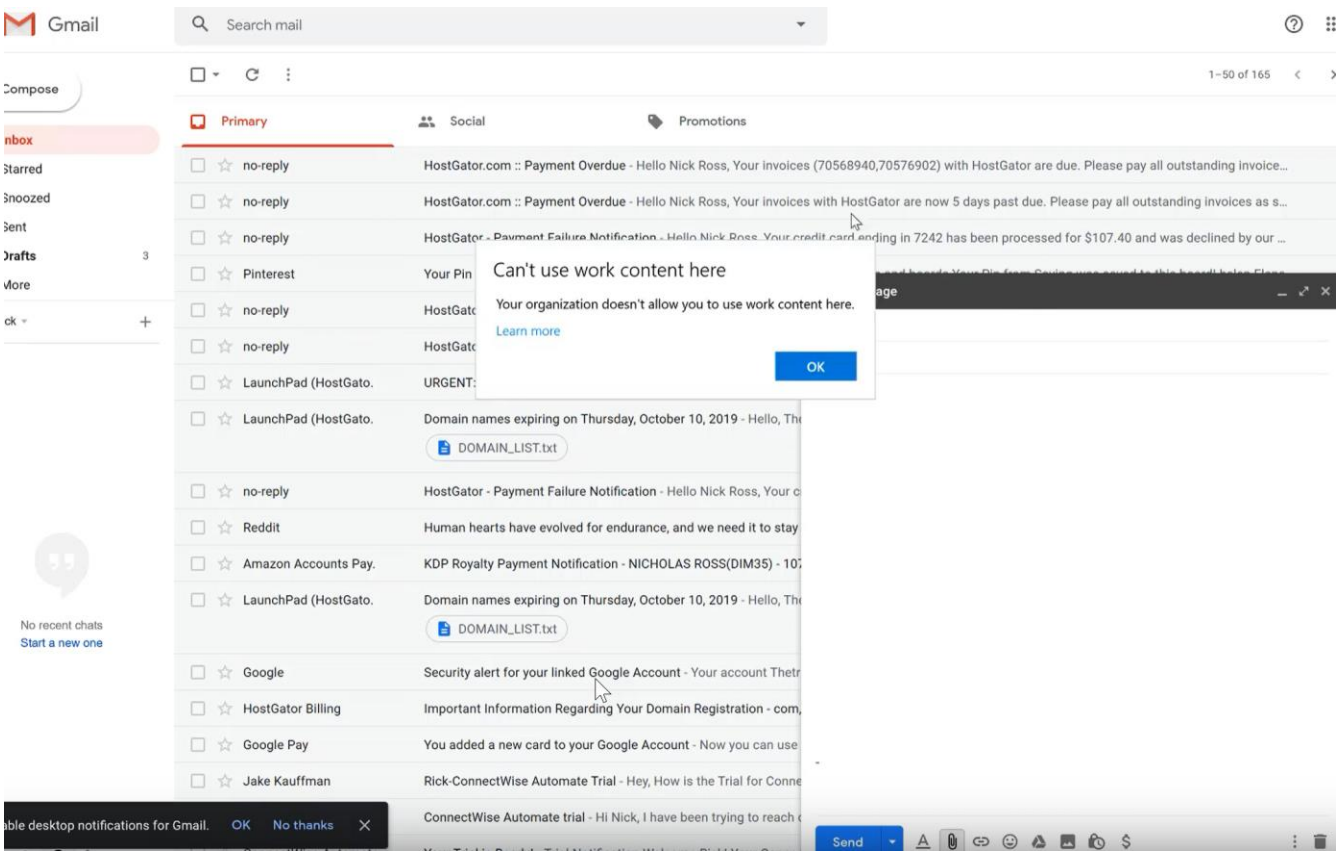
Azure Information Protection (AIP): This technology allows you to identify, classify, protect, and monitor data across the organization. You can classify pieces of data with tags such as "confidential" and apply certain policies around that classification. It also allows you to provide email encryption automatically with policy detection or on-demand.

Overview & Business Case

App Protection Policies: You can create app protection policies for Windows, Android, and iOS devices. These policies do not require a device to be enrolled in Intune. They allow you to prevent saving of data to unmanaged applications and restrict cut/copy/paste abilities.

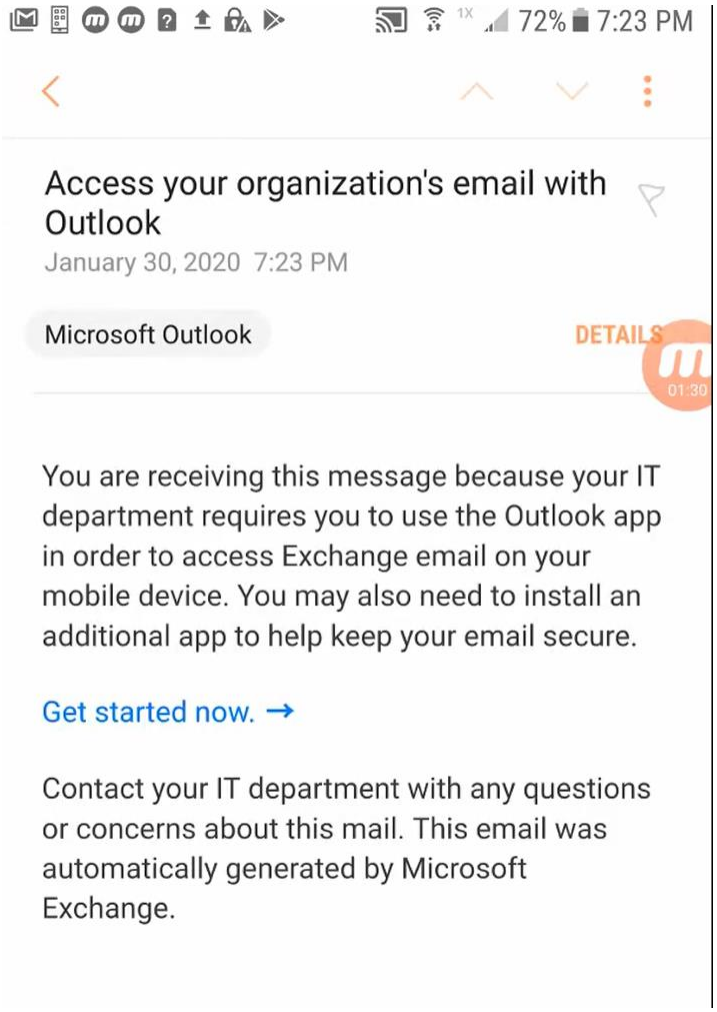
Data Loss Prevention Policies: These policies allow you to automatically detect sensitive information across Exchange, SharePoint, OneDrive, and Teams and take protective action when that information is being shared. This action could include a policy tip or blocking the action completely or both.

