2020



CIS CONTROLS WITH MICROSOFT 365

BUSINESS CASE AND OVERVIEW

NICK ROSS, MICROSOFT CERTIFIED EXPERT ADMINISTRATOR

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

PURPOSE

This document is a guide for mapping Microsoft 365 Business Premium solutions to the Center for Internet Security (CIS) Controls™. It is meant to help define the starting point for your defenses, direct scarce resources towards actions with immediate and high-value payoff, and then focus your attention and resources on additional risk issues that are unique to the business or mission.

Offense Informs Defense: Continually learn from knowledge of actual attacks that have compromised systems to provide a foundation for building effective, practical defenses.

Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment.

Measurements and Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to quantify the effectiveness of security measures within an organization so that required adjustments can be quickly identified and implemented.

Continuous Diagnostics and Mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures and to help prioritize next steps.

Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

AUDIENCE

This guide was written for Managed service providers (MSPs), but can be used by other parties to assess the Microsoft 365 Business solution with CIS Controls.

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

EXECUTIVE SUMMARY

For years, IT professionals have provided a variety of technology services to small-to-midsized businesses (SMBs) across the globe. Many started as break/fix shops before moving into managed services. Some Managed service providers (MSPs) have partnered with Managed Security Service Providers (MSSPs) to offer a heightened security and compliance solution. Others have simply decided to take on the challenge of providing these services themselves, or have partnered with internal IT at local businesses to offer a co-managed solution.

An evolution is taking place in which the IT professional is now being viewed as the trusted business advisor for the SMB market. New technologies have positioned IT providers with a great opportunity to guide these businesses as they grow. Additionally, the technological shift to the cloud has changed the way people work, while the attack surface for threats is greater than ever. SMBs look to their IT providers to ensure they are protected against new threats. MSPs, attorneys, regulators, CIOs, CISOs, and business managers can all agree that perfect cybersecurity is not possible. Keeping up with the ever-changing threat landscape is difficult when multiple business priorities are competing for limited resources, such as time, money, or expertise. Differing business models make it hard to implement a cybersecurity standard across all clients and the mission-critical assets they need to protect.

Growing Threats

According to the World Economic Forum's Global Risks Report 2020, cyberattacks are the second most concerning risk for global business over the next 10 years. The decentralization of corporate networks, the explosion of third-party SaaS applications, and the evolution of bring-your-own-device (BYOD) policies have made IT providers question where to turn to secure the organizations that rely on their advice. Additionally, new technologies such as Internet of Things (IoT) devices and Artificial Intelligence (AI) are in the infancy stage while creating further exposure to cybersecurity risk.

"The Fog of More"

Whether you are a one-man shop or an MSP with one hundred employees, the wide range of cybersecurity frameworks and tools marketed to you can be confusing. IT professionals have more access than ever to forums, security software, training, vulnerability databases, security checklists, certifications, and assessments. In addition, there are ever-evolving compliance requirements that must be kept up with to ensure the solutions you give to your clients meet industry standards. The "fog of more" is a term used by cybersecurity professionals to describe this landscape of "competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action". *Note: the term enterprise is used here but it can be extended to SMBs, especially with all the client*

OVERVIEW & BUSINESS CASE

verticals that MSPs maintain. In many cases, due to all the available resources, IT professionals end up putting in more security controls, and then get blamed for inhibiting productivity.

Introduction to CIS Controls

The Center for Internet Security (CIS) Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls were developed by a community of IT experts who applied their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who developed the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others. This community continues to update the Controls over time. Prioritization is a key benefit to the CIS Controls. They were designed to help organizations rapidly define the starting point for their defenses, direct their scarce resources towards actions with immediate and high-value payoff, and then focus their attention and resources on additional risk issues unique to their business or mission.[1]

Microsoft 365 Business

Traditionally, IT professionals have been vendor-agnostic across their solution stack except for Active Directory. MSPs have been using Microsoft's solution for Active Directory for years and many have now extended those identities to the cloud. It is usually the very first vendor an MSP integrates when acquiring a new client. Bolting on third party solutions to enhance the offering and improve efficiencies is usually a secondary priority. When thinking about the CIS Controls and high-value payoff actions, focusing your attention around Microsoft makes sense. Microsoft 365 Business comes with many solutions that address the shifting technology landscape and can greatly improve an organization's security posture in a short amount of time. In this guide, we will map the M365 Business solutions to each of the 20 CIS Control and give you tips to recognize risk within an organization.

Investor Considerations

The main goal for most business owners to ultimately sell to another company or grow large enough to acquire investment money to continue to expand. This is true both for the MSP and the small business owner. SMBs are looking for a grounded security practice to make them more attractive to investors. Nearly 90% of SMBs would consider hiring a new managed services provider if they offered the right cybersecurity solution, and nearly half would pay at least 20% more for the right security solution from a new MSP.[2] Private investors are looking for concrete information demonstrating that risk is being minimized throughout the company and cybersecurity is high on their watchlist. If you are a larger MSP looking to acquire another, you should weigh their existing cybersecurity policies and procedures heavily in your valuation.

OVERVIEW & BUSINESS CASE

HOW THIS GUIDE IS STRUCTURED

Each section of this guide will cover one of the CIS Controls and show you which solution in the M365 Business stack meets the sub-controls available. We will provide questions that help you evaluate the risk for that Control with your client and offer safeguards from the Microsoft 365 Business solution that solves for that risk.

Risk Assessments

When performing a risk assessment with your clients, it's essential to have a consistent and repeatable method for estimating and evaluating risk. The language around the risk assessment should be universally understandable to all levels of knowledge around cybersecurity, whether you are talking to a novice or an expert. This allows you to use the same template across all clients and avoid rework.

Clearly defining "acceptable" and "unacceptable" risk across the organizations is important when performing a risk assessment. Impacts to the client's mission and obligations to various stakeholders will help better assess what is an acceptable risk. Defining acceptable and unacceptable risk will help you prioritize the M365 solutions you want to implement and help you garner more insight into potential upsell opportunities. We offer questions you should be asking your clients to help define risk in each section of this guide, as well as recommended safeguards.

Risk Assessment Criteria

The criteria you set for calculating risk should provide your client with a consistent method for rating the likelihood and impact of foreseeable threats that may comprise the security of information assets across the organization. Criteria definitions must include levels of impact and likelihoods that are meaningful to a client's business. The solutions we outline across the M365 stack will be consistent across many verticals, but the levels of acceptable and unacceptable risk will ultimately be defined by collaborating with the company.

For each Control in this guide, we will offer discovery questions you can ask your client to mutually understand the impacts of risk within their organization. Defining a risk score for each threat with help you better prioritize the solutions you want to implement. A formula you can use from the CIS Risk Assessment Method (RAM) v.1.0[3] is:

Risk = Max (Mission Impact, Obligations Impact) x Likelihood

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

This formula will be used to define a risk score for each threat we identify within each CIS Control, helping you:

1. Define the acceptable and unacceptable impacts to the company's mission and obligations
2. Determine the likelihood of the event
3. Prioritize solutions
4. Define the policies and controls to be put in place with the M365 Solution

DEFINING ACCEPTABLE RISK

We will first define an acceptable risk score based on the likelihood of the threat and unacceptable impact to the organization. *Note: The CIS Risk Assessment Method (RAM) has another model based on the NIST Cybersecurity Framework with an additional column for Impact to Objectives. We recommend using this additional column for organizations that have a more mature cybersecurity practice.*

Threat Likelihood Score	Likelihood Score Definition
1	Not foreseeable
2	Foreseeable
3	Expected
4	Common
5	Current

OVERVIEW & BUSINESS CASE

Impact Score	Impact to Mission	Impact to Obligations
	Define the organization's mission.	Define the organization's information security obligations to prevent harm to others.
1. Acceptable	Describe a scenario in which consequences would be acceptable to all parties.	Describe a scenario in which consequences would be acceptable to outside parties who could be harmed.
2. Unacceptable	Describe a scenario in which consequences would be unacceptable to all parties but would be recoverable with some effort.	Describe a scenario in which consequences would be unacceptable to others, but would be recoverable with some effort.
3. Catastrophic	Describe a scenario that could not be recovered from.	Describe a scenario that others could not recover from.

As an example, let's take a look at a common event in today's landscape: corporate data being leaked to unmanaged devices such as personal laptops. In this example we are working with a financial firm. Multiplying the likelihood (3) by the unacceptable impact score (2) will create an acceptable risk of 6. We chose a default unacceptable impact score of 2 because we must reduce risk that **creates intolerable impacts** to the organization.

- Threat: Data Loss to Personal Device
- Likelihood Score: 3
- Impact Score: 2 (Unacceptable)

Acceptable Risk
< 6

OVERVIEW & BUSINESS CASE

CALCULATING OBSERVED RISK

Now the client should follow the chart below to understand the possible impacts to their mission and obligations. Having them select an impact score will help them understand the importance of the solution. The chosen impact score should be based on the likelihood of the event.

Ex.

Impact Score	Impact to Mission	Impact to Obligations
	We need to protect consumer PII and grant access to data in a secure manner.	Our customers require that we protect all their data and understand we are using best security practices.
1	We are able to perform work-related tasks on personal devices, but the applications are managed by our company.	Company data on personal devices is accessed on a managed app for which we have the ability to wipe data.
2	Employees are accessing corporate data with PII on their personal laptops in unmanaged applications.	Company data is leaked to a personally managed device for which we do not have the ability to wipe data if the employee leaves. This leaves client data exposed.
3	We have no way of controlling or knowing what PII is leaked to personal devices.	Client data is leaked onto an unmanaged device that is stolen. We are liable for financial and legal implications.

Based on the definitions, the client selects 2 for mission impact and 3 for obligation impact. We now use our formula from earlier to calculate the observed risk score:



OVERVIEW & BUSINESS CASE

Now compare the calculated observed risk to the defined acceptable risk to determine if the level of risk is acceptable:

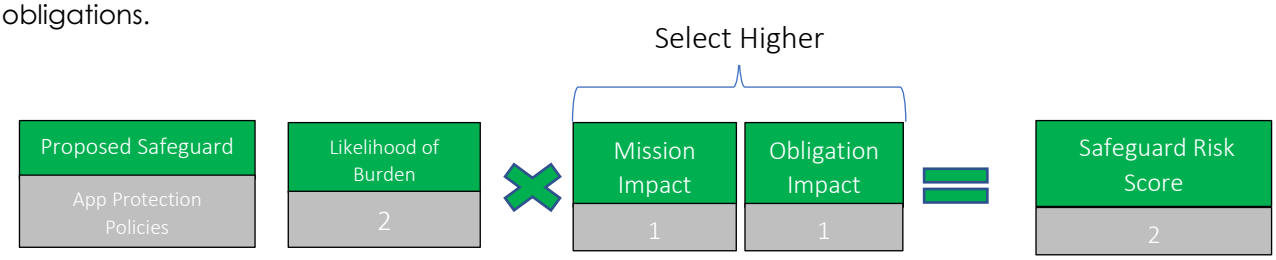
Acceptable Risk: < 6

Observed Risk: 9

Risk Acceptability: Not Acceptable

PROPOSING SAFEGUARDS

Laws and regulations require that organizations apply "reasonable" and "appropriate" safeguards to ensure that the resulting risk is acceptable[4]. You will want to evaluate the likelihood of the burden to the company just as equally as you would evaluate the threat. This will help you define the granularity of the policies you implement. This will also help you understand the impacts to the client's mission and obligations.



In our example of a proposed safeguard, we are implementing app protection policies which restrict the ability to save corporate data on unmanaged applications. How is this going to burden the company? We know that they will have some frustrations about having to use managed apps, but does it inhibit their ability to do business? Do they have obligations to clients that they wouldn't be able to meet because of these new safeguards?

We suggest following this format for each CIS Control. By assessing risk to a proposed safeguard, IT professionals can benefit from:

1. Demonstrating to business leaders how recommended security safeguards can be implemented without creating too much of a burden on the business mission.
2. Demonstrating to regulators and other legal authorities that safeguards are reasonable because the risk of the safeguard (i.e. the "burden" to the organization) is not greater than the risk that it is meant to reduce.
3. Demonstrating that recommended safeguards would be appropriate by showing that they would not foreseeably create an impact that would be intolerable to the client.

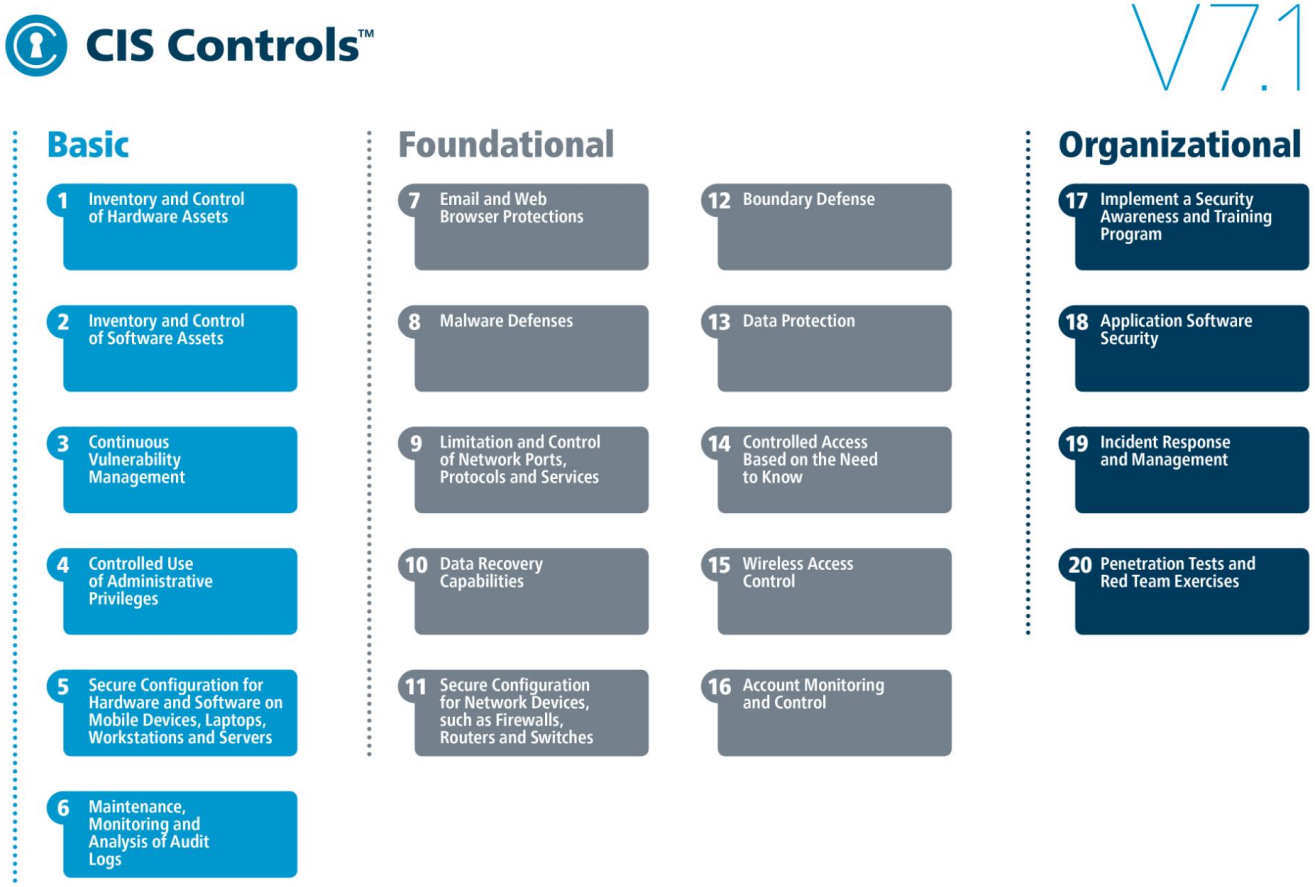
OVERVIEW & BUSINESS CASE

DISCLAIMER

The partner and client 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.

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE



CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 1: INVENTORY AND CONTROL OF HARDWARE ASSETS



Description: *"Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access."*

Discovery Questions:

- How are users accessing resources today? On what devices?
- Do users access data on their personal devices?
- Is important company data being accessed on personal devices?
- How do you protect that data if that device is lost or stolen?
- How do you prevent infected devices from joining your network?

Overview:

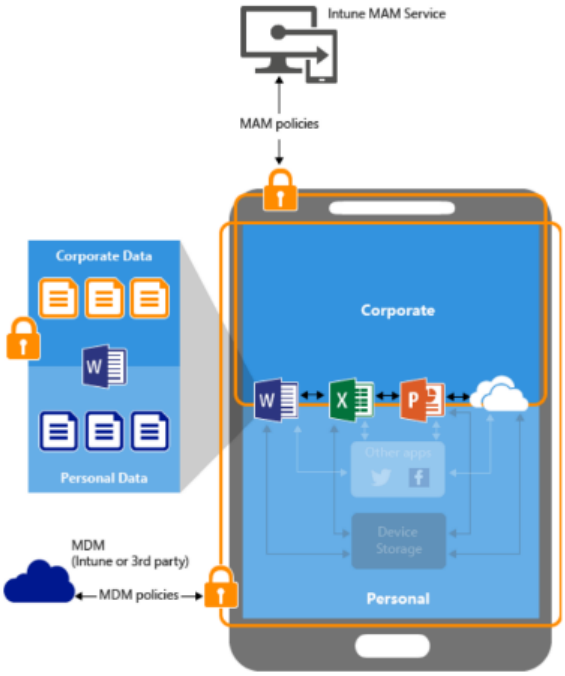
Digital transformation has changed the way people work and how companies do business – the workforce is beginning to expect the ability to work remotely, on any device, while accessing all their resources. The idea of a "trusted" perimeter network is gone. Attackers are constantly scanning the address space of targeted organizations and waiting for unprotected systems to be attached to the network. Unmanaged personal laptops and cell phones used in Bring-Your-Own-Device (BYOD) models are of particular interest to attackers. These devices are more susceptible to compromise because the organization has no control over patch updates, security configurations, and threat protection software. If a device is compromised off-network, an attacker can enter an organization once the device rejoins. Companies need a zero-trust model for gating access to resources based on user and device health, rather than being on-network.

OVERVIEW & BUSINESS CASE

MICROSOFT 365 SOLUTIONS: INTUNE AND CONDITIONAL ACCESS

Intune

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. By joining a device to Azure AD and Intune, you can centrally push down policies, configuration profiles, and applications to that device. The policies you set determine if the device is in a "healthy state". By creating policies around applications that contain corporate data, you can protect that data even on unmanaged devices such as personal cell phones. This protection includes controls on restricting "save as" and "cut/copy/paste" permissions.