Ex. App protection policies preventing user from attaching corporate document in personal Gmail Account:



Overview & Business Case

Ex. An Android user trying to access their mail through the native mail client. They are redirected to the Google Play Store to download the outlook app:



NIST CSF WITH MICROSOFT

Overview & Business Case

Business Case: *A customer wants to ensure that all corporate documents are saved in a managed application like OneDrive. For these documents, they want to protect artifacts that have their customers credit card information. Currently users can save documents to any location like their personal Google Drive and copy corporate information to unmanaged Word documents. As the IT Pro, you can configure a Windows app protection policy for all applications in this customer's environment that contain corporate data. You can configure this policy to block save as permissions to unmanaged apps and restrict cut/copy/paste abilities as well. When a user goes to save a corporate document to a local or unmanaged location, they will get a message telling them their company does not allow this action. Additionally, you can configure an Azure Information Protection label to apply to documents with credit card information. The policy you set for this label will prevent users from sending documents to users outside the organization.*

Action Items:

- *Understand what devices types you will support from a Mobile Device Management standpoint (Windows, macOS, iOS, Android)*
- *Create a Compliance Policy for each Device type you defined above. For Windows 10 Devices, include requiring Bitlocker encryption as part of the compliance policy*
- *Enroll Devices into MDM*
- *Create an app protection policy for Windows, iOS, and Android devices for mobile application management*
- *Create AIP Labels custom to the business needs*

Category Controls Met: PR.DS-1, PR.DS-2, PR.DS-5, PR.DS-6, PR.DS-8

NIST CSF WITH MICROSOFT

Overview & Business Case

Protective Technology

"Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements."

Discovery Questions to Ask:

- *Can a user access their corporate data on their personal device?*
- *Can a user save corporate data to their personal storage?*
- *How do you prevent data loss to a lost or stolen device?*
- *How do you prevent data loss when an employee leaves the company or is fired?*
- *Do users send documents and emails with sensitive company info externally without you knowing?*
- *How do you know if data is being accessed on a device with malware?*
- *What resources are accessed off your corporate network?*

Microsoft 365 Solutions: Intune, Conditional Access, Data Loss Prevention, Azure Information Protection, Advanced Threat Protection

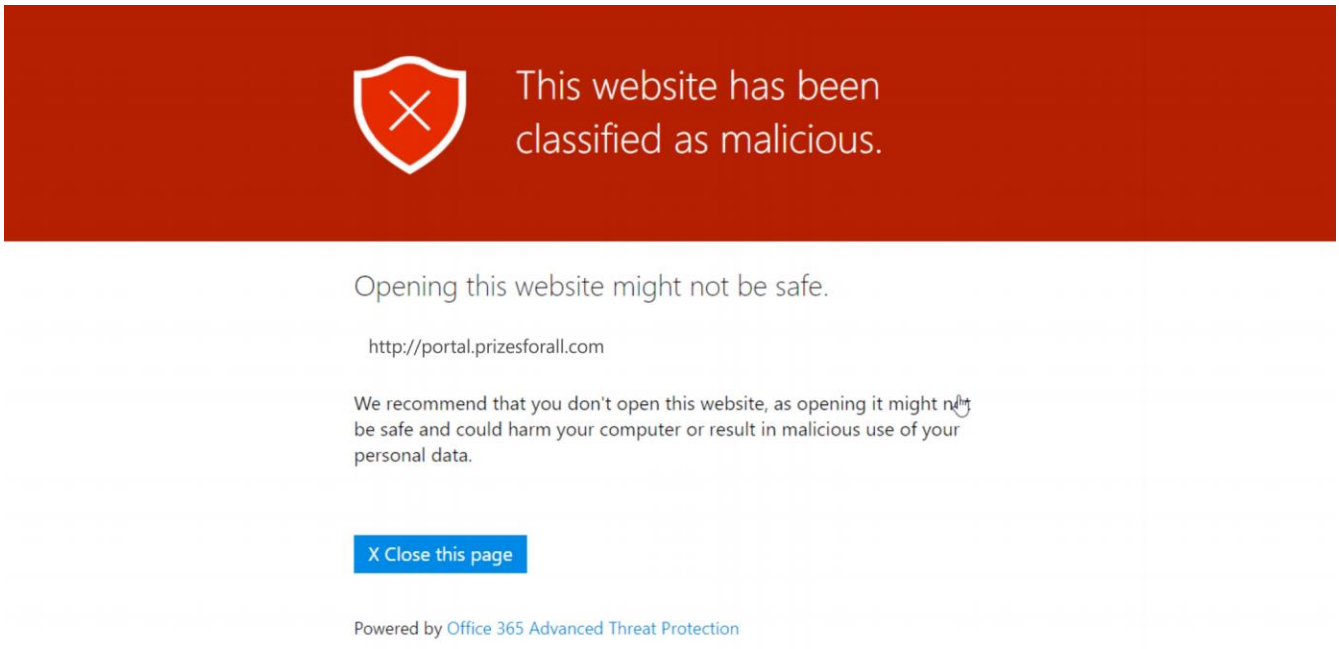
Device Level: We can centrally manage Windows, macOS, Android, and iOS devices and create policies that detect if the device is in an unhealthy state. Bitlocker encryption can be enforced on Windows 10 devices and we can remotely wipe a device if it is lost or stolen.

User Level: With conditional access, we can now protect sensitive information no matter the user's location. We can create policies that require heightened security from the user if they are located outside of our network. Users can leverage SSO to avoid sharing or storing credentials in an unsecure manner. For data loss prevention, users can be prompted with policy tips that let them know when they are sharing sensitive data in an unsecure manner. Certain documents can be automatically encrypted if they are detected with PII. For user security, Office 365 Advanced Threat Protection provides policy tips on strange behavior and quarantines links and attachments across Exchange, Teams, SharePoint, and OneDrive.