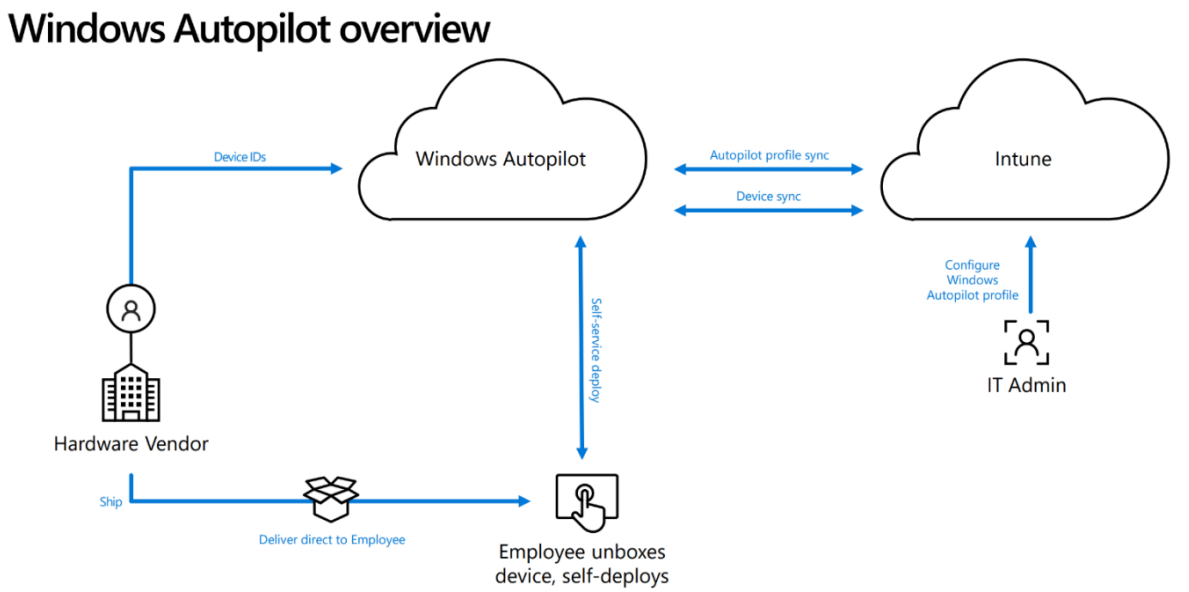


Windows Autopilot

Windows Autopilot is Microsoft's new solution for managing the lifecycle of Windows 10 devices. Traditionally, IT pros spend a lot of time building and customizing images that will later be deployed to devices. In most deployments, you also need to update driver information, install your RMM software, configure VPN settings, join the device to a local domain, and install client specific apps. This cumbersome and time-consuming process is now simplified with Windows Autopilot. When initially deploying new Windows devices, Windows Autopilot leverages the Original Equipment Manufacturer (OEM) optimized version of Windows 10 that is pre-installed on the device, saving organizations the effort of having to maintain custom images and drivers for every device model being used. Instead of re-imaging the device, your existing Windows 10 installation can be transformed into a "business-ready" state, applying settings and policies, installing apps and your RMM software, and even pushing VPN profiles. You can also use Windows Autopilot reset to repurpose and recover the device.

Microsoft is working with top OEM providers like Dell, HP, and Lenovo that provide a list of hardware IDs you can upload into the Windows Autopilot service when you order new devices. This allows you to centrally manage the device and ship them directly to the client. Inventory management is simplified because you can track the lifecycle of the device within the Microsoft Endpoint Manager admin center.

OVERVIEW & BUSINESS CASE



Hybrid Deployment

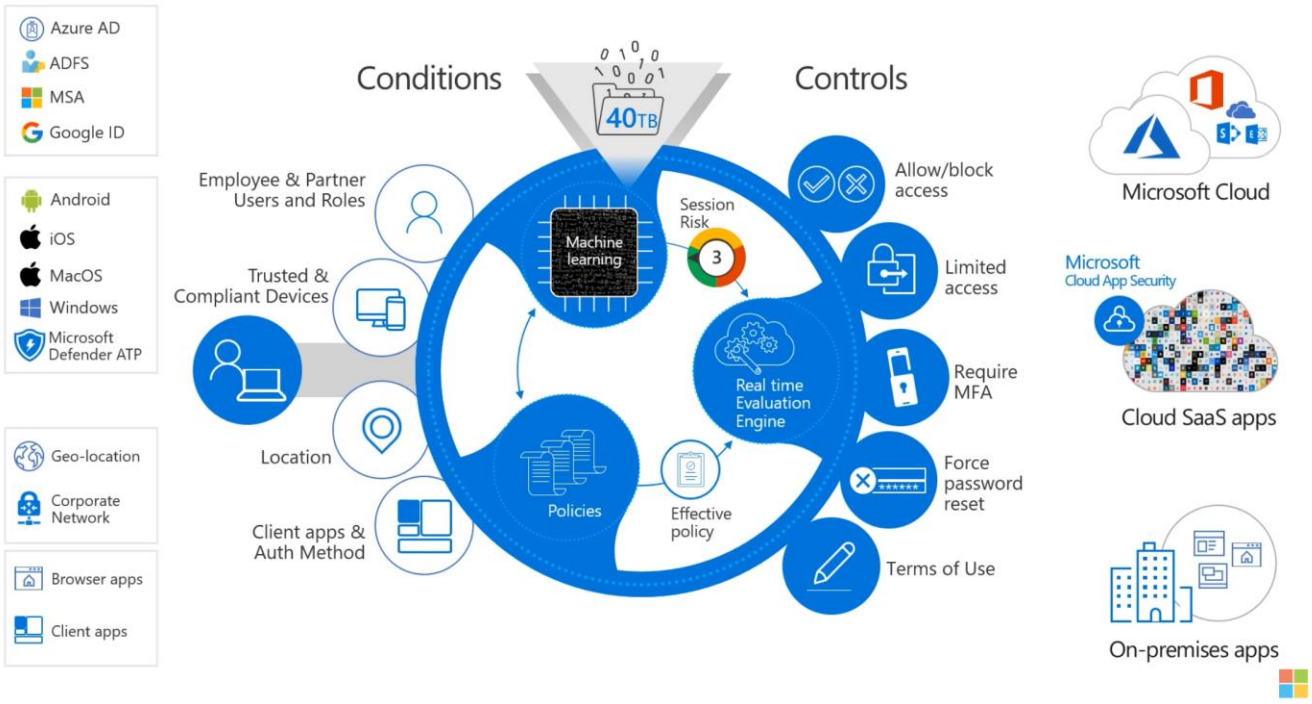
Many clients have CapEx tied up with existing infrastructure. Most notably, this includes an on-premise domain controller for Active Directory. Beyond these existing expenditures, there are many group policies (GPOs), file shares, security settings, printers, and more that make moving to a full cloud deployment illogical. You can configure Intune and Windows Autopilot for a hybrid deployment of device management. With Windows Autopilot hybrid join, you can push a device down to your local domain, applying legacy GPOs when the device is booted. This allows you to transition to full cloud management over time and take advantage of the application management policies available with Intune.

Conditional Access

Conditional Access is Microsoft's new identity solution for granting access to resources within the organization. When you create a policy, you define certain conditions that are met to enforce certain controls. An example would be a policy you create that grants access to the Office suite when a user is off your network, but requires their device to be enrolled in your MDM solution and also requires them to use MFA. These policies can get as granular as you would like and can be customized to every application the organization uses.

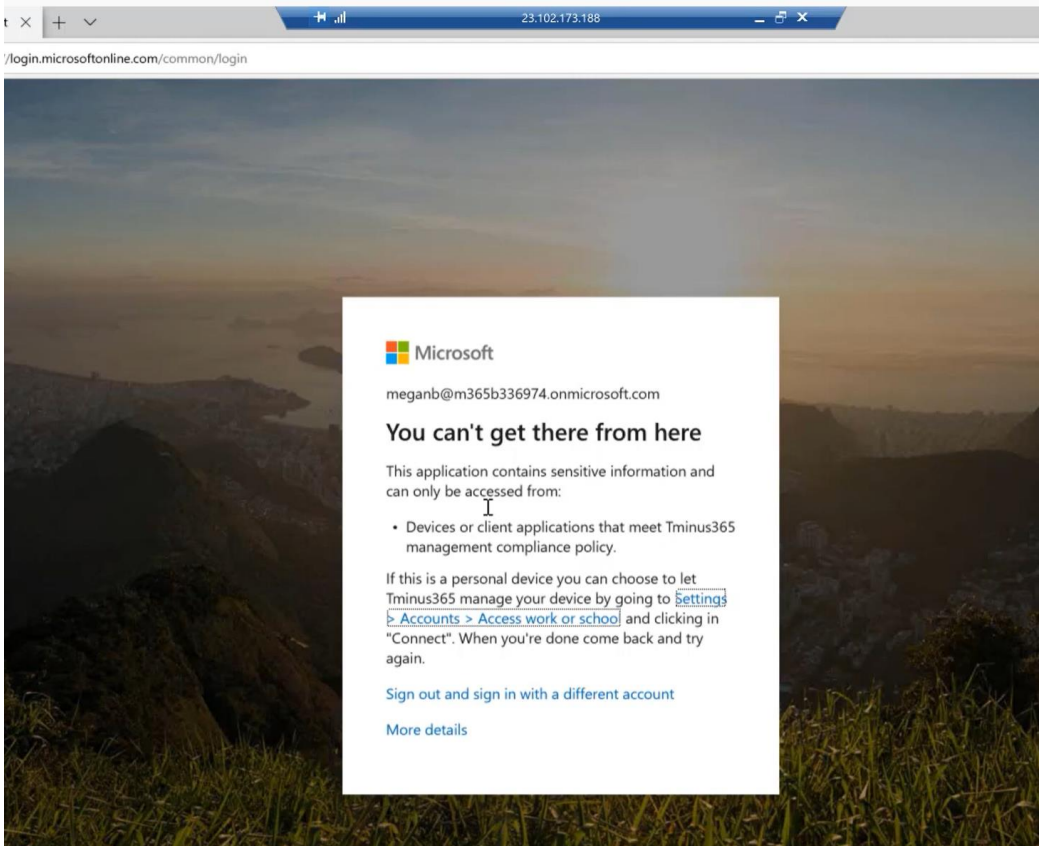
CIS CONTROLS WITH MICROSOFT

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



Risk Analysis

Observed Risk:

- Unmanaged device brings malware to corporate network
- Unmanaged device with corporate data is lost or stolen
- Unmanaged device encrypts corporate documents with ransomware
- Employee leaves with sensitive data on personal device

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE



Recommended Baseline Safeguards:

- Gather a list of all hardware devices that the company manages
- Determine what device platforms you will manage (Windows, iOS, macOS, Android)
- Enroll devices in Intune
- Create a device compliance policy for each platform
- Create a conditional access policy that grants access to corporate resources when the device is in a compliant state
- Prevent access to your corporate network by unmanaged or unhealthy devices
- Create an App Protection Policy for iOS and Android to manage applications on unmanaged devices



Least to Most Restrictive Actions:

1. Set up app protection policies to manage applications with corporate data. Devices do not need to be enrolled in MDM. Corporate data will be encrypted and you will have the ability to remotely wipe data. You are still susceptible to the device being infected with malware and spreading it to your corporate network if they are able to join.
2. Set up app protection policies for personally owned devices and set up a policy to not allow these devices to join to your network.
3. Require that all devices accessing corporate data are enrolled in Intune and are in a compliant state.

CIS Sub-Control(s) Met: 1.4, 1.6

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 2: INVENTORY AND CONTROL OF SOFTWARE ASSETS



Description: *"Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution."*

Discovery Questions:

- Which applications do users access across the company?
- Are users transferring corporate data to unmanaged applications?
- Do users access applications with corporate data on their personal devices?
- How do you protect application data if a personal device is lost or stolen?
- How do you know when a new application for the company has been onboarded?
- What does your application management lifecycle look like today?

Overview:

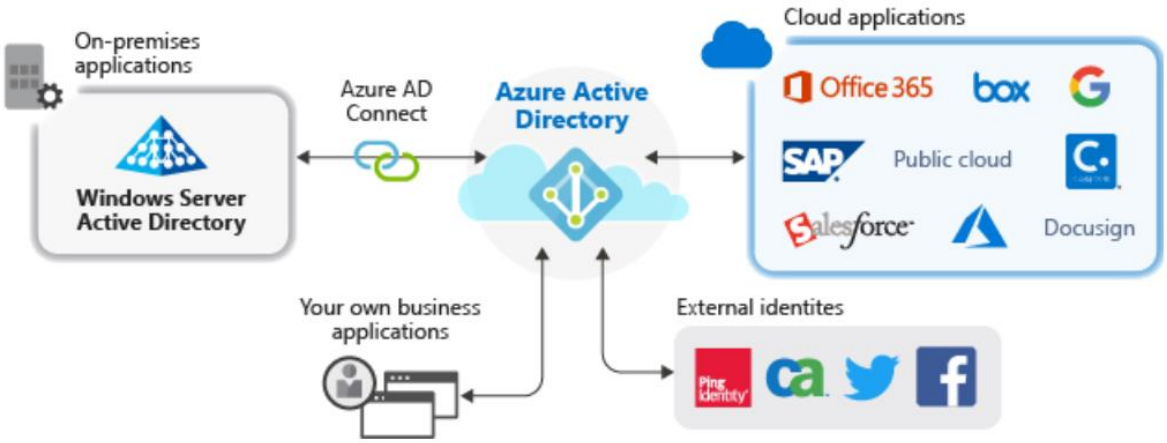
Software vulnerabilities have been a reoccurring threat for many years. Attackers look for ways to exploit unpatched software and distribute malicious content through many applications that users find online. The explosion of third-party SaaS applications and rise of shadow IT is expanding the attack surface. Vulnerability assessments against deployed software can detect new threats, but are not often implemented in organizations. A larger vulnerability lies in personally owned devices that are not protected from these types of attacks; usually these devices are the ones to get infected, which attackers can use as a staging point for collecting sensitive information and spreading laterally throughout the corporate network. Additionally, protecting data leakage across unauthorized apps is extremely important. Many new apps are being brought on at a rapid pace in efforts to enhance productivity, but they are often onboarded with few security controls in place.

OVERVIEW & BUSINESS CASE

MICROSOFT 365 SOLUTIONS: Azure AD, Intune, and Conditional Access

Azure Active Directory (AD)

Gathering an inventory of all the software assets within the company is a critical first step to controlling risk. With this list, you can define which apps will be authorized to access and share corporate data. Azure AD allows you to add enterprise applications, custom applications, and also on-premises line of business applications for single sign-on access. This allows you to maintain an inventory of approved applications, improve security, and improve change management processes. Users often store and share passwords in an insecure manner and create a great deal of helpdesk calls due to the volume of passwords they need to maintain. Single sign-on access alleviates this burden and increases security. You can assign apps to users or groups so that their access is granted or removed immediately throughout the employee life cycle at the company.



Intune

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. By joining a device to Azure AD and Intune, you can centrally push down all managed applications to that device. Windows Information Protection allows you to create policies to restrict users from saving or sharing corporate data to unmanaged applications such as their personal Gmail account.

OVERVIEW & BUSINESS CASE

Conditional Access

Combining Intune with Conditional Access creates powerful security gains. You can build policies that prevent access to data on a device that is not in a healthy state or restrict permissions when a user is not on your network. Additionally, you can require that an approved client application be used to access corporate data. A good example of this is redirecting a user to use the Outlook app on their iOS device instead of the native mail client.

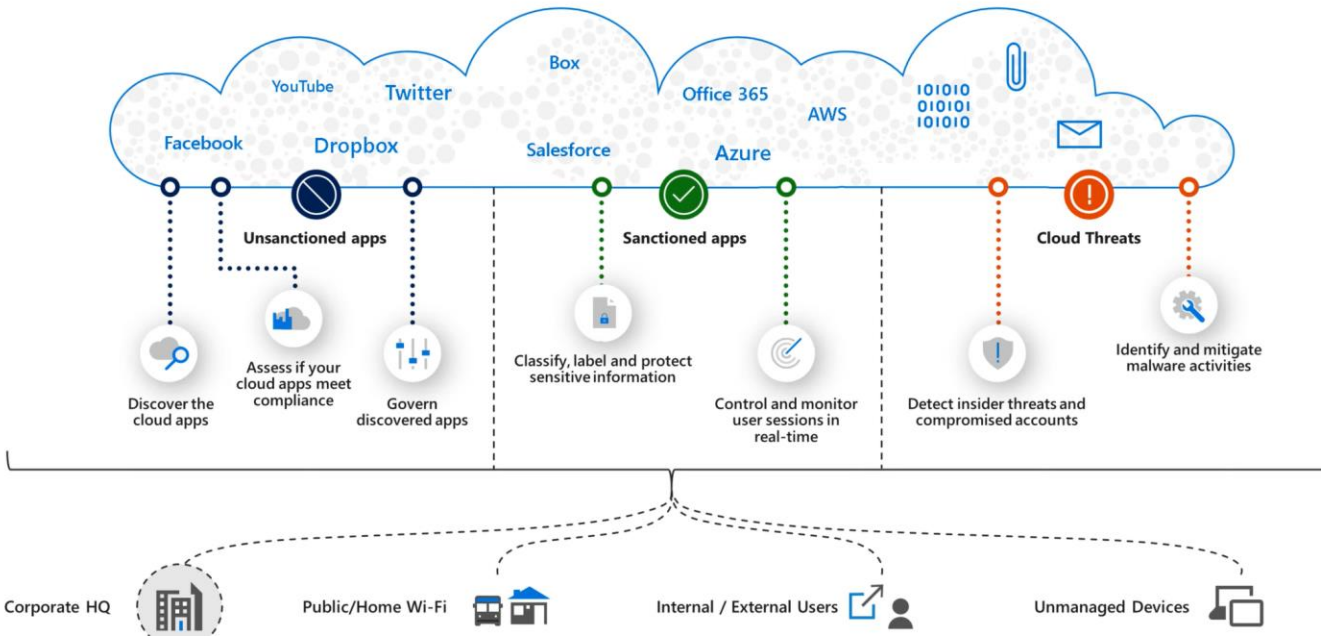
Business Case: *Users of a growing marketing company are getting frustrated with the company's managed Dropbox app for storing their files. They begin to download and store documents to their unmanaged laptop. Their laptop does not receive an important patch update and the device becomes infected. The attacker finds a file with all user passwords in the company, allowing him to expand the attack.*

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

UPSELL OPPORTUNITY: CLOUD APP SECURITY $3.50/USER/MONTH

- **Discover and control the use of shadow IT**: Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, then assess the risk levels and business readiness of more than 16,000 SaaS apps against more than 80 risks. Start managing these apps and services to ensure security and compliance.
- **Protect sensitive information anywhere in the cloud:** Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real-time across all your cloud apps.
- **Protect against cyberthreats and anomalies:** Detect unusual behavior across cloud apps to identify ransomware and compromised users or rogue applications, analyze high-risk usage, and remediate automatically to limit the risk to your organization.
- **Assess the compliance of your cloud apps:** Assess if your cloud apps meet relevant compliance requirements including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps and limit access to regulated data.



CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

Risk Analysis

Observable Risk

- *Software vulnerability causes unmanaged device to get infected*
- *Data loss to unmanaged application*
- *Infected device encrypts sensitive corporate documents with ransomware*
- *Employee leaves with sensitive data on personal device*
- *Shadow IT prevents you from effectively securing access to company assets*



Recommended Baseline Safeguards:

- Perform an asset inventory checklist and determine what apps are authorized to access corporate data
- Add applications to Azure Active Directory for single sign-on access
- Enroll devices in Intune
- Set up device compliance policies for every device you are going to support
- Set up app protection policies for Windows, iOS, and Android
- Push out managed applications to managed devices with Intune
- Set up a conditional access policy for policy-managed apps. Only grant access to applications such as the Office suite if they are using a client approved app
- Remove users' ability to register an app in Azure Active Directory

OVERVIEW & BUSINESS CASE



Least to Most Restrictive Actions:

1. Set up app protection policies to manage applications with corporate data. Devices do not need to be enrolled in MDM. Corporate data will be encrypted and you will have the ability to remotely wipe data. You are still susceptible to the device being infected with malware and spreading it to your corporate network if they are able to join.
2. Set up app protection policies for personally owned devices and set up a policy to not allow these devices to join to your network. Create a conditional access policy to only allow access to data on client managed applications
3. Require that all devices accessing corporate data are enrolled in Intune and are in a compliant state. Create an app protection policy and conditional access policy to only use client managed applications.