Overview & Business Case

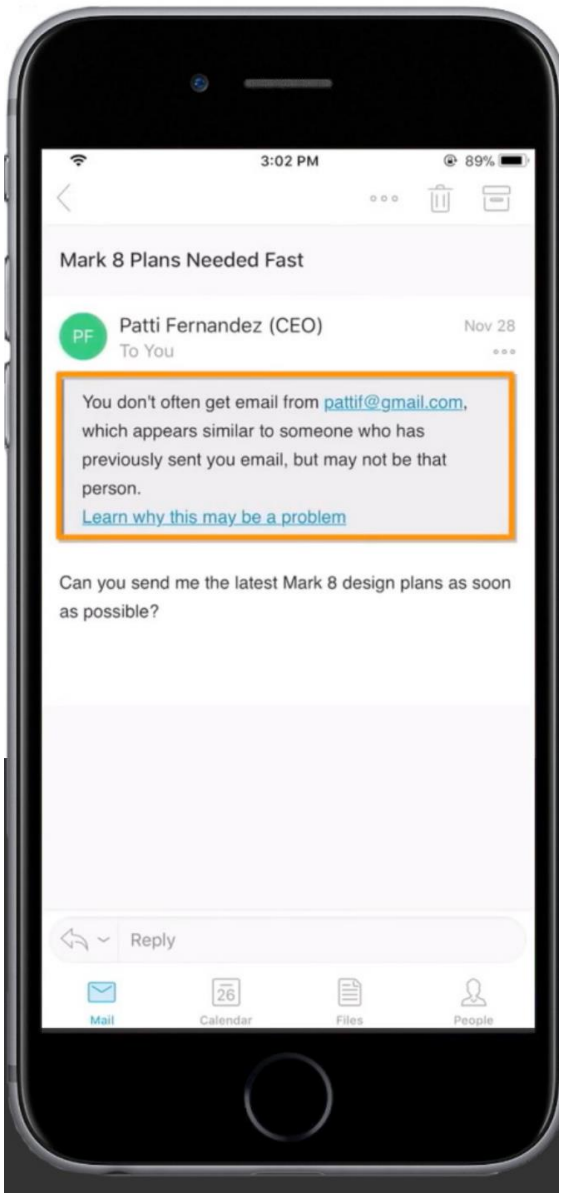
Application Level: With app protection policies we can secure access of corporate data on managed or unmanaged devices. We can even encrypt corporate data on personal cell phones and remotely wipe that data when an employee leaves the company. We can inventory all apps a company uses and assign a risk tolerance to each one. With this information, we can create conditional access policies that enforce controls for more security or remove access when certain conditions are met. Office 365 Advanced Threat Protection can scan Exchange, Teams, OneDrive, and SharePoint for malicious attachments.

Ex. ATP:



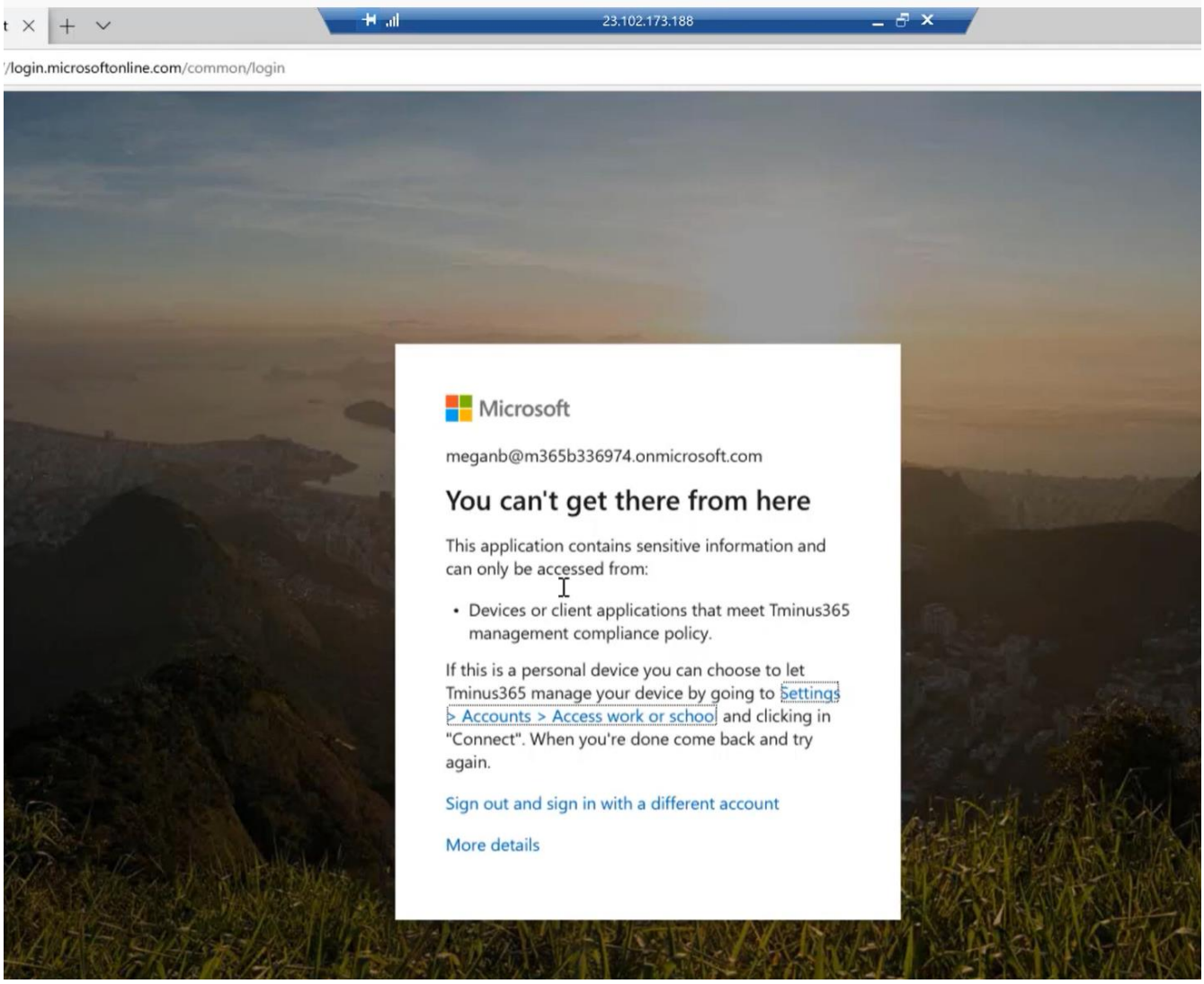
Overview & Business Case

Ex. User tips from ATP:



Overview & Business Case

Business Case: *A user's device is infected with malware. They do not know their computer is infected and they try to access corporate data. We set up a conditional access policy to prevent access if the device is in an unhealthy state. The user will get a message about this when they try to sign-in and will reach out about the problem.*



Overview & Business Case

Action Items:

- *Understand what devices types you will support from a Mobile Device Management standpoint*
- *Create a Compliance Policy for each Device type you defined above.*
- *Enroll Devices into MDM*
- *Create an app protection policy for Windows, iOS, and Android devices for mobile application management*
- *Create AIP Labels custom to the business needs*
- *Set up a Policy for ATP Safe Links and Safe Attachments*
- *Set up a policy for Anti-phishing*

Category(s) Met: PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7

Information Protection Processes and Procedures

"Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets."