CIS Sub-Control(s) Met: 2.1, 2.2, 2.4, 2.5, 2.6

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 3: CONTINUOUS VULNERABILITY MANAGEMENT

Description: *"Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers."*

Discovery Questions:

- How do you assess vulnerabilities today?
- Are you enabled to quickly digest deployment signals and rapidly respond in order to react, identify, and remediate with minimal impact?
- What is your triage and documentation process for new vulnerabilities?
- Does the delivery of patches disrupt business?
- What is your plan to address user feedback and revise communications or make adjustments quickly around software update cycles?
- Are there features that address pain points, open new opportunities, and/or provide a better experience adopted?

Overview:

When a new vulnerability is reported there are often three parties involved that take action. The attacker looks for ways to weaponize the vulnerability and exploit unpatched devices. Software vendors looks to quickly develop and deploy patch updates, and, in many cases try to quickly follow Microsoft's lead because Microsoft's patches can cause the vendor's application to stop working on client systems. Lastly, IT professionals look to assess the risk of the vulnerability and test the updates to client environments before performing a broad update.

Proactive management of threats and vulnerabilities is essential to minimizing impact. Keeping up with the volume and variety of new vulnerabilities consumes a tremendous amount of resources. Solutions are needed for automated detection and response as well as the ability to track trends for threats that may occur.

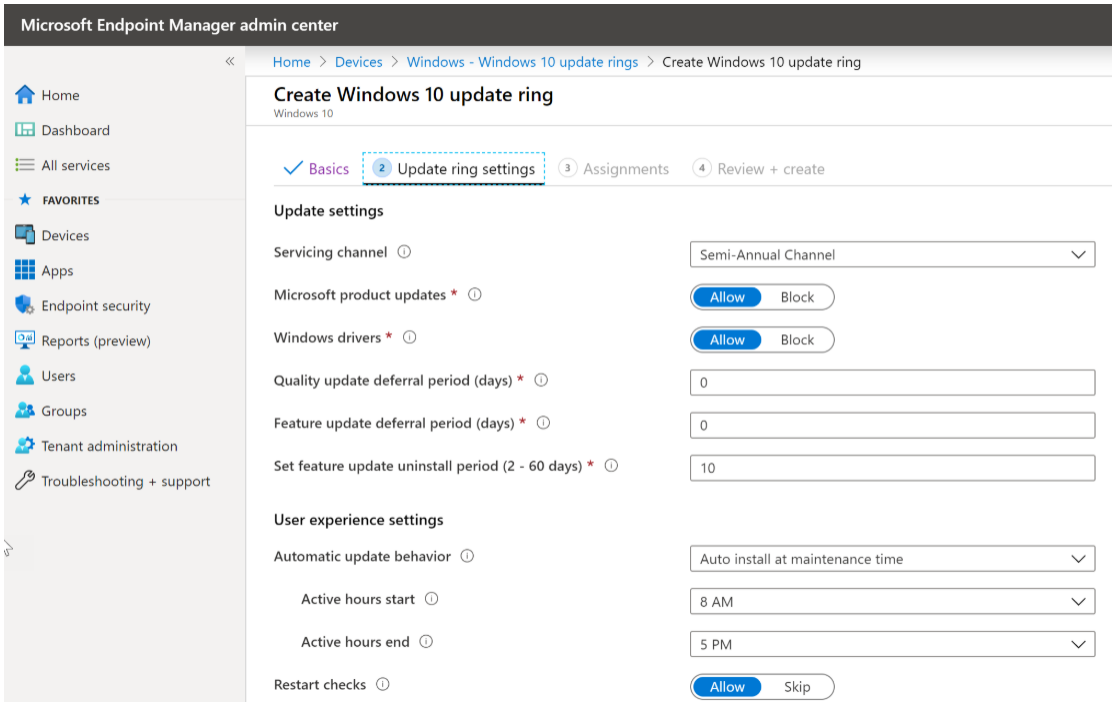
CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

Microsoft 365 Solutions: Intune Deployment Rings, Secure Score, and Threat Dashboard

Windows Deployment Rings

OS management is shifting to a landscape that Microsoft calls "modern deployment." With Windows-as-a-service, the methodology of updates has completely changed, moving away from major upgrades every few years to iterative updates twice per year. Each iteration contains a smaller subset of changes rather than substantial differences. Windows updates will function much like traditional Office software and quality updates for security will occur on a monthly basis. Intune allows you to define the cycle of these security patches via functionality they call "deployment rings," which works much like you are familiar with in an RMM tool.



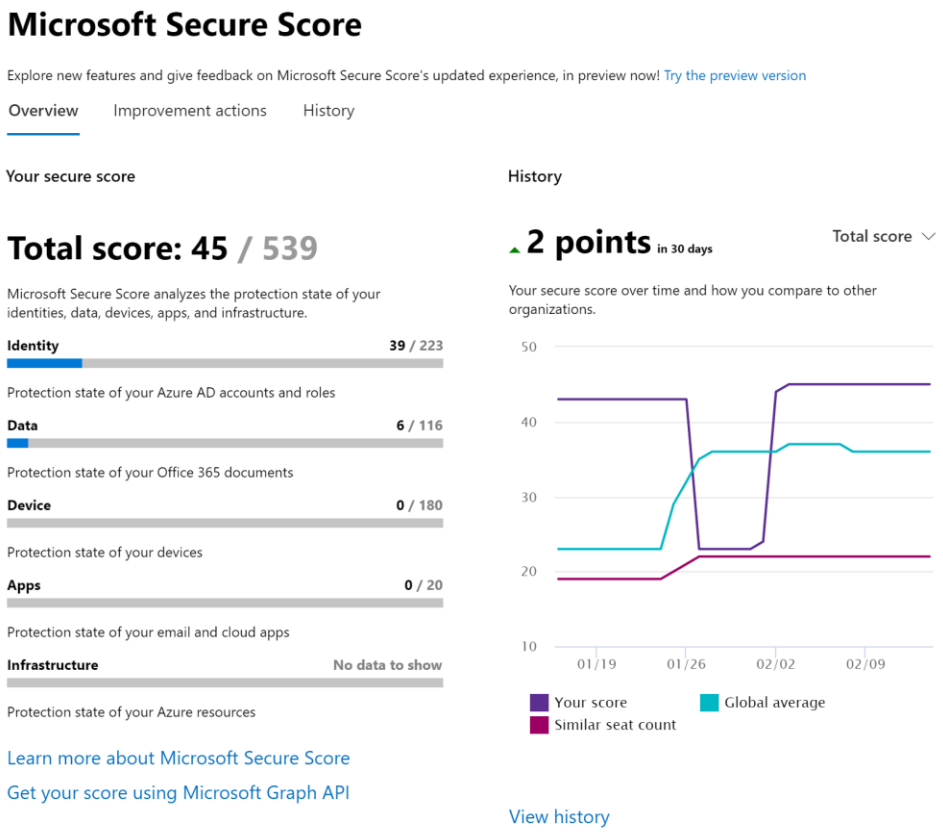
You can control your patch updates and scope the servicing channel to certain groups within the organization. For more information on deployment rings, click here.

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

SECURE SCORE

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

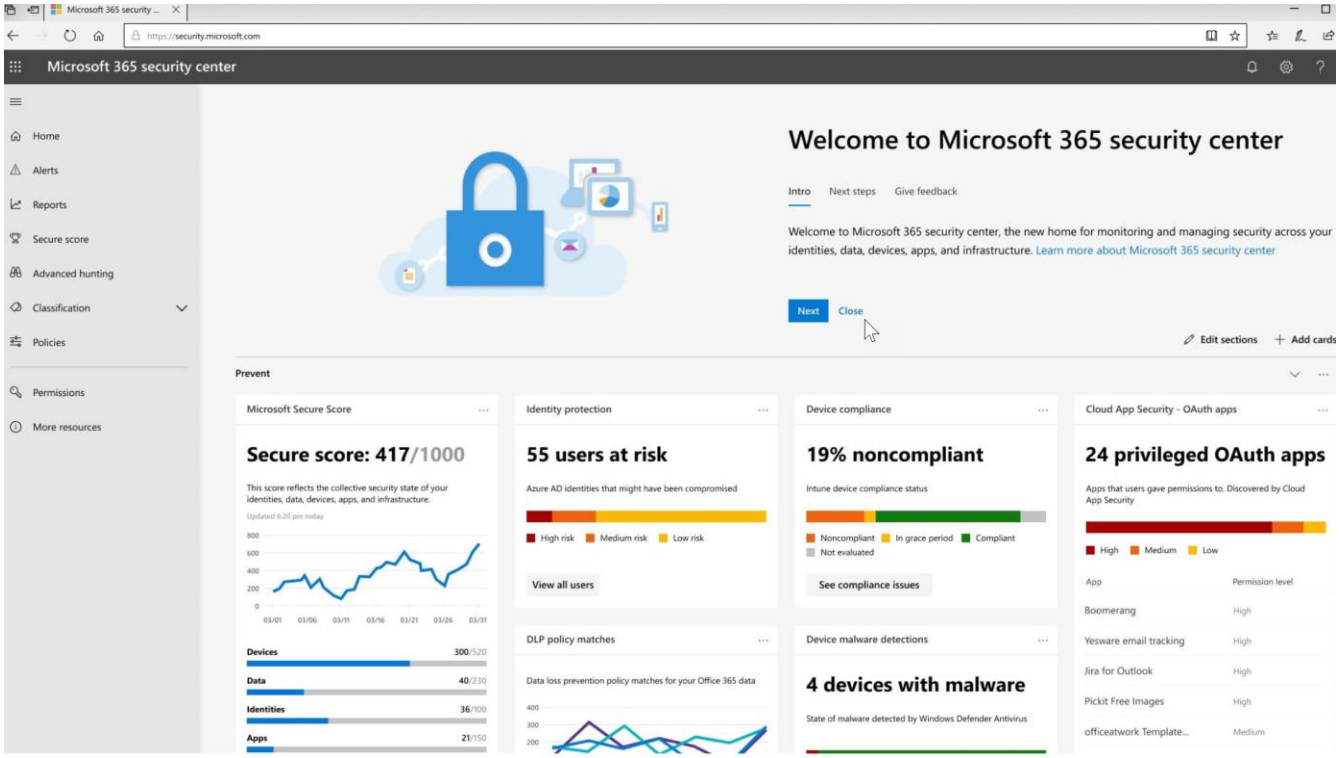


OVERVIEW & BUSINESS CASE

THREAT MANAGEMENT DASHBOARD

The Microsoft Security Graph collects and analyzes an estimated 6.5 trillion data signals from user sign-ins, device endpoints, email messages, documents, cloud applications, and Azure public cloud. This allows Microsoft to collect a ton of data that could be malicious to the end users and enhance their vulnerability detection capabilities.

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



OVERVIEW & BUSINESS CASE

STACK IT UP

There is a good opportunity to stack a third-party security tool like **Novacoast novaSOC** for vulnerability management across software applications. novaSOC is a multi-tenant solution that integrates with your PSA tool to provide alerting capabilities. novaSOC creates an inventory of every application installed, and monitors behavioral data, network traffic, and security logs. Alerts can be generated that reference a published common vulnerability and exposure (CVE). If a security update is published, an alert/ticket will be generated for an admin.

Risk Analysis

Observable Risk:

- *Software vulnerability causes devices to become infected*
- *Patch updates are not performed in a timely manner, exposing machines to vulnerabilities*
- *Inefficient methods are used to scan for vulnerabilities reducing the ability to scale*

Recommended Baseline Safeguards:

- Review your vulnerability assessment processes and procedures to see where efficiencies can be found
- Enroll devices in Intune
- Create device compliance policies that require a certain OS build for all device platforms you support

OVERVIEW & BUSINESS CASE

- Review the deployment rings in Intune. Design deployment rings that meet the client's needs and minimizes disruption
- Review the client's secure score information and identify where you can make improvements
- Periodically review the threat management dashboard to see trends in malware, phishing, spoofing, device health, and more
- Create custom reports on trends in malware, phishing, spoofing, device health, and more to be sent on a periodic basis to your team for review.



Least to Most Restrictive Actions:

1. The policies and profiles you create will ultimately be determined by the information absorbed from the data points across your security stack for each client. While you are reviewing the secure score information, you will see an impact field that will help you determine scope and timelines for implementing safeguards.

CIS Sub-Control(s) Met: 3.4, 3.5, 3.7

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 4: CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES



Description: *"The processes and tools used to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications."*

Discovery Questions:

- How many global admins are present in your account?
- What multi-factor authentication solution do you have in place?
- How much money are you spending for your helpdesk to perform password resets?
- Are you implementing a model of least privilege for access to applications?
- Do you have an admin account dedicated to admin tasks?
- What password management tool do you use?

Overview:

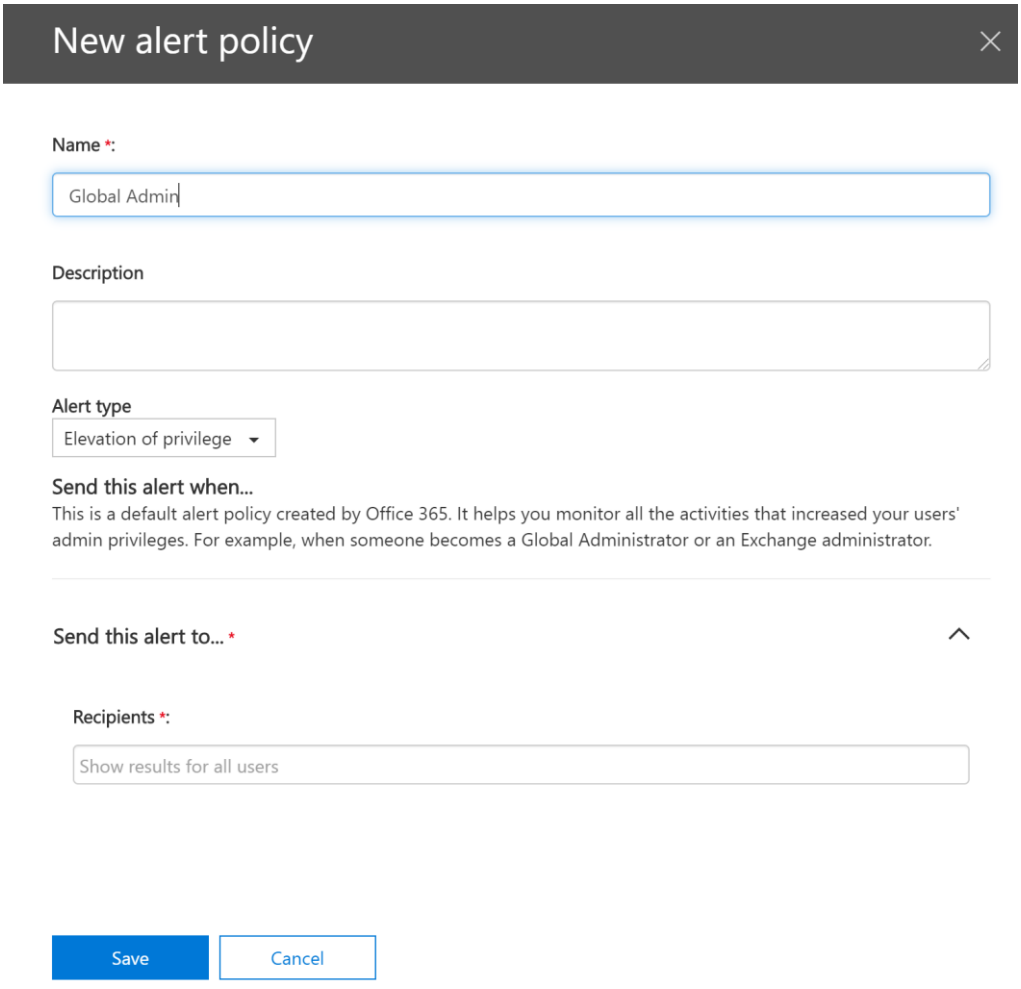
The misuse of administrative privileges across an organization can be one of the primary methods for an attacker to move laterally throughout a company. To reduce the chance of a malicious actor compromising an account with elevated privileges or an authorized user inadvertently impacting a sensitive resource, organizations need to minimize the number of people who have access to secure information and resources. Businesses need to follow a model of least privilege when granting access to applications to minimize the organization's attack surface. More than one global administrator should be designated so a single admin can be monitored and to provide redundancy should a single admin leave an organization. Additionally, there should be no more than four global admins set for any tenant. Multi-factor authentication should be enforced on all privileged accounts.

OVERVIEW & BUSINESS CASE

Microsoft 365 Solutions: Azure AD, Conditional Access, and Multi-factor Authentication

Role-Based Access Control and Self-Service Password Reset

Azure Active Directory (AD) has granular role-based access control to support a model of least privilege. Beyond a global administrator, you can assign custom admin roles such as user administrator, security administrator, etc. In the Azure AD portal, you can filter users based on role. In the security admin center, you can set alerts to detect when someone's role has been upgraded to global administrator. Self-service password reset can be set up so users do not have to reach out to admins to regain access to their accounts, reducing the need for many users with this level of access.



Overview & Business Case

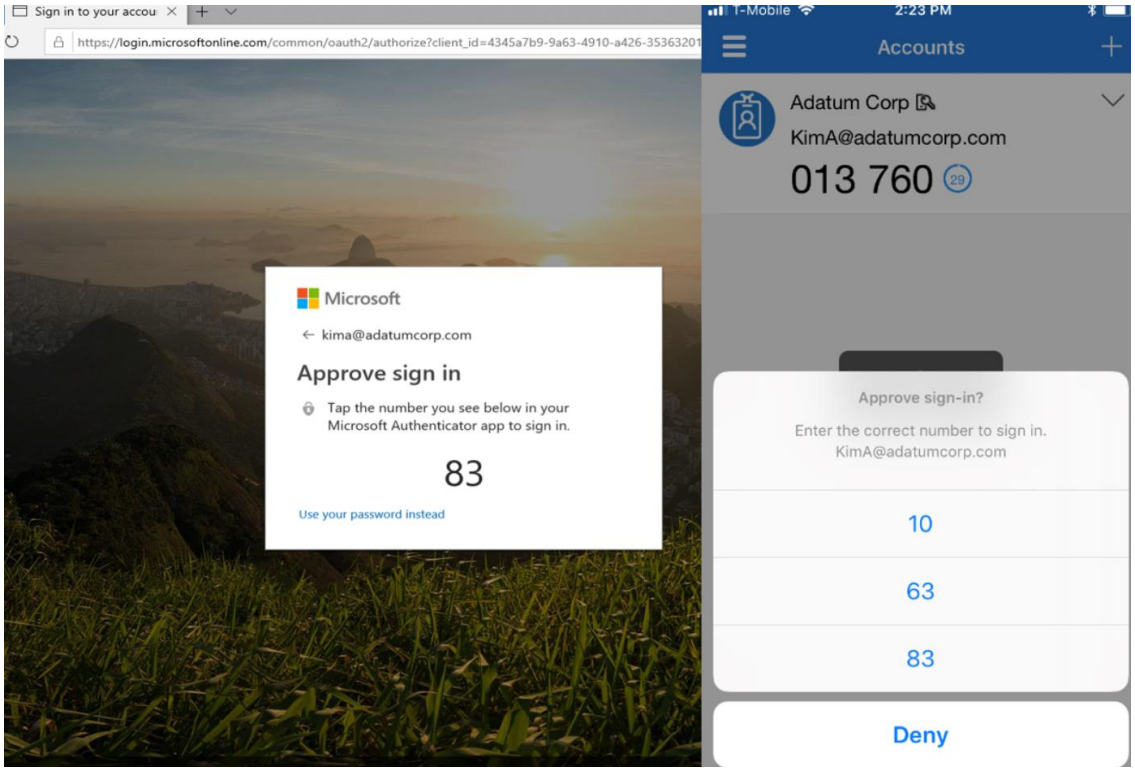
Multi-factor Authentication (MFA)

Conditional access is Microsoft's new identity solution for granting access to resources within the organization. When you create a policy, you define certain conditions that are met to enforce certain controls. These controls include enforcing additional security parameters such as MFA. You can scope the policy to certain users or groups, including directory roles like global administrator. You can even apply these controls to guest users within your active directory.

Passwordless Authentication

Password resets contribute to rising helpdesk costs and users frequently store passwords unsecurely due to "password fatigue". To combat this, the industry is making a move towards passwordless authentication. A variety of options for biometrics, security keys, and mobile apps are now available, providing a secure and convenient user experience. Azure AD can be set up for passwordless authentication with the Microsoft Authenticator app. Users are prompted with a code instead of having to type in a password and their second factor can be biometric, such as FaceID. Some compliance regulations prevent the use of passwordless authentication, so be careful before you decide to implement this at an organization.

Example of passwordless authentication with Microsoft Authenticator app:

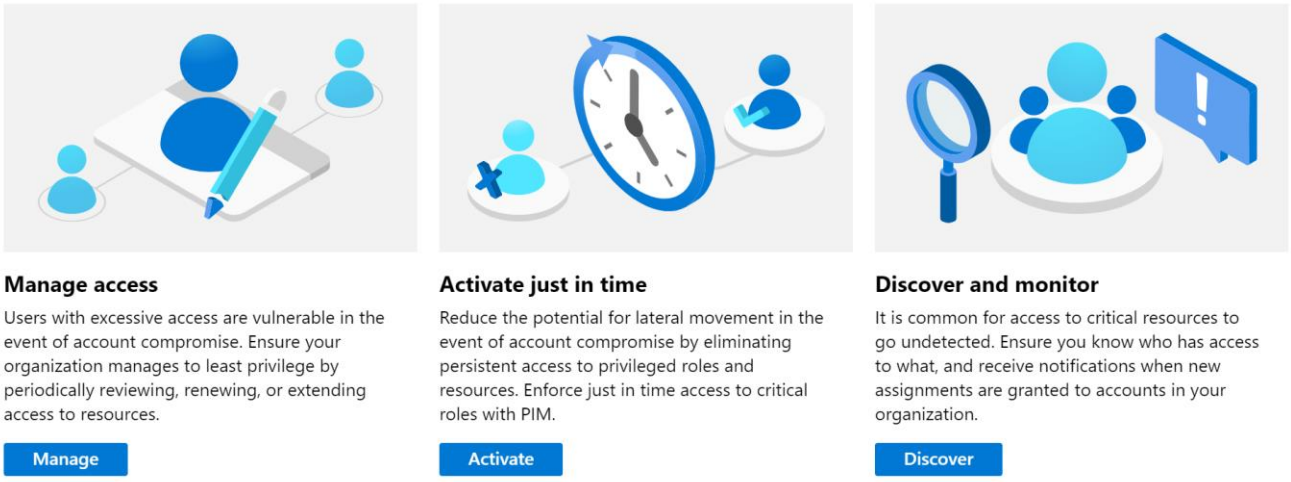


CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

UPSELL OPPORTUNITY: AZURE PRIVILEGED IDENTITY MANAGEMENT (PIM) $9/USER/MONTH

Azure Privileged Identity Management (PIM) allows for "just in time" and "just enough" access for elevation of privileges. Users can activate certain roles for a limited amount of time to perform administrative tasks. Users must provide reasons for the elevation when the role is activated, creating a complete audit log of activities. PIM is part of the Azure AD Plan 2 SKU that you can add to any base plan. It includes many other solutions, such as Identity Protection, which leverages machine learning to detect if a user is at risk.



OVERVIEW & BUSINESS CASE

RISK ANALYSIS

Observations

- *A global administrator account is compromised and an attacker moves throughout the organization*
- *Users are accessing sensitive data with global admin credentials on unmanaged devices*
- *Risk is significantly increased by giving global admin rights to users who do not need the full permissions of the role*
- *A global administrator's password is compromised and the attacker gains access because no MFA is in place*
- *Your helpdesk has continually rising costs due to password resets*
- *A user is subjected to a phishing attack and the admin's credentials are compromised because they are still using passwords*



Recommended Baseline Safeguards:

- Review the number of global administrators in your account – have at least two global admins for one account, but no more than four
- Enforce a model of least privileged access with the RBAC controls available
- Have a dedicated account solely for admin tasks
- Set up alerts in the Security Center for elevation of privileged roles
- Set up a conditional access policy to enforce MFA on all admin-level accounts
- Set up a conditional access policy to enforce MFA on user accounts when they are not on the corporate network
- Enable self-service password reset
- Enable passwordless authentication (if there are no regulatory concerns)

OVERVIEW & BUSINESS CASE



Least to Most Restrictive Actions:

1. Set up role-based access with only two global admins in place. Enforce MFA to all admin accounts with a conditional access policy. Enable self-service password reset
2. Set up role-based access with only two global admins in place. Enforce MFA to all admin accounts with a conditional access policy. Enable self-service password reset. Set up a conditional access policy to require MFA for users when they are not on your network.
3. Set up role-based access with only two global admins in place. Enforce MFA to all admin accounts with a conditional access policy. Enable self-service password reset. Set up a conditional access policy to require MFA for users at all times when they are trying to access corporate data.

CIS Sub-Control(s) Met: 4.1, 4.3, 4.4, 4.5

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 5: SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS, AND SERVERS



Description: *"Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings."*

Discovery Questions:

- How do you know if a device is it out of compliance from the policies you have put in place?
- How do you know if a user has changed settings on a device, creating a vulnerability?
- What additional controls should you be putting in place to protect your devices in the cloud?
- How can you move device management off the on-premise network if all devices have group policies (GPOs) being applied to them?
- What policies should you be applying to mobile devices?

Overview:

For years, IT professionals have been building custom images, updating driver information, and planning for major upgrades to devices. Group policies (GPOs) have been the primary vehicle for enforcing security requirements, remotely configuring settings, and more. Even though you can enforce these policies and controls on a device, how do you know when a device is out of compliance? How do you know if a user has changed settings, creating a vulnerability? As you look to full cloud deployments for device management, you need to understand what the transition path will look like and new security concerns for these devices.

Remote workers using devices outside of the perimeter network is a larger concern. What additional controls should you be putting in place to protect these devices? How can you move off your on-premise network if all devices have GPOs being applied to them? It's now becoming essential to manage mobile devices, but many IT professionals do not have as much experience in this area. Not having a plan for these devices will ultimately leave a company exposed to a higher likelihood of an attack.

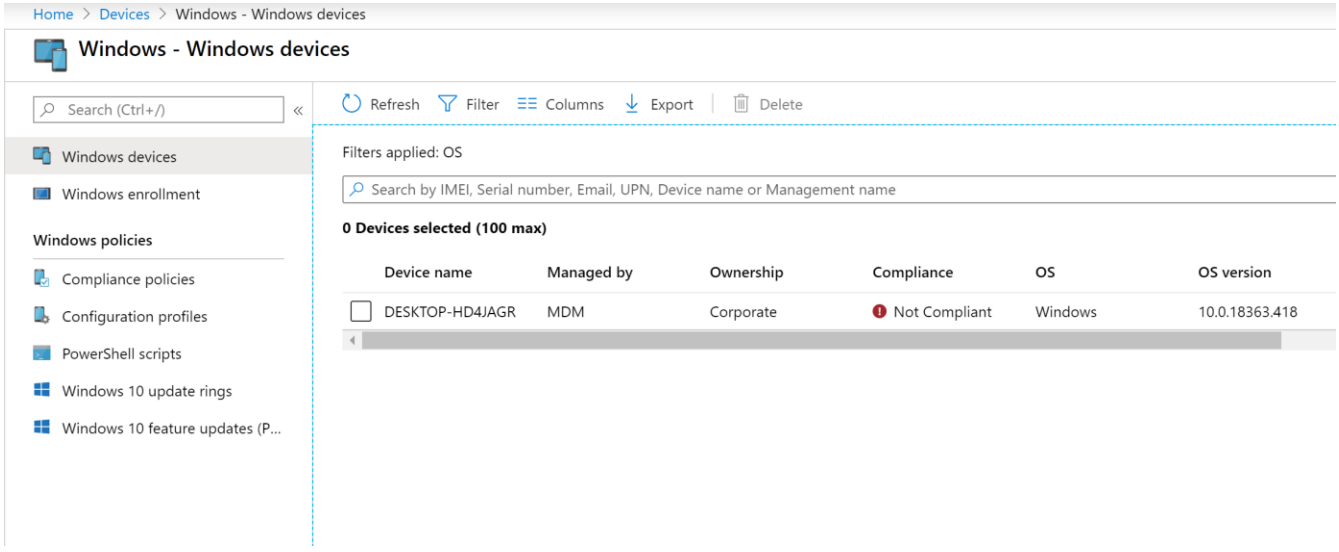
OVERVIEW & BUSINESS CASE

Microsoft 365 Solutions: Deployment Rings, Intune, and Security Baselines

The industry is shifting to a model of Windows-as-a-service. Iterative updates will be twice per year and quality updates for security will occur on a monthly basis. Intune allows you to define the cycle of these security patches via functionality that Microsoft calls “deployment rings,” which works much like you are familiar with in an RMM tool.

Compliance Policies

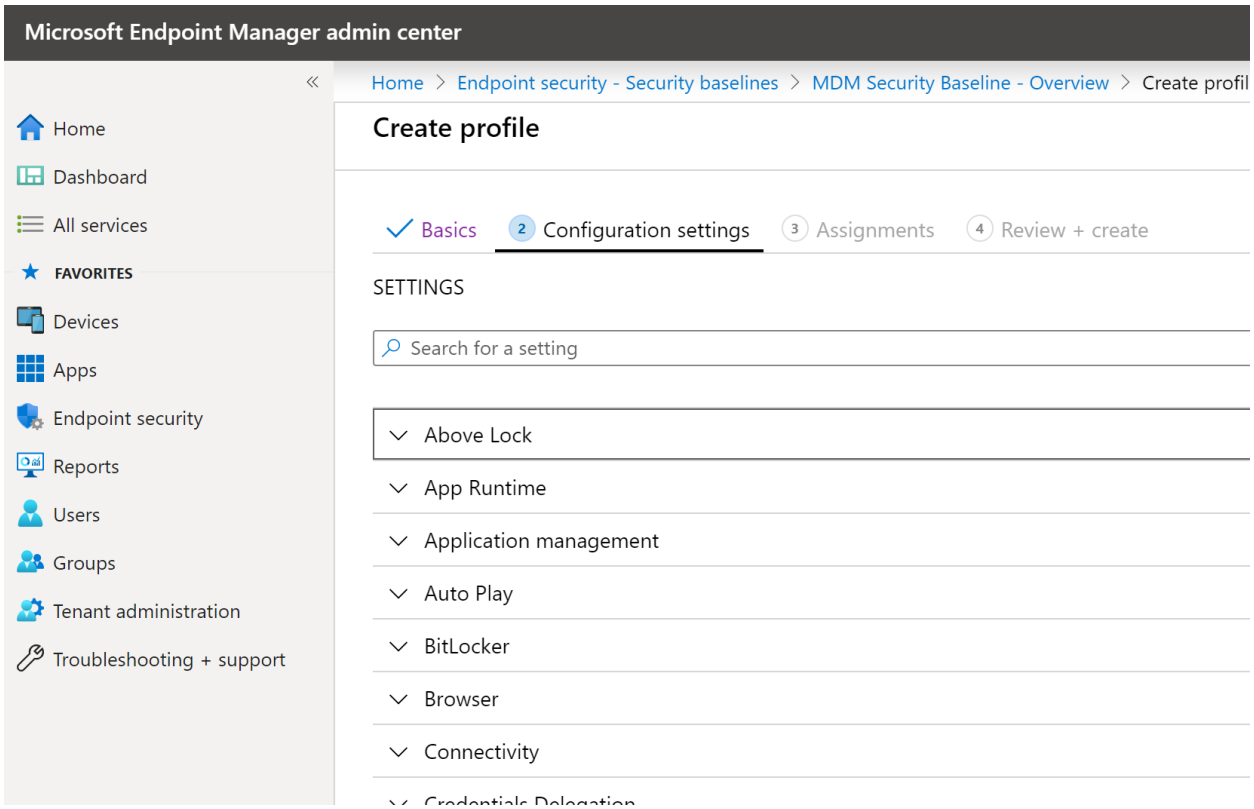
In the Endpoint Manager admin center, you have the ability to create device compliance policies for each device that you are going to support with Intune. These policies allow you to define when a device is in a “healthy state,” such as having a specified OS version, requiring Bitlocker, having active anti-virus installed, requiring secure boot, and more. When a device meets the prescribed requirements, you can see that it is in a healthy state in the Endpoint Manager admin center. If a device falls out of compliance, you can set a conditional access policy to prevent the user from accessing corporate data on that device. This helps contain risk and mitigate the impact as you get the device back into a healthy state. These policies extend into mobile devices, which you can require to use a managed email profile, block jail-broken or rooted devices, and define minimum password requirements.



OVERVIEW & BUSINESS CASE

Security Baselines

In addition to compliance policies, you can create configuration profiles that mimic traditional GPOs. These settings can get very granular; you set definitions for setting the start menu layout, defining the minutes of inactivity before lockout, blocking access to USB ports, etc. If you are not sure where to start to configure settings, Microsoft created MDM security baselines. These security baselines will be managed and updated directly from the cloud – providing clients with the most recent and most advanced security settings and capabilities available from Microsoft 365.



OVERVIEW & BUSINESS CASE

Hybrid Deployment

Many clients have CapEx tied up with existing infrastructure. Most notably, this includes an on-premise domain controller for Active Directory. Beyond these existing expenditures, there are many group policies, file shares, security settings, printers, and more that make moving to a full cloud deployment illogical. You can configure Intune for a hybrid deployment of device management. With Windows Autopilot hybrid join, you can push a device down to your local domain, applying legacy GPOs when the device is turned on. This allows you to transition to full cloud management over time and take advantage of the iOS and Android management policies available with Intune.

Risk Analysis

Observable Risk:

- *A device is not patched in a timely manner and is susceptible to an attack*
- *A managed device in an unhealthy state has access to corporate data*
- *Users are accessing sensitive data on an unmanaged device*
- *Your existing configurations and group policies do not protect remote workers*
- *Your existing configurations and group policies do not protect from cloud vulnerabilities*
- *You have no way to wipe corporate data from a device when a user leaves the organization or if the device is lost or stolen*
- *You are not sure if a device is configured to meet organizational standards for security*

Recommended Baseline Safeguards:

- Upgrade all existing devices to Windows 10 if they are running a Pro version of Windows
- Enforce MFA for device join to Azure AD
- Configure a device compliance policy for each platform you are going to support
- Create Windows 10 deployment rings for updates

OVERVIEW & BUSINESS CASE

- Enroll all devices in Intune
- Ensure that mobile device password reuse is prohibited
- Ensure that mobile devices are set to never expire passwords
- Ensure that mobile devices require a complex password to prevent brute force attacks
- Ensure that settings are enabled to lock devices after a period of inactivity to prevent unauthorized access
- Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data
- Ensure that connecting devices have AV and a local firewall enabled
- Ensure mobile device management policies are required for email profiles
- Enable UEFI Secure Boot
- Remove local administrator privileges from end users with Windows Autopilot



Least to Most Restrictive Actions:

1. Create a device compliance policy for every device platform that you will support. Set the actions for a non-compliant device to have a three day grace period. Create a conditional access policy to prevent access to all corporate data on non-compliant devices.
2. Create a device compliance policy for every device platform that you will support. Set the actions to mark the device as non-compliant immediately if the device does not meet policy settings. Create a conditional access policy to prevent access to all corporate data on non-compliant devices.
3. Create a device compliance policy for every device platform that you will support. Set the actions to mark the device as non-compliant immediately if the device does not meet policy settings. Create a conditional access policy to prevent access to all corporate data on non-compliant devices. Create device configuration profiles to enforce additional devices restrictions on all platforms you support

CIS Sub-Control(s) Met: 5.4

OVERVIEW & BUSINESS CASE

CIS CONTROL 6: MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS



Description: *"Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack."*

Discovery Questions (for the IT Professional):

- How often do you review audit logs?
- What are the data sources from which you should review audit logs?
- How do you automate some of the review processes for audit logs across clients?

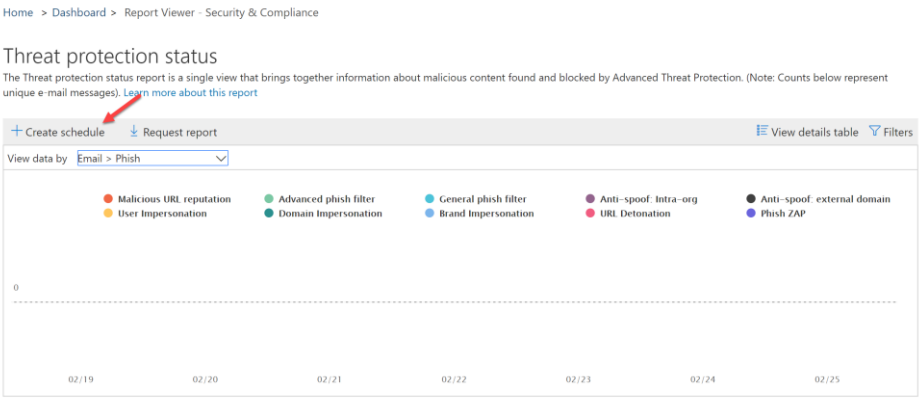
Overview:

Periodic review of audit logs is essential to track trends and be more proactive against suspicious activity. Attackers often breach a system and lie dormant for weeks or months at a time. Sometimes the audit logs are the only records you have to identify a successful attack.

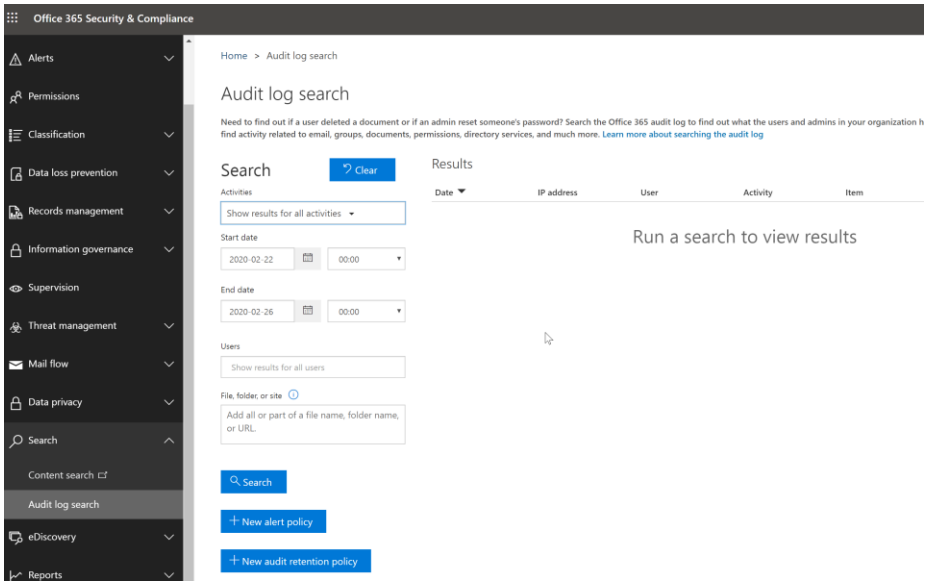
OVERVIEW & BUSINESS CASE

Microsoft 365 Solution: Security and Compliance Center
In the Security Center, Microsoft provides near real-time reports on many different security events that they are tracking, such as malware, phishing, spoofing, data loss triggers, uncompliant devices, and more. These insights allow you to proactively set up policies and triggers that you can continually refine if needed. Additionally, you can create a report schedule for certain events that you want to closely monitor.