Discovery Questions to Ask (Internal to MSP):

- *Do we have a SaaS backup solution in place? What solutions should we be backing up?*
- *What RPO or RTO metrics do we want to meet?*
- *What are the company's retention policies for Exchange, SharePoint, OneDrive, and Teams?*
- *How long after a user leaves the organization is information permanently deleted?*
- *How long after a user leaves do we delete backups?*

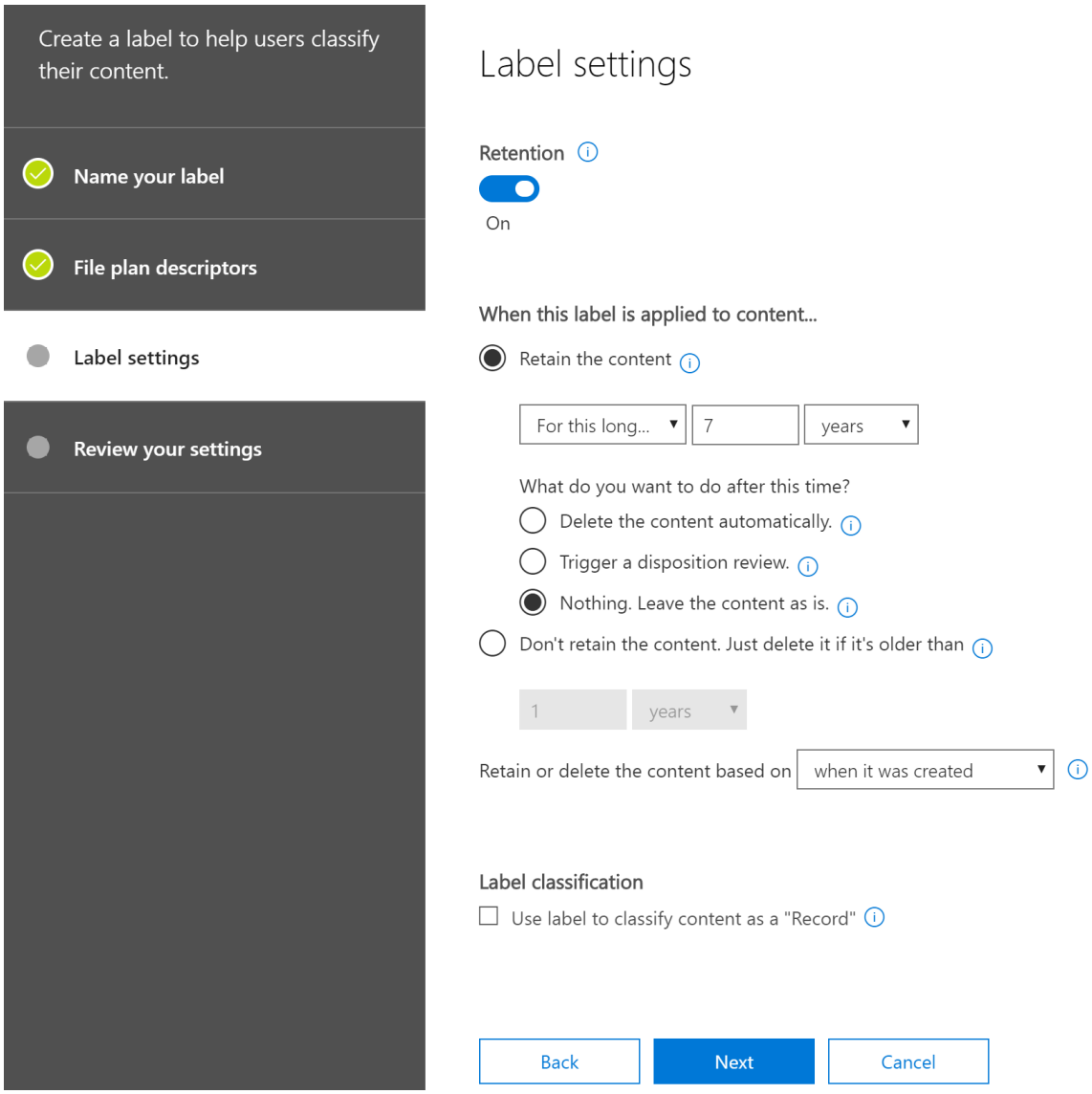
NIST CSF WITH MICROSOFT

Overview & Business Case

Microsoft 365 Solution: Unlimited Archiving, Custom Retention Policies, Litigation Hold

Within the security and compliance center you can turn on email archives and set custom retention policies across exchange, SharePoint, OneDrive, and Teams. Litigation holds can be put on certain users and their activity can be tracked over a specified time.

Ex. Creating a retention label



NIST CSF WITH MICROSOFT

Overview & Business Case

It's likely you already have a standard operating procedure as an MSP for retention. *Incorporate Microsoft Business solutions into your SOP to deliver more value to the customer. Determine the baseline policies that you can turn on in every tenant. Have a HIPPA baseline policy, NIST baseline policy, etc.*

STACK IT UP

This is another great opportunity to layer in a continuity solution like **Dropsuite** for SaaS backup. Dropsuite can backup 365 emails, OneDrive, SharePoint, and even Teams chat messages. This is highly important for your firms that have compliance regulations enforced.

Dropsuite

Business Case: *By default, the retention policy set for deleted mail items in 365 is 30 days. If you do not have a backup provider this data will be permanently deleted. You could set up a retention policy to extends that retention period and even scope the policy to certain type of sensitive data. Retention tags can be created with custom controls to apply at a user level rather than an organizational level.*

Action Items:

- *Ensure you have Office 365 Backup from a 3rd party provider*
- *Define your retention policies across email, documents, and chat.*
- *Define your retention policies for backups*
- *Set custom retention policies depending on the business needs*
- *Align with the HR department at the company to ensure proper management of employee records*