Ex. Threat methods used for phishing:



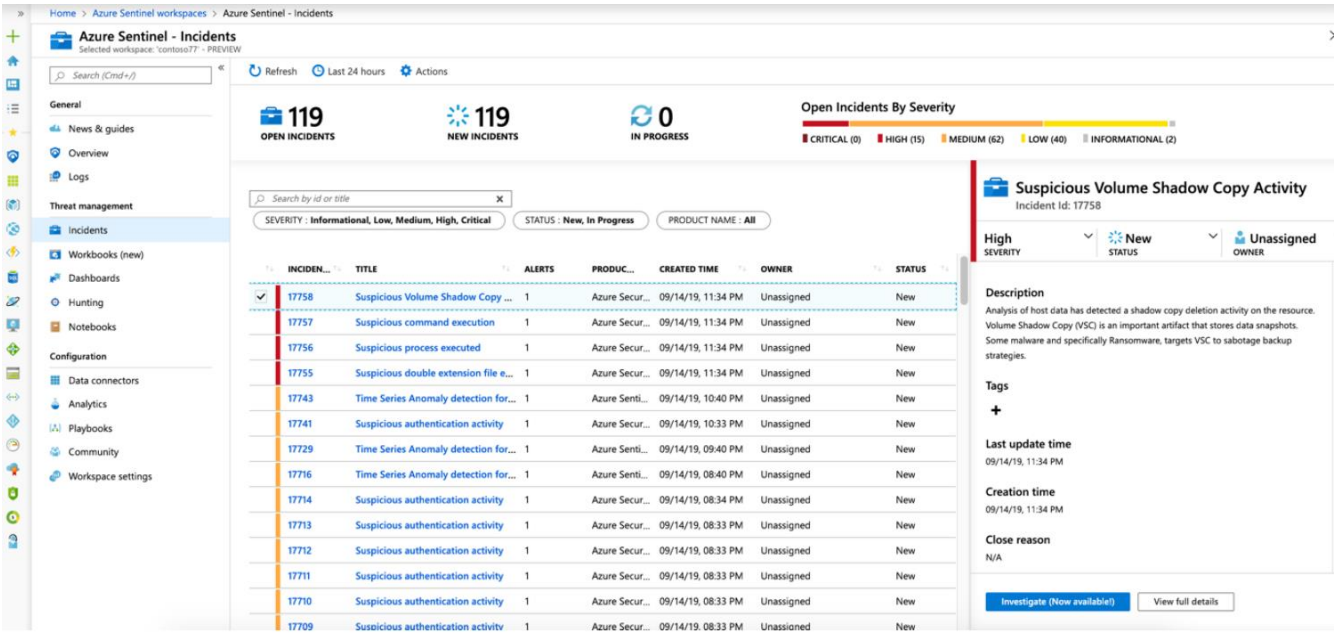
All of these reports across malware, phishing, spoofing, DLP policy matches, ATP files types, and more can be seen in one view to get a quick snapshot on any trends. An audit log can be turned on in the Security and Compliance Center, as well to run investigative reports on certain activities perform in a certain data range.



OVERVIEW & BUSINESS CASE

UPSELL OPPORTUNITY: AZURE SENTINEL

Azure Sentinel is Microsoft's security information event management (SIEM) and security orchestration automated response (SOAR) solution. Sentinel allows you to connect *all* of your security sources (not just Microsoft!) and consolidates the data in one location. It has automated investigation, detection, and response capabilities to minimize the number of alerts you respond to. Pricing for Azure Sentinel is based on the volume of data ingested for analysis. Click here for the pricing calculator.



OVERVIEW & BUSINESS CASE

RISK ANALYSIS

OBSERVABLE RISK:

- *An attacker breaches your environment and you do not know that they are in your systems because you never review the event logs*
- *You do not review trends for threats within your tenant and a user is compromised because addition controls were not put into place*



Recommended Baseline Safeguards:

- Ensure Microsoft 365 audit log search is enabled
- Ensure mailbox auditing for all users is enabled
- Ensure user role group changes are reviewed at least weekly
- Ensure mail forwarding rules are reviewed at least weekly
- Ensure the mailbox access by non-owners report is reviewed at least biweekly
- Ensure the malware detections report is reviewed at least weekly
- Ensure the spoofed domains report is reviewed at least weekly
- Ensure non-global administrator role group assignments are reviewed at least weekly
- Ensure the report of users who have had their email privileges restricted due to spamming is reviewed
- Ensure guest users are reviewed at least biweekly

CIS Sub-Control(s) Met: 6.2, 6.3, 6.7

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 7: EMAIL AND WEB BROWSER PROTECTIONS



Description: *"Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems."*

Discovery Questions (for the IT Professional):

- Are users taking precautions when reviewing email or clicking on links sent to them?
- Are you able to scan attachments for malicious content?
- What does your anti-malware solution look like today?
- Do you have real-time click protection on links for sophisticated attacks?
- What is the impact if a user's credentials are compromised from a phishing attack?

Overview:

Web attacks are executed in a variety of ways, but most commonly attackers use social engineering to entice a user to take a certain action. This is often from a user clicking on a link in an email that brings them to a malicious webpage where malware is downloaded to their device. Other times, attackers are simply using phishing emails to capture the user's credentials, taking them to a familiar location where they usually sign in. Cross-Site Scripting (XSS) is another method an attacker uses to put malicious code into trustworthy websites. When a user visits the site, malicious scripts are executed in their browser. These scripts can be used to log keystrokes or remotely access and control a user's machine.

OVERVIEW & BUSINESS CASE

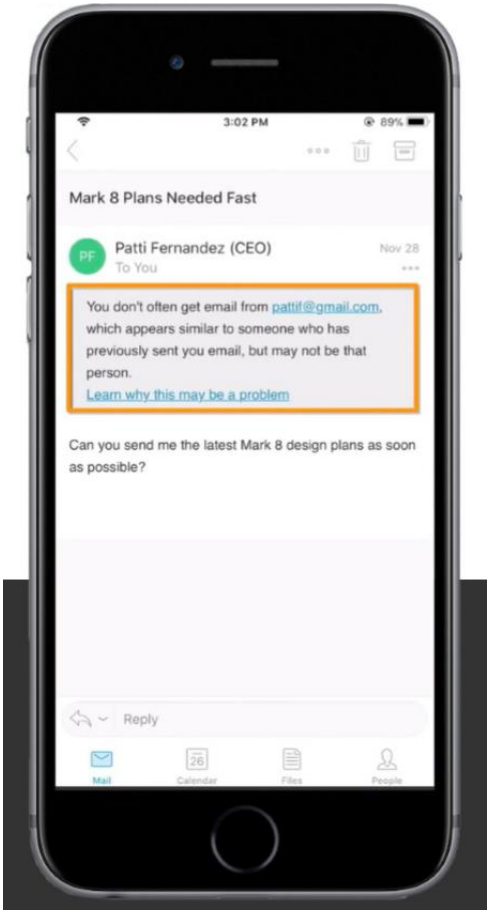
Microsoft 365 Solutions: Office 365 Advanced Threat Protection, DMARC, and DKIM

The Microsoft Security Graph collects and analyzes an estimated 6.5 trillion data signals from user sign-ins, device endpoints, email messages, documents, cloud applications, and Azure public cloud. This allows Microsoft to collect a ton of data that could be malicious to end users and enhances 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.[5]

Office 365 Advanced Threat Protection (ATP)

Microsoft Office 365's ATP solution provides a tremendous amount of protection to end users. The technology uses a layered defense approach which results in 25% of all malicious messages being received and blocked at the edge before even reaching the organization. IP reputation is analyzed against the known data collected from the security graph to see if it's already on the block list. You should configure SPF records, DKIM, and DMARC to authenticate mail senders and ensure that destination email systems trust messages sent from your domain. Anti-phishing policies will verify the authenticity of the domain source against these frameworks. If it detects anomalies, the user will get a warning message when they open the item, telling them it could be a spoofed user.

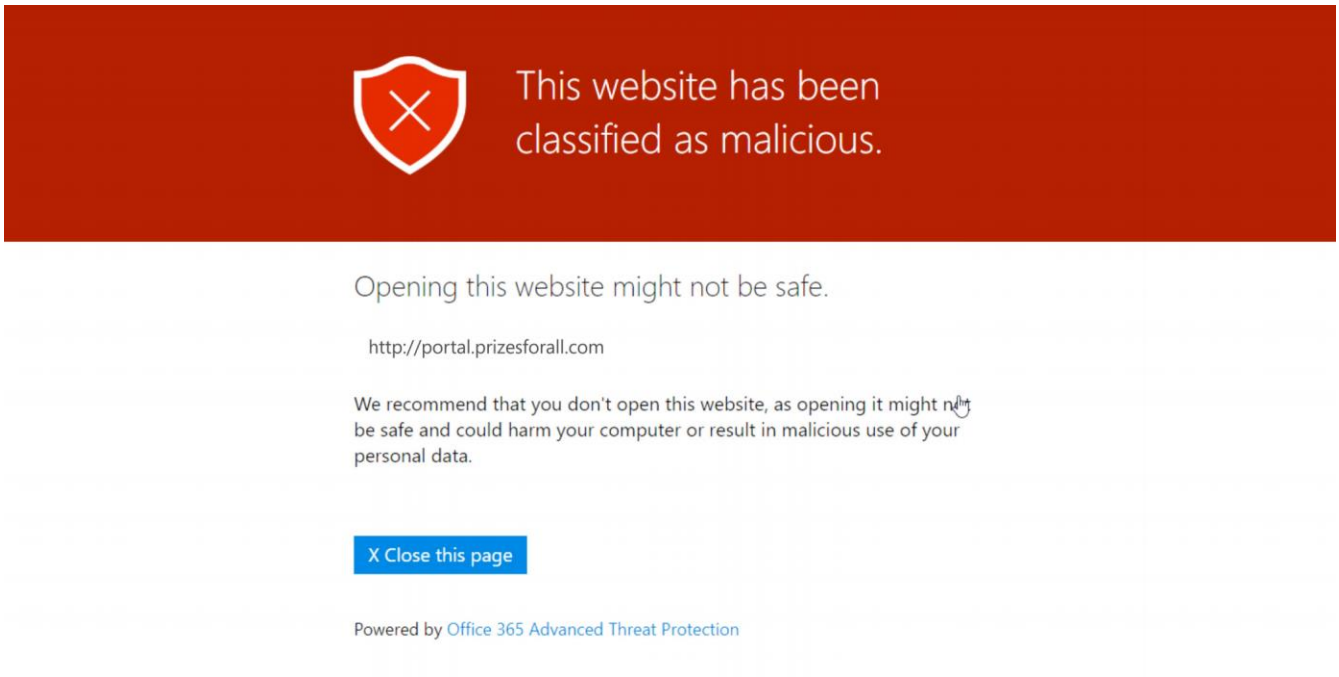
You can define custom anti-phishing policies that leverage mailbox intelligence capabilities to learn who a user interacts with. After it has gathered enough data, the solution can better detect impersonation attempts of trusted individuals in a company.



OVERVIEW & BUSINESS CASE

SAFE LINKS AND SAFE ATTACHMENTS

Advanced threat protection allows you to create policies for safe links and safe attachments across Exchange, Teams, OneDrive, and SharePoint. Real-time detonation occurs when a user clicks on any link and the content is contained in a sandbox environment. Attachments are opened inside a sandbox environment as well before they are fully delivered over email. This allows zero-day malicious attachments and links to be detected.



Enhanced email filtering can be set up if you have a connector in 365 (third 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 allows you to overlook, or "skip", any IP addresses that are 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, and anti-spoofing from Microsoft's known malicious list based off IP. In a way, it provides a secondary layer of protection by allowing Microsoft to view the IPs of the original email and check them against their database

OVERVIEW & BUSINESS CASE

RISK ANALYSIS

OBSERVABLE RISK:

- *A user clicks on a malicious link in an email message and is infected with ransomware*
- *A user is subject to a social engineering attack and then visits a malicious website where malware is download to their device*
- *A user gets a malicious message from a user impersonating someone at the company*
- *An actor spoofs an internal domain and gets sensitive data sent to him through a social engineering attack*
- *You do not review threat trends within your tenant and a user is phished because additional controls were not put into place*
- *A user clicks on a link or opens an attachment internally on Teams, OneDrive, or SharePoint and a device is infected*

Recommended Baseline Safeguards:

- Implement ATP safe links, safe attachments, and an anti-phishing policy
- Periodically review trends in the Threat Management Dashboard
- Ensure Exchange Online spam policies are set correctly
- Ensure mail transport rules do not forward email to external domains
- Ensure mail transport rules do not whitelist specific domains
- Ensure that SPF records are published for all Exchange domains
- Ensure DMARC records for all Exchange Online domains are published
- Ensure that DKIM is enabled for all Exchange Online domains
- Ensure MailTips are enabled for end users

OVERVIEW & BUSINESS CASE



Least to Most Restrictive Actions:

1. Set up a policy for safe links and safe attachments. Allow for user override.
2. Set up a policy for safe links and safe attachments. Prevent user override.
3. Set up a policy for safe links and safe attachments. Prevent user override. Set up a custom anti-phishing policy for key staff in the company and configure mailbox intelligence.

CIS Sub-Control(s) Met: 7.1, 7.6, 7.8, 7.10

OVERVIEW & BUSINESS CASE

CIS CONTROL 8: MALWARE DEFENSES



Description: *"Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action."*

Discovery Questions (for the IT Professional):

- Are users taking precautions when reviewing emails or clicking on links sent to them?
- Are you able to scan attachments for malicious content?
- What does your anti-malware solution look like today?
- Do you have real-time click protection on links for sophisticated attacks?
- What is the impact if a user's credentials are compromised from a phishing attack?
- What does your containment method look like if a device is infected?

Overview:

Malware defenses are highly important in today's shifting cybersecurity landscape. Ransomware remains the most prominent malware threat and is often sourced from infected links. In 2019, 85% of MSPs reported ransomware as the most common malware threat to small to medium-sized businesses.[4] Sophisticated attackers will make links appear benign to pass through the first round of security filters. From there, they alter the destination of the link to a malicious website, weaponizing the message after it is delivered. With the new emergence of file storing software and collaboration tools, its essential to scan these environments as well for malicious content. The containment strategy an organization takes is just as import as the prevention strategy put into place. You need controls to quickly mitigate the threat and reduce the spread to other systems or users.

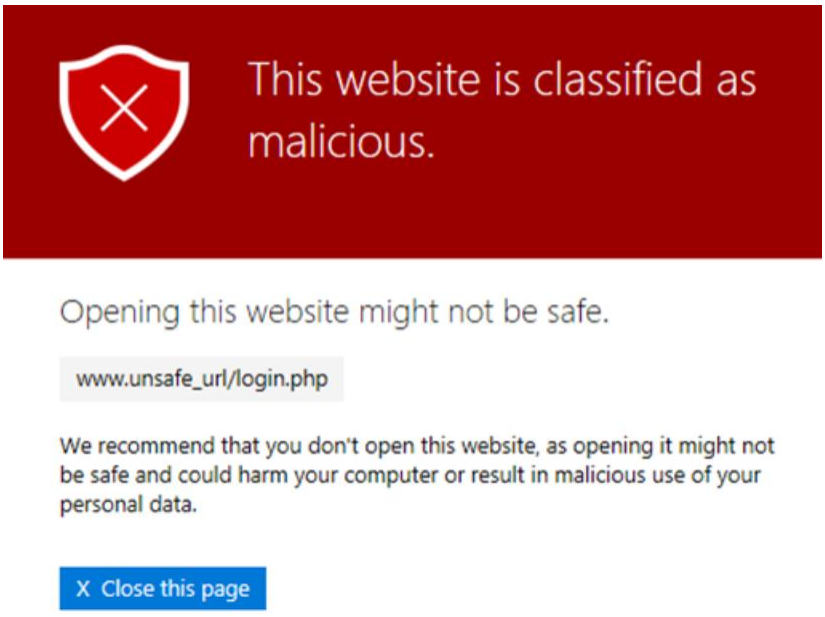
OVERVIEW & BUSINESS CASE

Microsoft 365 Solutions: Anti-malware, Office 365 Advanced Threat Protection, Intune, Conditional Access, and Windows Defender Anti-Virus

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. The data collected from the intelligent security graph spans across their entire stack and enhances their machine learning algorithms to stop malicious content at the edge before it even hits your organization. Malware trends can be seen in a single view on the Threat Dashboard in the Security Center.

Office 365 Advanced Threat Protection (ATP)

Office 365 ATP comes with safe links and safe attachment policies that can span across Exchange, Teams, SharePoint, and OneDrive. Safe links provide real-time click protection to safely detonate a malicious link in a sandbox environment before allowing a user to continue to a website. Files are scanned for malicious content and you can configure settings for dynamic delivery of messages where a user can get the body of the email while the attachment is being scanned to avoid delays.



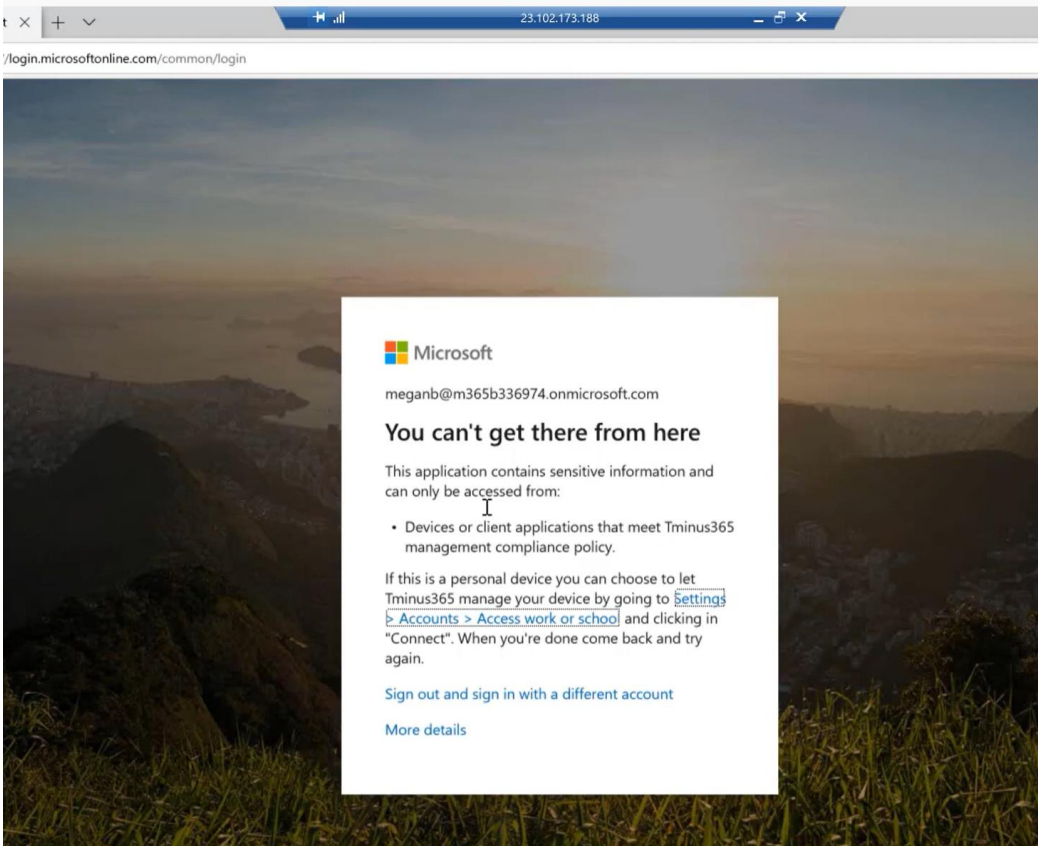
OVERVIEW & BUSINESS CASE

INTUNE AND CONDITIONAL ACCESS

To reduce supply chain risk, you need automated, timely patch updates to software. Automatic updates for Windows 10 can now be controlled with deployment rings in the Endpoint Manager admin center. You can assign different update cycles to different groups of users whose devices are enrolled in Intune.

Intune allows you to create custom configuration profiles to push out to certain devices, much like you're used to with group policies. A common profile to push out restricts removable media like USBs.

Risk containment strategies can be simplified with Intune and conditional access policies. You can deploy device compliance policies to all devices enrolled in the MDM service and additionally apply a conditional access policy that denies access to applications when a device falls out of compliance. This allows you to quickly contain an incident and work on a mitigation strategy without the pressures of wondering what corporate data is at risk.



OVERVIEW & BUSINESS CASE

RISK ANALYSIS

OBSERVABLE RISK:

- *A user clicks on a malicious link in an email message and is infected with ransomware*
- *A user is subject to a social engineering attack and then visits a malicious website where malware is download to their device*
- *A user gets a malicious message from a user impersonating someone at the company*
- *An actor spoofs an internal domain and gets sensitive data sent to him through a social engineering attack*
- *A USB device with malicious content is injected onto a device*
- *A device is compromised and you are unable to contain the incident, leading to the spread ofmalware throughout your organization*



Recommended Baseline Safeguards:

- Implement ATP safe links, safe attachments, and an anti-phishing policy
- Ensure notifications for internal users sending malware are enabled
- Review the anti-malware policy and turn on the common attachments filter
- Periodically review trends in the Threat Management Dashboard
- Create a device compliance policy for all device platforms you are going to support
- Create a device configuration profile to block removable media
- Enroll devices in Intune
- Create a conditional access policy to block access to all applications when a device is out of compliance

OVERVIEW & BUSINESS CASE



Least to Most Restrictive Actions:

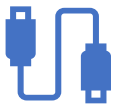
1. Set up a policy for safe links and safe attachments. Allow for user override
2. Set up a policy for safe links and safe attachments. Prevent user override. Set up a device restriction profile to block USB devices.
3. Set up a policy for safe links and safe attachments. Prevent user override. Set up a device restriction profile to block USB devices. Set up a custom anti-phishing policy for key staff in the company and configure mailbox intelligence. Set up a conditional access policy to prevent users from accessing data when their device is not in a compliant state.

CIS Sub-Control(s) Met: 8.1, 8.2 ,8.4, 8.5, 8.6

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 9: LIMITATION AND CONTROL OF NETWORK PORTS, PROTOCOLS, AND SERVICES



Description: *"Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers."*

Discovery Questions (for the IT Professional):

- Do you have any systems still using legacy authentication like IMAP, POP, SMTP, etc.?

Overview:

Threats to cloud applications are growing and traditional methods of protecting them with passwords is no longer secure enough to defend against sophisticated attacks. Multi-factor authentication (MFA) has been introduced for heightened security, but not all protocols support this method of authentication. Attackers are still able to abuse legacy protocols like IMAP and POP with brute force methods to compromise a system. Some environments still have email clients, ticketing systems, and other applications that use these protocols and password-spray attacks can easily compromise these systems. End of support has been announced for these legacy authentication methods in October 2020.

Microsoft 365 Solution: Conditional Access

Conditional access allows you to grant or block access to resources when certain conditions are met. Additional security controls like MFA can be enforced when riskier scenarios arise. Conditional access can detect what authentication methods are being used to access resources. You can specifically create a conditional access policy to block legacy authentication to all applications, but exclude or whitelist applications that you may not be ready to move yet. For those applications, it is recommended that you set a password for the application to reduce the likelihood of breach from a password-spray attack. For printers or copiers that use SMTP relay, you can "exclude" those as well from a policy that enforces MFA.

OVERVIEW & BUSINESS CASE

RISK ANALYSIS

OBSERVABLE RISK:

- *You have systems using legacy authentication and cannot enforce MFA on these accounts, making your orgnization more susceptible to an attack*
- *You are more likely at risk for brute force attacks on systems that still use legacy protocols*
- *End of support for IMAP and POP legacy authentication is October 2020. If you do not upgrade these authentication methods, you are subject to more risk*



Recommended Baseline Safeguards:

- Review all systems that still use legacy authentication and implement a strategy to move them to a modern authentication method
- Set up a conditional access policy to block legacy authentication



Least to Most Restrictive Actions:

1. Set up a conditional access policy to block all legacy authentication. Exclude all applications you know still use this protocol internally for business functions.
2. Set up a conditional access policy to block all legacy authentication. Exclude all applications you know still use this protocol internally for business functions. Give those applications passwords for additional security.
3. Set up a conditional access policy to block all legacy authentication. Upgrade all systems using legacy protocols to a modern authentication method like OAuth2.0.

CIS Sub-Control(s) Met: 9.2

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

Description: *"The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it."*

Discovery Questions to Ask (Internal to MSP):

- Do we have a SaaS backup solution in place?
- What solutions should we be backing up (e.g. email, documents, chat, etc.)?
- What RPO or RTO metrics do we want to meet?
- If we were to lose client data, what messaging do we want to provide?

Overview:

Back up and data recovery are essential secondary measures of protection in the event of a breach. The cost of downtime from a ransomware attack is often many times greater than the ransom request amount. Data recovery capabilities need to expand beyond email and move into the collaboration tools used today, such as Teams. Backups should be performed multiple times per day and should be tested periodically to ensure you can meet documented recovery time objectives (TRO) and recovery point objectives (RPO).

Note: In this section, we are not going to be talking about the M365 Business solution as this relates primarily to backup and disaster recovery scenarios.

STACK IT UP

This is a great opportunity to layer in a third-party continuity solution like **Dropsuite** for SaaS backup. Dropsuite can back up 365 emails, OneDrive, SharePoint, and even Teams chat messages. This is highly important for clients that have compliance regulations enforced.

Dropsuite

OVERVIEW & BUSINESS CASE

RISK ANALYSIS

OBSERVABLE RISK:

- *Email is deleted in Office 365 and is removed after 30 days by default; you are at risk of not being able to recover sensitive information*
- *If you lose access to critical systems, the cost of downtime will cripple the company*
- *You are unable to back up Teams chat messages for litigation cases that may result in the future*
- *A ransomware infection results in the loss of some or all corporate data.*



Recommended Baseline Safeguards:

- Implement a SaaS backup solution
- Ensure backups occur multiple times per day
- Periodically test recovery to maintain documented RPOs and RTOs

CIS Sub-Control(s) Met: 10.1, 10.2

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 11: SECURE CONFIGURATION FOR NETWORK DEVICES, SUCH AS FIREWALLS, ROUTERS, AND SWITCHES



Description: *"Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings."*

Note: This is not a control we will be covering as it is not in scope for the M365 Business offering.

CIS CONTROL 12: BOUNDARY DEFENSE



Description: *"Detect, prevent, and correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data."*

Discovery Questions to Ask (for the IT Pro):

- Do you allow personal devices to join your network?
- What safeguards do you have in place for infected devices that join the network?
- What additional security controls do you want to put into place when a user is off-network?
- Are applications with corporate data protected on unmanaged devices?
- Do you know if a user is saving corporate data to a personal location?

Overview:

With the rise of BYOD policies and remote workers, businesses need to ensure additional safeguards are in place to only allow trusted, healthy devices on the corporate network. In today's environment, a user is more likely to get breached outside of your network and bring an infected device back inside your trusted perimeter. However, tightening your existing infrastructure or blocking access to data on personal devices is likely going to cause extreme frustration with today's employees who want the flexibility to work anywhere, on any device. To handle new threats, you need a solution that applies different controls based on the risk associated to an off-netork user or personal device compared to users and devices on the corporate network.

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

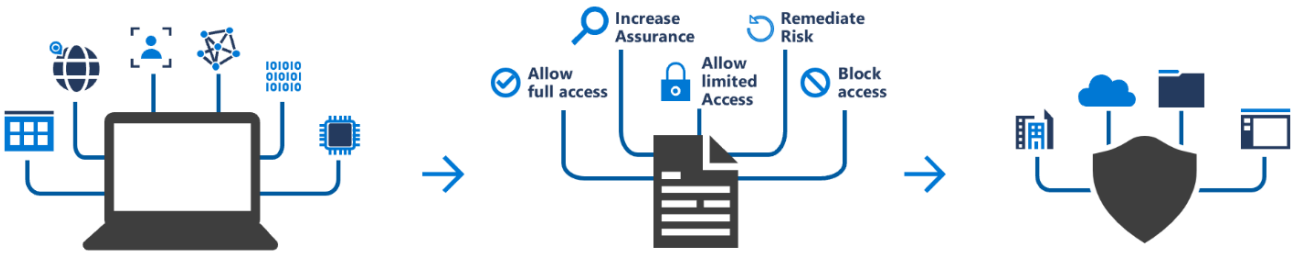
Microsoft 365 Solutions: Conditional Access and Intune

Conditional access allows you to create policies based on a set of conditions that include:

- Users/Groups: To whom do you want to scope this policy? Is there anyone you want to exclude?
- Applications: To which applications does this policy apply? Consider apps that have the most sensitive data.
- Devices: Are there certain device platforms to which you want apply this policy? Do you not want to grant access to a device that isn't enrolled in Intune?
- Locations: Is this user on your network?

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

- Let users access applications unimpeded (in low risk scenarios such as the user being on-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 (in scenarios where an app is too critical to be accessed off network, a user's device is comprised, an app uses legacy authentication, an MFA prompt failed, etc.)



OVERVIEW & BUSINESS CASE

MAM POLICIES

Intune's Mobile Application Management (MAM) technologies enable you to create policies across Windows, Android, and iOS devices to protect corporate data. You can define your managed applications and which permissions users have around those applications, even on unmanaged devices. This is a great way to prevent data leakage to untrusted locations. Conditional access policies can be put in place to force users to only use these trusted applications.

RISK ANALYSIS

OBSERVABLE RISK:

- *An infected personal device joins the corporate network and malware spreads throughout the organization*
- *You block the access to data on personal devices and get blamed for inhibiting productivity*
- *The company has remote workers all over the country and you are not sure what protections are set up on their personal devices*



Recommended Baseline Safeguards:

- Gather a list of all hardware devices that the company manages
- Determine what device platforms you will manage (Windows, iOS, macOS, Android)
- Enroll devices in Intune
- Create a device compliance policy for each platform
- Create a conditional access policy that grants access to corporate resources when the device is in a compliant state
- Prevent access to your corporate network by unmanaged or unhealthy devices
- Create an app protection policy for iOS and Android to manage applications on unmanaged devices

OVERVIEW & BUSINESS CASE



Least to Most Restrictive Actions:

1. Set up app protection policies to manage applications that access corporate data. Devices do not need to be enrolled in MDM. Corporate data will be encrypted and you will have the ability to remotely wipe data. You are still susceptible to devices being infected with malware and spreading it to your corporate network if they are able to join.
2. Set up app protection policies for personally owned devices and set up a policy to not allow these devices to join to your network.
3. Require that all devices accessing corporate data are enrolled in Intune and are in a compliant state.

CIS Sub-Control(s) Met: 12.11, 12.12

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 13: DATA PROTECTION



Description: *"The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information."*

Discovery Questions:

- What applications or portals are employees using to access corporate data?
- Where is sensitive data stored today?
- How do you classify sensitive data?
- Are users accessing corporate data from personal devices?
- What would be the cost to the company if sensitive data was leaked?
- What safeguards do you have in place to prevent accidental deletion of sensitive information?
- Do users access email through their personal devices?
- If a user leaves, how do you know they don't have corporate data stored on their personal device?
- Are there business-critical pieces of data that would leave you exposed if a personal device was compromised?
- Are you compliant if data is leaked to unmanaged applications?
- Do employees have access to corporate apps after they leave the company? How do you know whether they do or not?
- Can you remotely wipe corporate data when someone leaves or if their device is lost or stolen?

Overview:

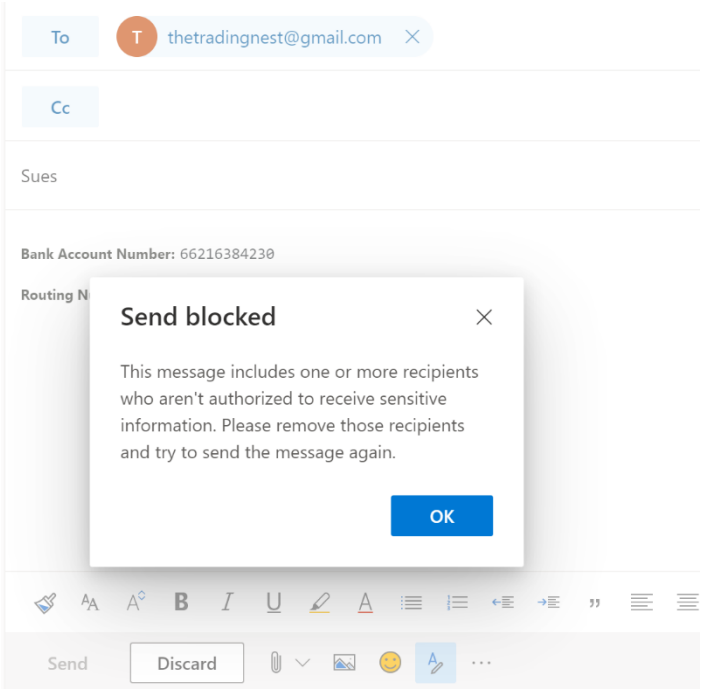
As business moves to a larger population of remote workers using personal devices, it is more important than ever to implement policies to protect corporate data. Attackers can often breach an organization and immediately gain access to sensitive data because additional security controls are not in place. When exploring sensitivity levels for data, organizations need to put together a list of the key types of data and their overall importance to the organization. Additional security controls can then be put into place that defines where data is stored, who has access to it, and permission levels for sharing

outside the organization. For organizations that must meet regulatory controls, it is important to put in controls to reduce exfiltration of sensitive data due to human error.

Microsoft 365 Solutions: Data Loss Prevention, Azure Information Protection, Intune, and Email Archiving

Data Loss Prevention (DLP) Policies

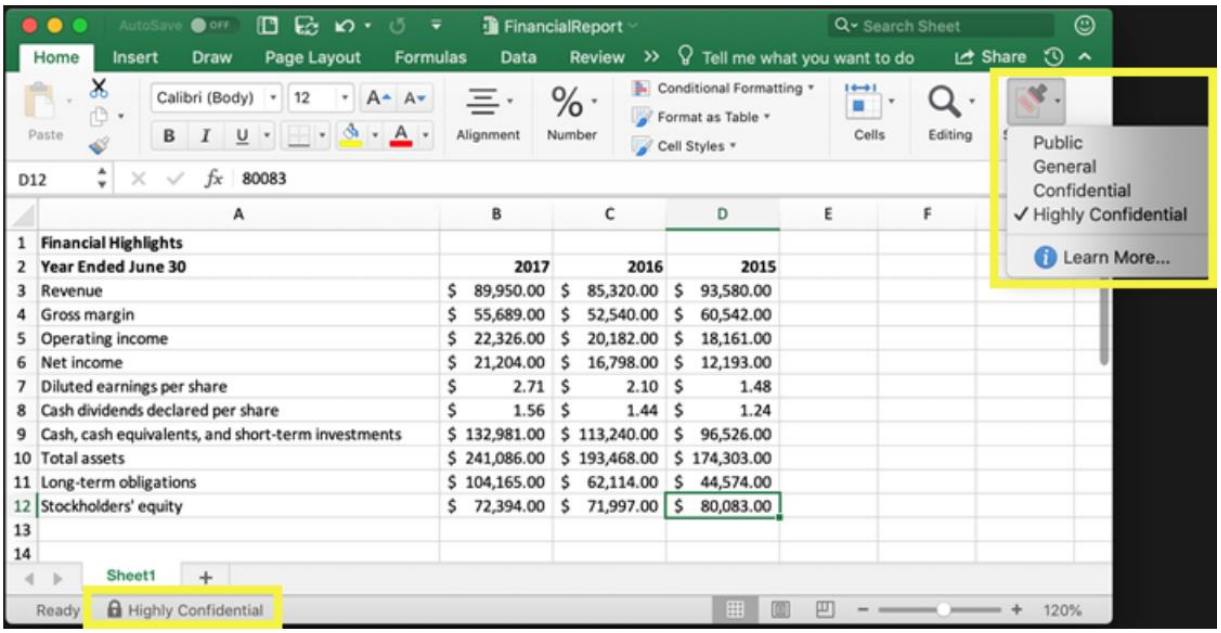
DLP policies allow you to automatically detect sensitive information across Exchange, SharePoint, OneDrive, and Teams and take protective action when that information is shared. This action could include a policy tip, applying encryption, or blocking the action completely. Sensitive data templates are preconfigured when setting up a policy that relates to common compliance regulations.



OVERVIEW & BUSINESS CASE

Azure Information Protection (AIP)

AIP 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. Custom retention policies can be set based on the label applied. Additionally, you can configure the option to prompt users to provide a reason when they select a label that has a lower sensitivity level than the original.