Category(s) Met: PR.IP-4, PR.IP-6, PR.IP-9

Overview & Business Case

Maintenance

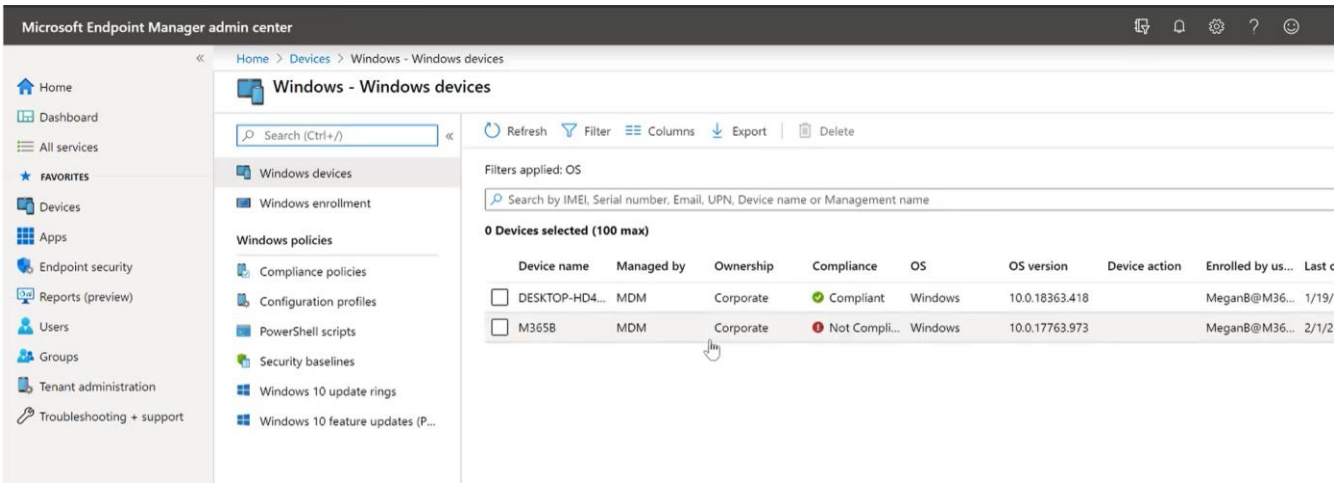
"Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures."

Discovery Questions to Ask (Internal to MSP):

- *How do we track tickets for maintenance and repairs?*
- *Are there any vulnerabilities when maintenance and repairs are going on?*

Microsoft 365 Solution: Intune

PR.MA-1 and PR.MA-2 (the only two subcategories here), refer to the maintenance and repair of "organizational assets". The assets I consider in scope here are devices managed by Intune and on-prem infrastructure if you are running a hybrid environment. If you are an established MSP, you most likely have a ticketing system where you would be tracking such information. You can create alerts in M365 to report when a device is in an uncompliant state. I would suggest, creating a ticket off this alert to track your interaction in getting it back to a healthy state. For on-prem infrastructure, the same is true any time you are making configuration changes or repairs to Azure AD Connect.



Overview & Business Case

Action Items:

- *Review your process around remoting into devices that you perform maintenance on and try to identify any vulnerabilities*
- *Ensure techs are opening tickets to solve issues when devices in Intune fall out of compliance.*



DETECT

"Develop and implement appropriate activities to identify the occurrence of a cybersecurity event."

Anomalies and Events

"Anomalous activity is detected in a timely manner and the potential impact of events is understood."

Discovery Questions to Ask (Internal to MSP):

- *What is our average response time on threats that are detected?*
- *What kind of reporting do we get on targeted attacks and methods used?*
- *What are all of our data points for security detection? (Microsoft, 3rd party AV, etc)*
- *Does the customer understand impacts of a breach?*
- *What alerts do we have in place for high level threats? Are these automated to create a ticket in our ticketing system?*

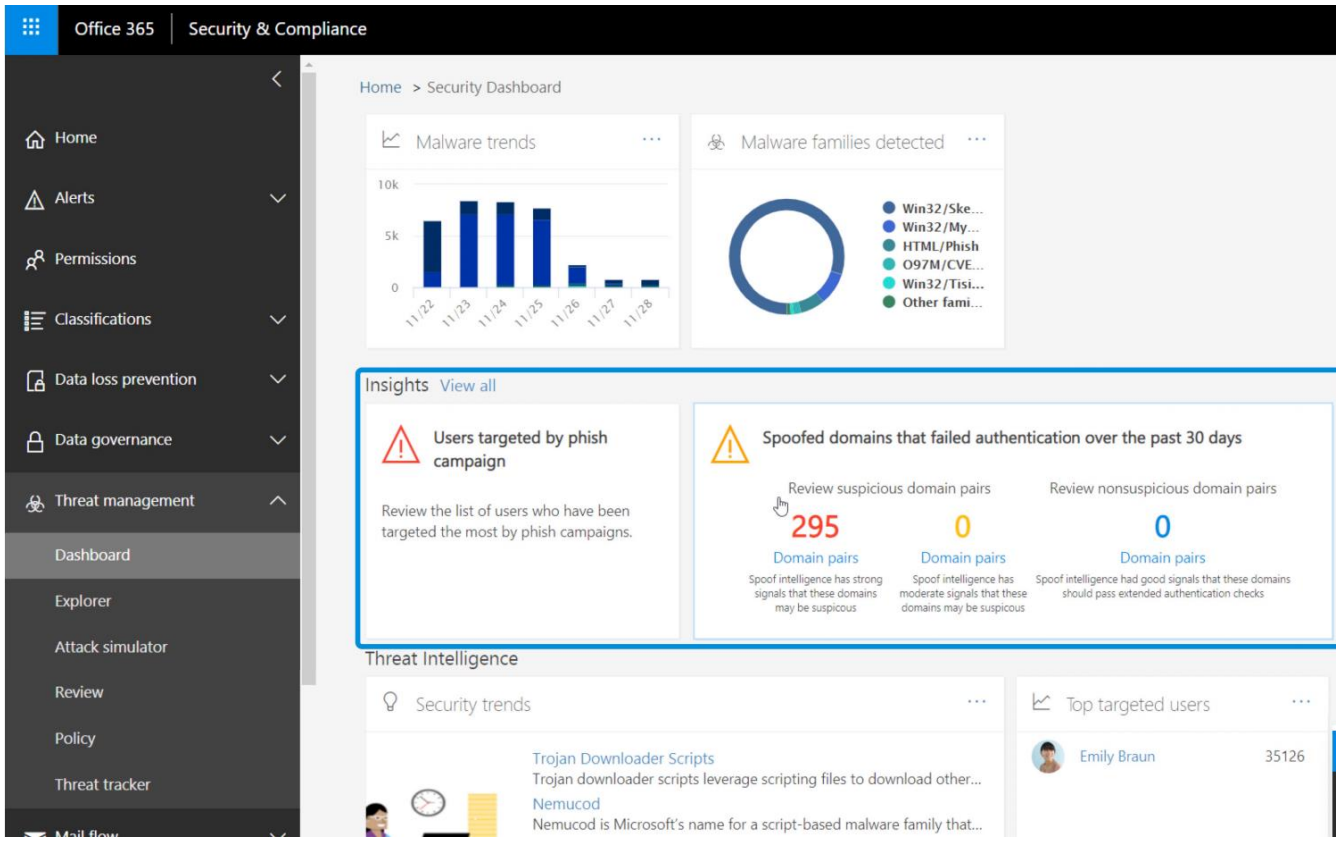
Microsoft 365 Solution: Security Center, Advanced Threat Protection, Data Loss Prevention

The Microsoft Security Graph, collects and analyzes an estimated 6.5 trillion signals per data from user sign-ins, device endpoints, email messages, documents, cloud applications, and Azure public cloud. This allows them to collect a ton of data that could be malicious to the end users and enhance their vulnerability detection capabilities. Microsoft's average malware catch rate for Office 365 email is the highest in the industry at 99.9% and they have the lowest miss rate of phishing emails for Office 365. Office 365 ATP blocked 5 billion phish emails in 2018 alone. Additionally, you can set up triggers for data loss prevention policies, malware detections, conditional access policies met, and more to be

Overview & Business Case

proactive in your response times. Showing these statistics to you customer in a monthly report can show them how much value you are providing.