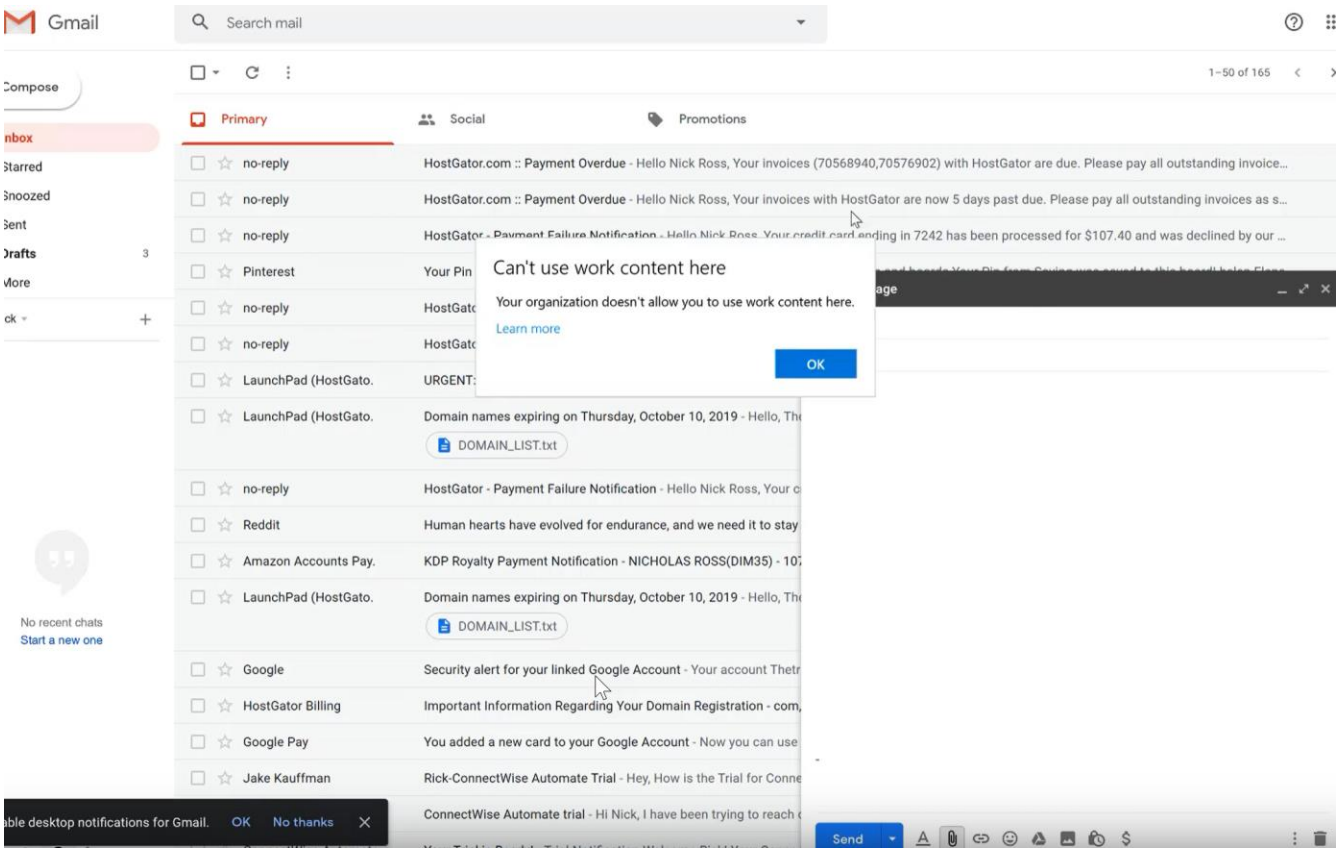


OVERVIEW & BUSINESS CASE

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 data from being saved to unmanaged applications and restrict cut/copy/paste abilities. All corporate data with app protection policies can be encrypted on personal devices and remotely wiped at any time. Additional security can be applied for users accessing applications on mobile devices, requiring them to provide a PIN to access the resources.

Ex. App protection policies preventing users from attaching corporate documents in their personal Gmail accounts:



OVERVIEW & BUSINESS CASE

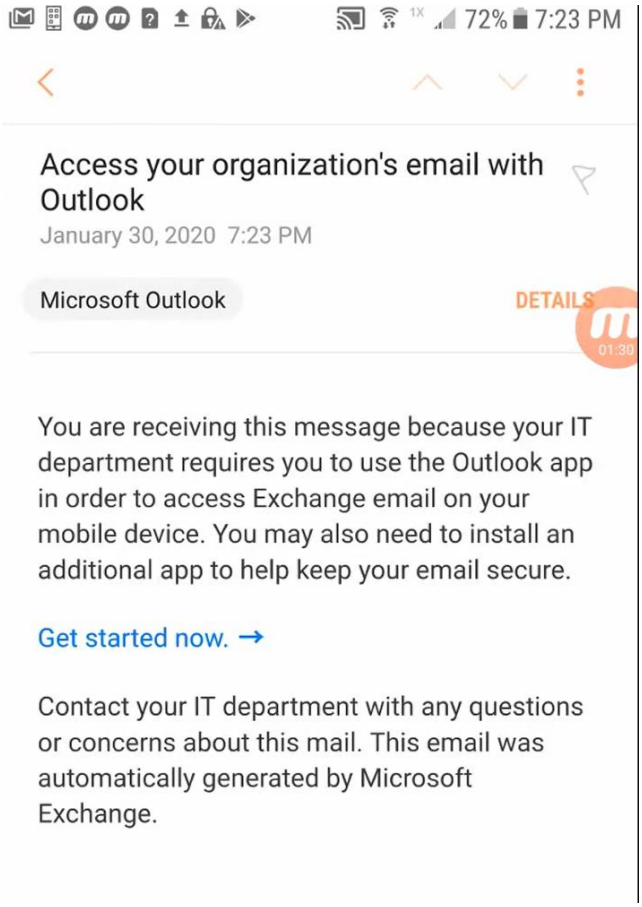
Retention

Unlimited email archiving can be enabled for any mailbox within M365. Custom retention tags can be created and applied automatically or on demand to email or documentation. Litigation holds can be placed for any user across the entire solution stack, including Teams.

Conditional Access

Conditional access allows you to apply certain controls to applications to restrict access when a user is not on your network or a managed device. Policies can be put into place to require the use of a managed client application when on a personal device.

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



OVERVIEW & BUSINESS CASE

RISK ANALYSIS

OBSERVABLE RISK:

- *Sensitive information is being shared internal or externally without your knowledge*
- *Sensitive information is being shared in an insecure manner outside the organization*
- *Sensitive information is being saved in unmanaged locations*
- *Sensitive information is being sent in an insecure manner due to human error*
- *Sensitive information is not retained or archived properly*
- *Sensitive information is being accessed unsecurely on unmanaged devices*
- *You are unable to place a litigation hold on users' information and that information is deleted*



Recommended Baseline Safeguards:

- Determine where data is stored and define classification labels for sensitive information
- Determine what sensitive information is being shared internally and externally
- Create Azure Information Protection labels and define custom policies for access, retention, encryption, and sharing permissions
- Create a data loss prevention policy
- Create a conditional access policy to prevent access to unmanaged client applications when a user is not on your network or is using an unmanaged device
- Create a conditional access policy to block access to certain applications with highly critical business data when a user is trying to access them from an unmanaged device
- Review the default retention policies and customize them for business needs
- Turn on email archiving
- Create an app protection policy for Windows, iOS, and Android

OVERVIEW & BUSINESS CASE

- Enroll devices in Intune
- Ensure external domains are not allowed in Skype or Teams
- Ensure external file sharing in Teams is only enabled for approved cloud storage services
- Ensure document sharing is being controlled by domains with whitelist or blacklist
- Block OneDrive for Business sync from unmanaged devices
- Ensure expiration time for external sharing links is set
- Ensure that external users cannot share files, folders, and sites they do not own



Least to Most Restrictive Actions:

1. Set up app protection policies to manage applications that access corporate data. Devices do not need to be enrolled in MDM. Classify content with Azure Information Protection without using any protection settings. You can use this classification to generate usage reports and see activity data for your sensitive content. Based on this information, you can always choose to apply protection settings later. Set up data loss prevention policies to detect specific types of sensitive data and provide policy tips only. You can track the number of times a policy was triggered in the Security and Compliance Center.
2. Set up app protection policies and a conditional access policy to require a client managed app to access corporate data. For Azure Information Protection, set a policy that requires justification to change a classification. Set a data loss prevention policy that blocks the user from sending sensitive information outside the organization, but allows for user override with justification.
3. Require that all devices be enrolled in Intune to access corporate data. Set a conditional access policy to prevent access to all applications if the device is not enrolled in Intune. Set an Azure Information policy to require that a label be applied upon saving a document. For documents labeled "confidential," block sending to external domains and prevent user override. Set up a data loss prevention policy to block users from sending sensitive data to external domains and prevent user override.

CIS Sub-Control(s) Met: 13.1, 13.2, 13.5

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 14: CONTROLLED ACCESS BASED ON THE NEED TO KNOW



Description: *"The processes and tools used to track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification."*

Discovery Questions:

- How are you classifying sensitive data?
- How do you protect sensitive information from leaving the organization today?
- What are the retention policies in place today around certain classification types?
- Is sensitive information encrypted when it leaves the organization?

Overview:

While some data is leaked or lost as a result of theft or espionage, the vast majority of data loss results from poorly understood data practices, a lack of effective policy architectures, and user error.[1] Every business should understand what sensitive information exists in their company, where it resides, and who needs access to it. All data should be classified and access rights should be scoped only to the users who need to interact with that data. Policies need to be put into place to reduce human error, especially when information is being shared externally. Data encryption at rest and in transit brings a certain level of assurance even if data is compromised.

OVERVIEW & BUSINESS CASE

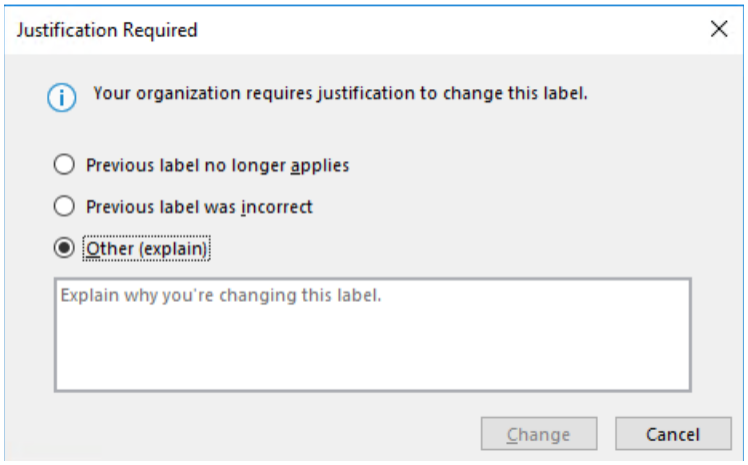
Microsoft 365 Solutions: Encryption, Azure Information Protection, Intune, Data Loss Prevention, and Conditional Access

Encryption

Data is encrypted at rest and in transit across Microsoft's cloud. Device encryption for Windows 10 devices is available and devices enrolled in Intune can have device compliance policies that require Bitlocker. Device profiles can be set up that automatically configure Bitlocker without IT intervention.

Azure Information Protection (AIP)

AIP 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. Custom retention policies can be set based on the label applied and encryption can be applied to emails or documents with certain labels. You can scope the policies and access rights around these labels to certain users within the organization. If a user tries to change a label, you can require them to provide justification for additional auditing records.

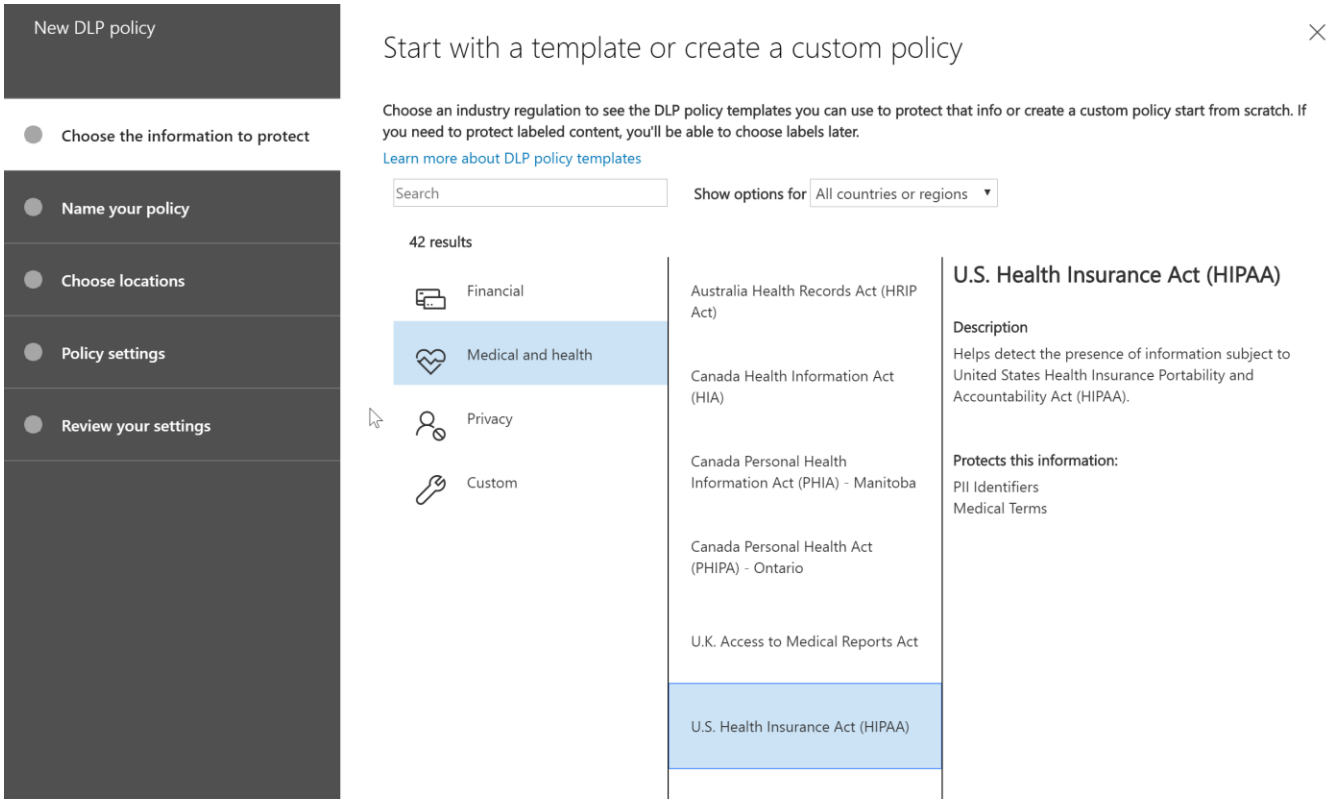


CIS CONTROLS WITH MICROSOFT

Overview & Business Case

Data Loss Prevention Policies

DLP 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, applying encryption, or blocking the action completely. Sensitive data templates are preconfigured when setting up a policy that relate to common compliance regulations. You can track records for when a DLP policy was triggered and identify user overrides.



OVERVIEW & BUSINESS CASE

RISK ANALYSIS

OBSERVABLE RISK:

- *Sensitive information is being shared internal or externally without your knowledge*
- *Sensitive information is being shared in an insecure manner outside the organization*
- *Sensitive information is being saved in unmanaged locations*
- *Sensitive information is not being encrypted at rest or in transit*
- *Sensitive information is being sent in an insecure manner due to human error*
- *Sensitive information is not retained or archived properly*
- *Sensitive information is being accessed unsecurely on unmanaged devices*



Recommended Baseline Safeguards:

- Determine where data is stored and define classification labels for sensitive information
- Determine what sensitive information is being shared internally and externally
- Create Azure Information Protection labels and define custom policies for access, retention, encryption, and sharing permissions
- Create a data loss prevention policy
- Create a conditional access policy to prevent access to unmanaged client applications when a user is not on your network or is using an unmanaged device
- Create a conditional access policy to block access to certain applications with highly critical business data when a user is trying to access them from an unmanaged device
- Review the default retention policies and customize them for business needs
- Turn on email archiving
- Create an app protection policy for Windows, iOS, and Android
- Enroll devices in Intune

OVERVIEW & BUSINESS CASE

- Ensure external domains are not allowed in Skype or Teams
- Ensure external file sharing in Teams is only enabled for approved cloud storage services
- Ensure document sharing is being controlled by domains with whitelist or blacklist
- Block OneDrive for Business sync from unmanaged devices
- Ensure expiration time for external sharing links is set
- Ensure that external users cannot share files, folders, and sites they do not own



Least to Most Restrictive Actions:

1. Set up app protection policies to manage applications that access corporate data. Devices do not need to be enrolled in MDM. Classify content with Azure Information Protection without using any protection settings. You can use this classification to generate usage reports and see activity data for your sensitive content. Based on this information, you can always choose to apply protection settings later. Set up data loss prevention policies to detect specific types of sensitive data and provide policy tips only. You can track the number of times a policy was triggered in the Security and Compliance Center.
2. Set up app protection policies and a conditional access policy to require a client managed app to access corporate data. For Azure Information Protection, set a policy that requires justification to change a classification. Set a data loss prevention policy that blocks the user from sending sensitive information outside the organization but allows for user override with justification.
3. Require that all devices be enrolled in Intune to access corporate data. Set a conditional access policy to prevent access to all applications if the device is not enrolled in Intune. Set an Azure Information policy to require that a label be applied upon saving a document. For documents labeled "confidential," block sending to external domains and prevent user override. Set up a data loss prevention policy to block users from sending sensitive data to external domains and prevent user override.

CIS Sub-Control(s) Met: 14.1, 14.4, 14.5, 14.6, 14.7, 14.8 14.9

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 15: WIRELESS ACCESS CONTROL



Description: *"The processes and tools used to track, control, and correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems."*

Discovery Questions:

- Are users able to connect to public Wi-Fi networks?
- Do you have any restrictions for public access points?
- Is Wi-Fi traffic encrypted?
- Is uour SSID easily identifiable?
- Do you restrict Wi-Fi access and provide a guest network?

Overview:

Many organizations have made the switch from wired to wireless technologies for connecting to the Internet. In some cases, this has had a negative impact on their security posture because some businesses fail to perform adequate vulnerability assessments on their wireless network. These wireless network vulnerabilities could easily be exploited to steal sensitive data, take control of a router or connected device, or install malware.

Visitors to a hotel, coffee shop, bar, retail outlet, or restaurant now expect Wi-Fi to be provided free of charge – but they can often be at risk. Attackers create fake access points to these public Wi-Fi networks, closely aligning the name of the SSID with the establishment. Packet sniffing is one of the most commonly used wireless attack methods and many public locations are susceptible to this type of attack because of unencrypted traffic.

Microsoft 365 Solution: Intune

Microsoft Intune includes built-in Wi-Fi settings that can be deployed to users and devices in your organization. These settings include defining the SSID, defining the security type (e.g. WPA, WPA, Personal), and giving the ability to connect automatically when in range. They can be assigned to different users and groups. Once assigned, users gain access your organization's Wi-Fi network without configuring it themselves.

OVERVIEW & BUSINESS CASE

You can also define a device restriction profile that allows you to prevent users from connecting to Wi-Fi networks that aren't deployed by the defined configuration. This would prevent a user from connecting to an untrusted public access point.

RISK ANALYSIS

OBSERVABLE RISK:

- *Your guest network is not isolated and attackers are able to breach the internal network*
- *Your wireless traffic is not encrypted, leaving your network and data vulnerable*
- *Users are susceptible to attacks on unsecured public connections*
- *Users are susceptible to fake Wi-Fi access points*



Recommended Baseline Safeguards:

- Enroll devices in Intune
- Create a Wi-Fi configuration profile for every device platform you want to support
- Create a Wi-Fi configuration profile for each SSID that you want to support
- Create a device restriction profile to prevent users from accessing SSIDs that are not defined by your Intune profiles
- If you have a client that provides a free, wireless network to their customers, ensure the SSID is unique and that all traffic is encrypted
- Apply conditional access policies for additional security like MFA when a user is not on your network

OVERVIEW & BUSINESS CASE



Least to Most Restrictive Actions:

1. Create a Wi-Fi configuration profile for every device platform you want to support and push out to all enrolled devices
2. Apply conditional access policies for additional security like MFA when a user is not on your network. Create a separate wireless network for use by personal and untrusted devices.
3. Require that all devices be enrolled in Intune to access corporate data. Set a conditional access policy to prevent access to all applications if the device is not enrolled in Intune. Create a device restriction profile to prevent users from accessing SSIDs that are not defined by your Intune profiles.

CIS Sub-Control(s) Met: 15.1, 15.2, 15.4, 15.5, 15.10

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 16: ACCOUNT MONITORING AND CONTROL



Description: *"Actively manage the life cycle of system and application accounts – their creation, use, dormancy, and deletion – in order to minimize opportunities for attackers to leverage them."*

Discovery Questions:

- How many accounts do you have with over sixty days of inactivity?
- What are your policies around access to corporate data for contractors and third parties?
- Are there any contractors that still have access to corporate data?
- How often do you review access controls for users' rights to applications around the organization?
- What are your procedures when an employee leaves the company?

Overview:

Inactive accounts can be easily exploited by attackers to impersonate legitimate users at a company, making the discovery of the malicious attacker much more complicated. Interactions with outside contractors can also create a security concern, so there needs to be defined restrictions on what data contractors can access and for what duration.

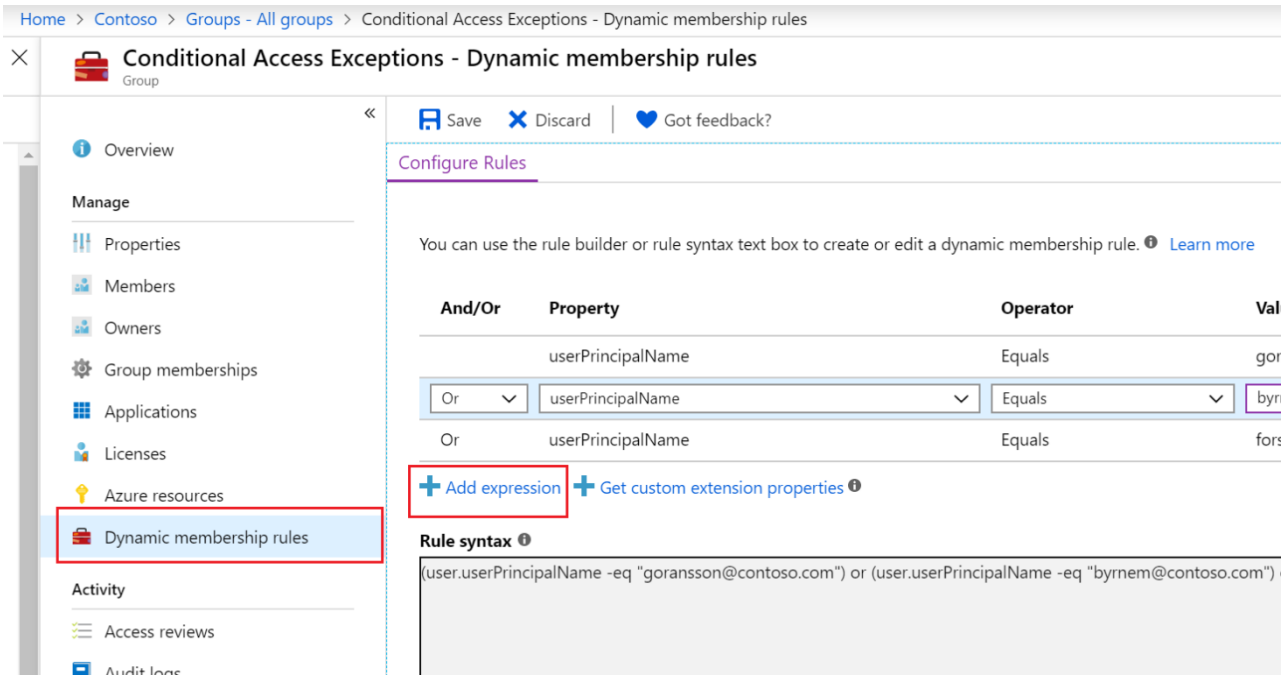
Physical devices need to have a well-defined policy for minutes of inactivity to before moving to a lock screen where a password is required. This is important for users in the office as well as remote users who may be accessing corporate data in a public location.

OVERVIEW & BUSINESS CASE

Microsoft 365 Solutions: Azure AD, Conditional Access, and Intune

Azure Active Directory (AD) and Conditional Access

Azure AD allows you to track user activity and configure dynamic groups based off of certain attributes such as job department. Additionally, you can add applications and configure them for single sign-on access. You can assign these applications to the dynamic group, immediately granting or revoke access throughout the user's lifecycle. This allows you to automate more of the change management process and helps avoid human error in access removal.



By combing Azure AD with conditional access, you can force multi-factor authentication (MFA) to all users across the company. This ensures that even if an inactive user's account is compromised, they will still not be able to gain access to corporate data. Azure Business-to-Business, or Azure B2B, enables organizations to work securely with other organizations even if they are not using Azure AD, so that you can invite external users to access specific pieces of data in your organization. Using conditional access, you can scope what applications those users have access to and require them to use MFA.

Intune

For devices enrolled in Intune, you can create a device profile policy to set the number of minutes of inactivity before lockout and require a passcode, biometric (e.g. Windows Hello), or PIN to regain access.

CIS CONTROLS WITH MICROSOFT

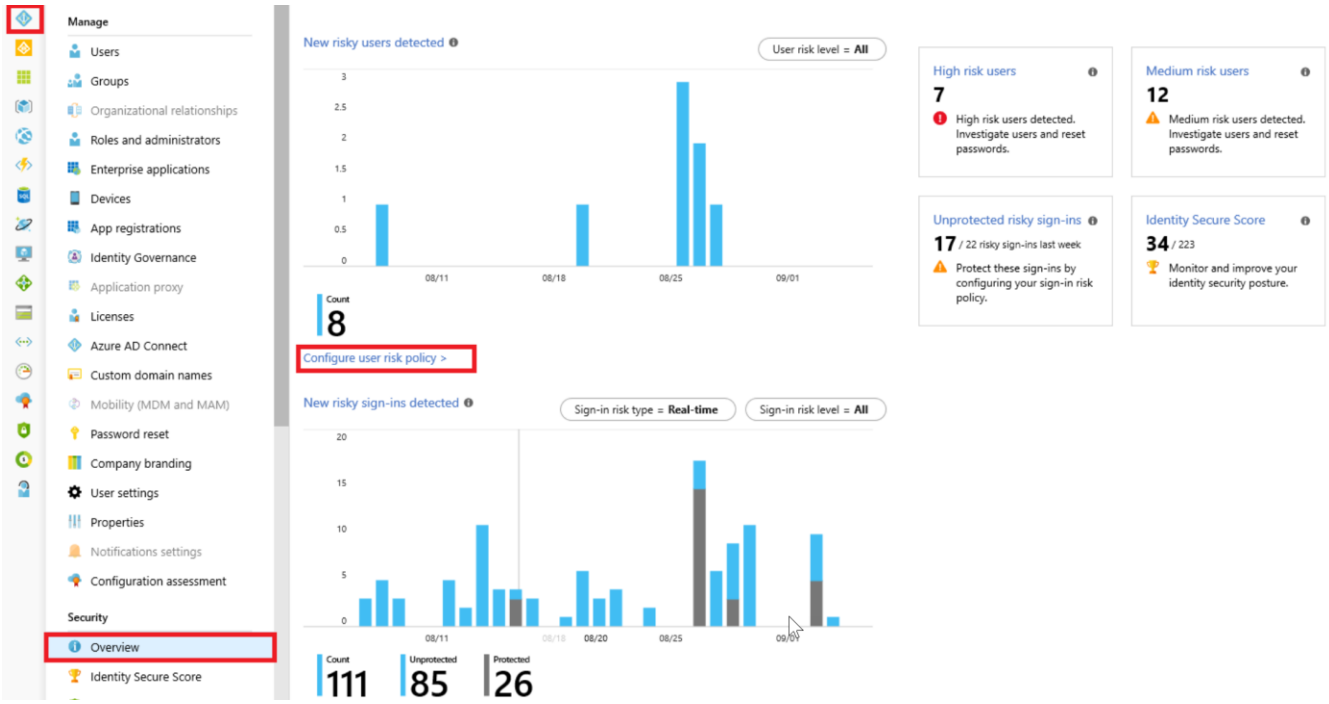
OVERVIEW & BUSINESS CASE

UPSELL OPPORTUNITY: AZURE ACTIVE DIRECTORY PLAN 2 - $9/USER/MONTH

Azure Active Directory Plan 2 can be an add-on to any base plan and includes premium features for identity protection and access control. Two technologies in this offering that we will highlight are Azure Privileged Identity Management and Azure Identity Protection.

Azure Privileged Identity Management (PIM) allows for "just in time" and "just enough" access for elevation of privileges. Users can activate certain roles for a limited amount of time to perform administrative tasks. Reasons for elevation must be provided when the role is activated to create a complete audit log of activities. Access Rreviews can scheduled to evaluate elevated privileges on a periodic basis to follow a model of least privilege.

Azure Identity Protection (AIP) automates the detection and remediation of identity-based risk. Leveraging data signals and machine learning, users can be identified as a risk based on certain classifications such as atypical travel, anonymous IP, unfamiliar sign-in, and more. Additionally, you gain deeper reporting into things such as inactive accounts and can create alerts based off this activity.



OVERVIEW & BUSINESS CASE

RISK ANALYSIS

OBSERVABLE RISK:

- *An inactive user's account gets compromised and an attacker gains undetected access to the organization*
- *A contractor continues to have access to corporate data even after their contract is terminated*
- *Employee access to critical applications is not removed when they leave the company*
- *A user leaves their computer unlocked in a public location and corporate data is compromised*



Recommended Baseline Safeguards:

- Periodically review accounts with inactivity and remove stale accounts
- Configure applications for SSO in the Azure AD portal
- Configure dynamic groups with attributes that match job title
- Assign access to applications based on dynamic groups
- Create a conditional access policy to force MFA for all users when they are not on your network
- Create a conditional access policy to grant access to external users only for the applications they need, requiring MFA
- Convert users to a shared mailbox when they leave the company and reset the password
- Ensure expiration time for external sharing links is set
- Ensure that external users cannot share files, folders, and sites they do not own
- Create a device profile to set the minutes of inactivity on a device to five and require a password, PIN, or biometric to regain access

OVERVIEW & BUSINESS CASE

Least to Most Restrictive Actions:

1. Create a conditional access policy to force MFA for all users when they are not on your network.
2. Create a conditional access policy to force MFA for all users when they are not on your network. Create a device profile to set the minutes of inactivity on a device to 15 minutes and require a password, PIN, or biometric to regain access.
3. Create a conditional access policy to require users to be on your network to access corporate applications. Require MFA in all locations. Do not allow browser sessions to persist. Create a device profile to set the minutes of inactivity on a device to 5 minutes and require a password, PIN, or biometric to regain access.

CIS Sub-Control(s) Met: 16.1, 16.2, 16.3, 16.4, 16.6, 16.7,16.8, 16.9, 16.11

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 17: IMPLEMENT A SECURITY AWARENESS AND TRAINING PROGRAM



Description: *"For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs."*

Discovery Questions to Ask (Internal to MSP):

- Do you provide security awareness training to end users?
- Do users with elevated privileges understand the importance of continual security training?
- Does everyone at the company feel empowered with good cyber defense habits and hygiene?

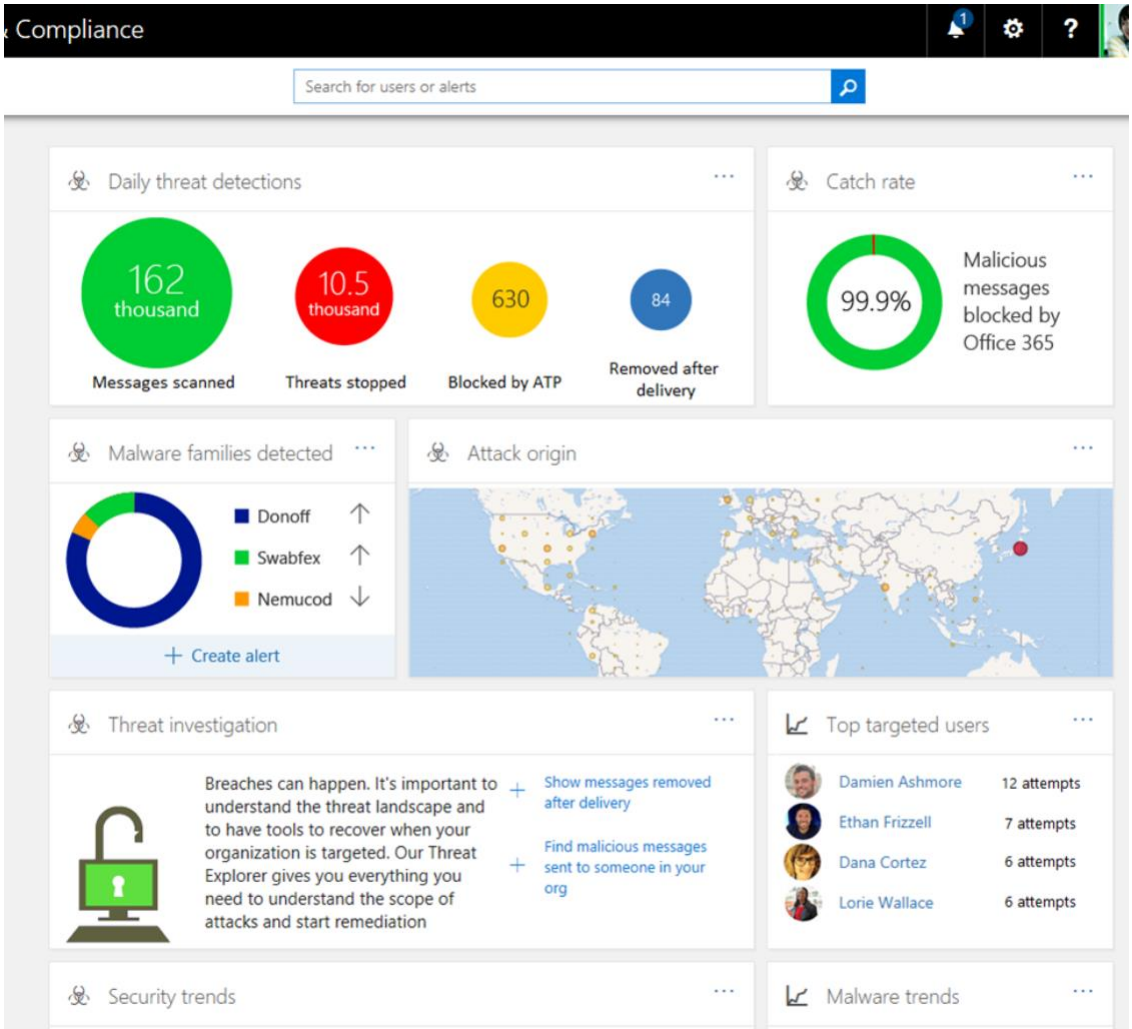
Overview:

Even with all the safeguards mentioned so far from a technical standpoint, the actions of people within an organization are critical to the success of a cyber defense program. There are ever-evolving threats to keep up with and users within the organization must be trained on a periodic basis to be able to identify and respond to new threats that arise. The types of training you deliver should be targeted to certain users or departments within the organization to maximize their benefits. It's extremely important to perform a skills gap analysis around cybersecurity on an on-going basis. Giving users a clear communication path for reporting incidents is extremely important for threat containment.

OVERVIEW & BUSINESS CASE

MICROSOFT 265 SOLUTION: Security Center

Within the Microsoft Security Center, you can view a threat dashboard which identifies attack trends within the tenant such as phishing attempts, malware detection, impersonation attempts, and more. Analyzing these attack trends on a periodic basis will give you greater insight into where you should apply additional policies or where you need to direct more training.



CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

STACK IT UP

Office 365 Advanced Threat Protection (ATP) comes with an attack threat simulator with enterprise plans, but not with M365 Business. This is a good opportunity to stack a third-party security training tool like **Breach Secure Now** to train end users.

Breach BSN Secure Now!

RISK ANALYSIS

OBSERVABLE RISK:

- *Users do not receive adequate training on cybersecurity threats, increasing the likelihood of getting breached*
- *Users at the company do not have an easy way of communicating attack attempts, suspicious activity, or a breach so you do not respond in time*

Recommended Baseline Safeguards:

- Perform a skills gap analysis on a periodic basis
- Security training is specific, tailored, and focused based on the specific behaviors and skills needed by the workforce, depending on their job role and responsibility
- Training is repeated periodically, and measured and tested for effectiveness
- Training is updated regularly
- Training includes information on secure data handling
- Training includes rationale for good security behaviors and skills to help increase adoption and discourage risky work-arounds

CIS Sub-Control(s) Met: 17.1, 17.2, 17.3, 17.4, 17.8

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY



Description: *"Manage the security lifecycle of all inhouse-developed and acquired software in order to prevent, detect, and correct security weaknesses."*

Discovery Questions to Ask (Internal to MSP):

- How do we test for vulnerabilities across all of our software applications?

Overview:

Attackers consistently look for vulnerabilities to exploit in software applications. With the rise of SaaS applications, you need additional tools and controls in place to ensure action is taken immediately when vulnerabilities are detected.

STACK IT UP

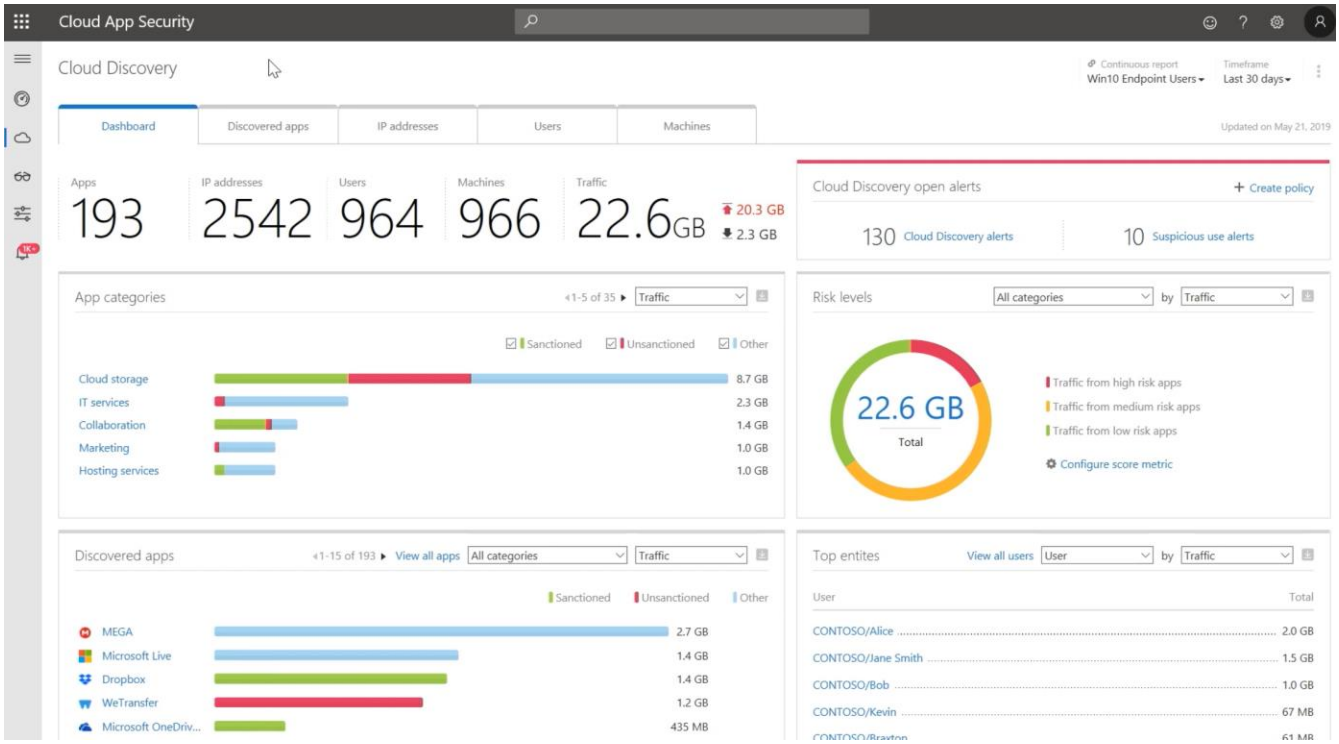
Microsoft 365 Business does not have a solution that directly solves for this control. For this reason, we will not be providing a risk analysis with observed risk and