Security Center is your central dashboard for tenant reporting and policy management for anti-phishing, anti-spam, anti-malware, data loss prevention, safe links, safe attachments, and more. This is a single view to see all the anomalies and events detected in certain time frames.

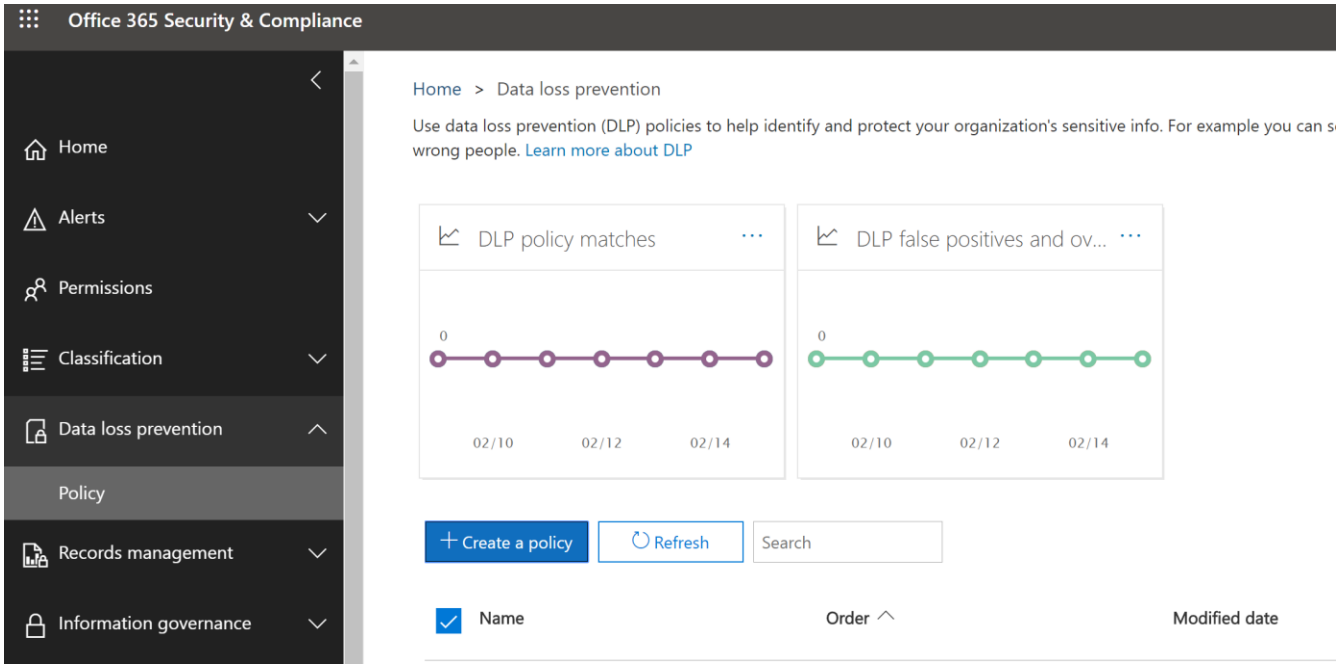


Advanced threat protection allows you to create policies for safe links, safe attachments, anti-spoofing, anti-phishing, anti-spam, and anti-malware. You can additionally configure DKIM and DMARC to authenticate mail senders and ensure that destination email systems trust messages sent from your domain. Enhanced email filtering can be set up if you have a connector in 365 (3rd party email filtering service or hybrid configuration) and your MX record does not point to Office 365. This new feature allows you to filter email based on the actual source of messages that arrive over the connector. This is also known as skip listing and this feature will allow you to overlook, or skip, any IP addresses that are

Overview & Business Case

considered internal to you in order to get the last known external IP address, which should be the actual source IP address. If you are using Office 365 ATP, this will enhance its machine learning capabilities and security around safe links/safe attachments/anti-spoofing from Microsoft's known malicious list based off IP. In a way, you are getting a secondary layer of protection by allowing Microsoft to view the IPs of the original email and check against their database

Data loss prevention policies allow us to automatically detect sensitive information across Exchange, SharePoint, OneDrive, and Teams and apply restrictive controls on what actions are taken. Events such as a user trying to send a document with a social security number outside the organization can be blocked or relayed to an admin for quicker response time on remediation if there is a breach.



Business Case: *You use a 3rd party AV/AS provider like Webroot or Proofpoint and you want to bundle in ATP from Microsoft. You want to fully leverage Microsoft's Security Graph and machine learning capabilities from the messages that are relayed to Office 365 from the connector you set up. You can configure enhanced filtering to get skip listing functionality you need to enhance the detection capabilities.*

Overview & Business Case

Action Items:

- *Review the Threat Management Dashboard in all customer tenants. See if there are any trends that you should take action on. These actions would include setting up more restrictive policies or setting up new alerts to decrease average response time.*
- *Send reports of information such as email sent/received, malware prevented, safe links/safe attachments quarantined, impersonation attempts, and spoofed domains.*
- *Set up a Policy for ATP Safe Links and Safe Attachments*
- *Set up a policy for Anti-phishing*
- *If you are using a 3rd party provider for Anti-virus protection like Webroot or Proofpoint, set up enhanced filtering*
- *Implement DMARC and DKIM*
- *Configure a DLP policy in the Security Center to protect sensitive data*

Category(s) Met: DE.AE-2, DE.AE-3, DE.AE-5

Security Continuous Monitoring

Description: "The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures."

Discovery Questions to Ask (Internal to MSP):

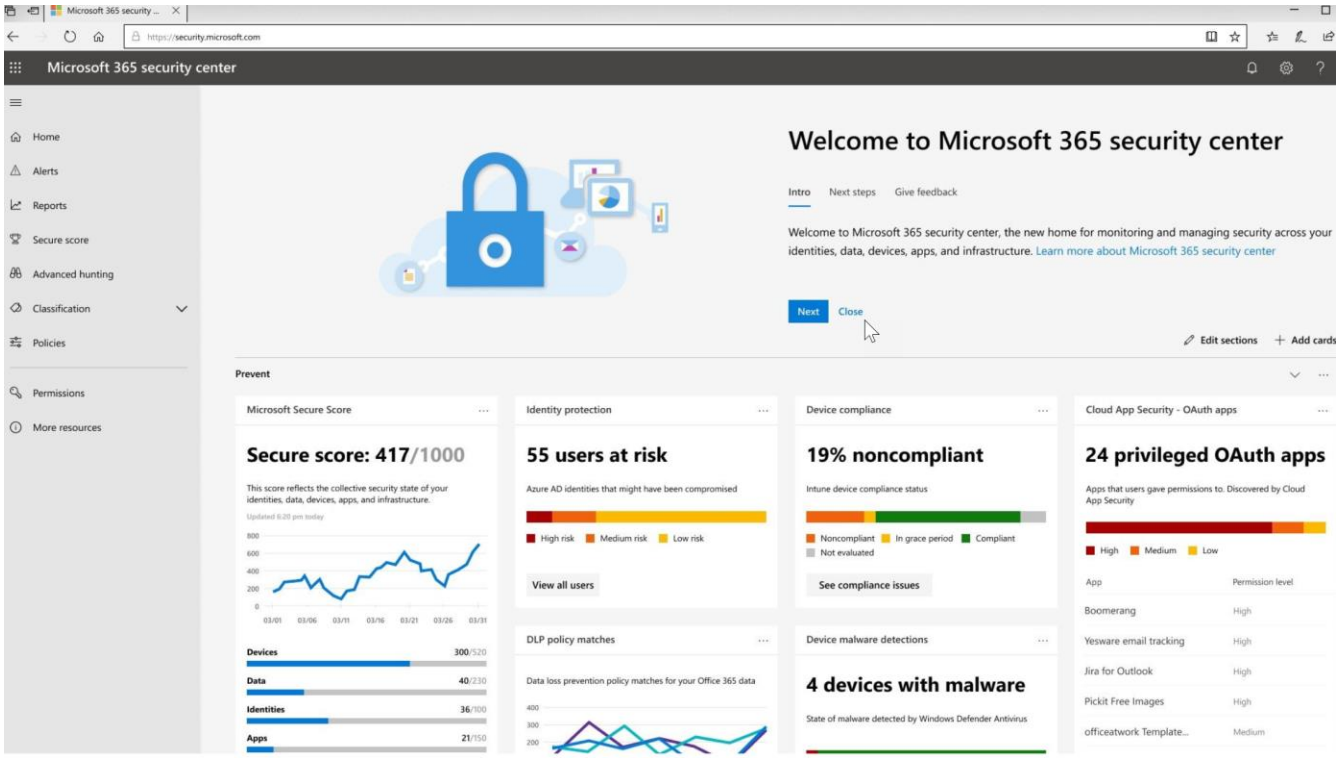
- *How is our network being monitored?*
- *How often do we review data analytics of threats identified?*
- *Are there any policies we should modify?*
- *How do external users access resources at the company?*

NIST CSF WITH MICROSOFT

Overview & Business Case

Microsoft 365 Solution: Security Center, Intune

In the security center, Microsoft give you near real-time reports on many different security events that they are tracking such as malware, phishing, spoofing, data loss triggers, and more. These insights allow you to proactively set up policies and triggers that you can continually refine if needed.



Intune allows you to monitor device health based on compliance policies that you set up. The compliance policies include things like password requirements, requirements of an AV present, requirement of Bitlocker, etc. You can monitor all devices, both corporate and BYOD, in the Endpoint Manager portal.

NIST CSF WITH MICROSOFT

Overview & Business Case

Business Case: *As an MSP, you do not have a periodic basis in which you review security trends in customer tenants. By reviewing the threat management dashboard on a monthly basis you realize you have customers that need more restrictive policies for phishing because there are users being continuously attacked.*

Action Items:

- *Review the Threat Management Dashboard in all customer tenants. See if there are any trends that you should take action on. These actions would include setting up more restrictive policies or setting up new alerts to decrease average response time.*
- *Send reports of information such as email sent/received, malware prevented, safe links/safe attachments quarantined, impersonation attempts, and spoofed domains.*

Category(s) Met: DE.CM-4, DE.CM-5, CM-7

Detection Processes

Description: "Detection processes and procedures are maintained and tested to ensure awareness of anomalous events."

Discovery Questions to Ask (Internal to MSP):

- *Are roles and responsibilities for detection of events defined at your company?*
- *How does the customer communicate those events to you?*
- *Have you tested your detection processes that are in place across your security stack?*
- *How is event detection communicated to the end users at the company?*
- *How often do you review your detection process with the customer?*

Overview & Business Case

Microsoft 365 Solution: Security Center

In security center, we can set up alerts and triggers for when certain events or anomalies are detected if you feel like they are high importance. Reviewing the threat management dashboard should be part of your detection process and should be periodically reviewed. Microsoft incorporates a mentality of "Assumed Breach" which we recommend you adopt as well to define the best detection processes.

Business Case: *You are starting to see your customers at XYZ Corporation engage you about certain events over email, phone, texting, and your internal chat tool. You begin to realize these request are getting every hard to track and everyone in your company responds to them in an ad hoc function with no definition of who owns what task.*

Action Items:

- *Make sure your event detection process is clearly defined and communicated with the company*
- *Review your event detection processes quarterly to see if there are things you can improve on*
- *Incorporate the threat management dashboard as part of your event detection process.*

Overview & Business Case



RESPOND

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Response Planning

"Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events."

Discovery Questions to Ask (Internal to MSP):

- *How do we triage incidents that come through from our customers?*
- *What are our SLAs for certain types of incidents?*

Microsoft Solution

The security center in Microsoft can give you deeper insight into trends going on with an organization so you can be more proactive about what kind of threats may come up with an organization. If you fully utilize Microsoft's solution stack many of these incidents will have been quarantined immediately so the likelihood of this incident being a high security risk is vastly reduced and will give you more time to remediate issues.

***Business Case**: A conditional access policy is triggered because a user's device is detected with malware, bringing it to an unhealthy state and preventing access to company resources. You can now effectively communicate this to the end user and work on getting the device back to a compliant state. Planning improves because you are not under as many pressures of corporate data being breached.*

Action Items:

- *Review how you triage tickets into the company and see if you can improve efficiencies*
- *Proactively review trends in the threat protection dashboard on a periodic basis to get a better idea of what threats may emerge*

Overview & Business Case

Communications

Description: "Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies)."

Discovery Questions to Ask (Internal to MSP):

- *Are roles and responsibilities defined when an incident occurs both internally and with the customer?*
- *When an incident is reported, has it been done so in a manner that meets the criteria I've established with the customer?*
- *Are we consistent with how we respond when a customer opens a ticket?*
- *Are all employees trained on how to communicate when they detect a threat?*

Microsoft 365 Solution: Advanced Threat Protection

ATP allows users to self-report emails when they detect certain malware or phishing attempts. Collectively this help improve the security posture of the organization outside of your controls and Microsoft's detections

Business Case: *A user see's an email from a sender they do not recognize asking them to click on a link for an Amazon gift card. The user reports this email from their outlook client for the admin to review for phishing.*

Action Items:

- *Make sure roles and responsibilities are clearly defined and communicated for an incident*
- *Review ticket correspondence and ensure consistent messaging and procedures are enforced*
- *Turn on Report Message add-in for outlook in the Security Center*
- *Review the user submitted reports on a periodic basis*

Overview & Business Case

Analysis

Description: “Analysis is conducted to ensure adequate response and support recovery activities.”

Discovery Questions:

- *Do you have categories of incidents with predefined response plans?*
- *If we were to get audited, can we easily provide documentation of how we responded to an incident and the outcomes?*
- *Can we easily identify the impact of certain issues? If not, what controls can we put in place to better protect ourselves from those types of incidents?*

Action Items:

- *Review how Microsoft’s solution fits in your security stack. Classify incidents based on severity and periodically review with changing security landscape*

Mitigation

Description: “Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.”

Discovery Questions:

- *Are newly identified vulnerabilities documented and assigned a risk category?*
- *Do we define how to contain incidents as part of our category definitions?*

Microsoft 365 Solution:

As the security landscape evolves, we can look to Microsoft to provide insights on new emerging threats because of all the data they gather from the Security Graph. We should take these new threats and have a formal method of how we document them and assign a risk category.

NIST CSF WITH MICROSOFT

Overview & Business Case

Business Case: *During recent weeks, an increase in OAuth phishing attacks has been spotted. There have been a lot of reports about OAuth phishing attacks where an attacker is given access to a user's account and is secretly extracting all the data without the user's knowledge. This is a new type of attack that needs to be reviewed and documented internally at your organization.*

Action Items:

- *Review your process for how you document new vulnerabilities and threats that emerge in the companies you manage*
- *Ensure that you have a column to define how to contain each incident that can occur*

Improvements

Description: "Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities"

Discovery Questions:

- *Does your organization ever do a retroactive meeting internally and at the customer site for certain incidents or breaches?*
- *How do you document new things you have learned from previous incidents?*
- *Do new users to your company have easy access to this information if they search for it?*

Actions:

- *Start conducting retro meetings internally for larger incidents if you are not already and document steps you are going to take to avoid faults in the future*

NIST CSF WITH MICROSOFT

Overview & Business Case

RECOVER

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

**NOTE* In this section we are not going to be talking about the M365 Business solution as this relates primarily to Backup/Disaster Recovery Scenarios*

STACK IT UP

This is another great opportunity to layer in a continuity solution like Dropsuite for SaaS backup. Dropsuite can backup 365 emails, OneDrive, SharePoint, and even Teams chat messages. This is highly important for your firms that have compliance regulations enforced.

Recovery Planning

Description: "Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents"

Improvements

Description: "Recovery planning and processes are improved by incorporating lessons learned into future activities."

Communications

Description: "Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors)."

Overview & Business Case

Discovery Questions to Ask (Internal to MSP):

- *Do we have a SaaS backup solution in place? What solutions should we be backing up?*
- *What RPO or RTO metrics do we want to meet?*
- *If we were to lose customer data, what messaging do we want to provide?*

Action Items:

- *Review your policies around backups and how long they are retained after a user leaves the organization*

NEXT STEPS

We hope this guide has provided you some guidance on mapping Microsoft 365 Business solutions to NIST Cybersecurity framework and brought some considerations around your existing cybersecurity policies. Understanding these solutions should help you navigate the conversations with your customer on upgrading them to the M365 Business solution. Here are some targeted next steps:

Start with Compliance!

The upsell of these solutions needs to focus on compliance. Almost every organization is accessing/sharing data in an insecure manner. Asking customers about data loss to personal cell phones is very eye-opening whether or not they fall under compliance regulations. Help customers understand where they are exposed and evaluate the cost of a breach or data loss. For businesses under compliance regulations, this becomes even more of an importance from the standpoint of an audit or violations due to a data breach.

Overview & Business Case

Implement Intune and Conditional Access

While there are a ton of great solutions in the Microsoft 365 stack, we want to focus on the most impactful solutions for the cost of implementation. Paint with a broad brush. Intune's mobile application management policies can immediately protect all corporate data on mobile devices which is a massive security risk existing today. These policies do not require the device to be enrolled in the MDM solution. Users will just get prompts to use a managed app like outlook to access data. With this in place, you can monitor, encrypt, and remotely wipe corporate data.

Conditional Access allows us to be IT Heroes because we are allowing access to data and applications in a secure manner without inhibiting productivity. Create custom policies that cover security holes in today's workplace. Evaluate most critical applications based on business data and create policies that protect that data both on and off your network.

Review your Cybersecurity Policies

As we mentioned in the executive summary of this guide, it would be highly beneficial to review your existing cybersecurity policies, risk management/mitigation policies, vulnerability assessments, and overall business practices with the recommendations outlined here. Whether you are just starting out as an MSP or have been in business for many years, we think it's always good to periodically review the policies and procedures that you have in place. If you find you do not have policies clearly defined, make this your top priority.

Overview & Business Case

Phased Rollout of Solutions

If you do upsell your customer to Microsoft 365 Business, it doesn't make sense to rollout all solutions in the stack at one time. It would be incredibly taxing to your internal staff and you will reduce employee adoption/compliance. Follow the method of least to most restrictive for the policies you create and ALWAYS test solutions with a pilot group of users. Here is a good way to line this up:

1. Evaluate the solution and compare it to the business practices at the company
2. Define least to most restrictive policies to create
3. Define the scope of users, groups, devices, applications that the policies would be applied to
4. Rollout the policy to pilot users (champions of the organization)
5. Gather their feedback and adjust accordingly
6. Create a communication plan on broad deployment. Clearly define expectations
7. Perform a broad deployment release and gather feedback
8. Refine the policies or refine documentation for the company
9. Move on to the next solution

This is a great way to project manage the solutions to your customers, understand and maximize your own internal bandwidth for implementation, and create documentation that you can use as a template for every one of your customers. Over time you should have baseline policies that you apply to every company and the feedback you get on improvements should reduce with each iteration.

NIST CSF WITH MICROSOFT

Overview & Business Case

REFERENCES

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1

National Institute of Standards and Technology

April 16, 2018

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

FedRAMP Security Assessment Framework v2.4

FedRAMP

November 15, 2017

https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf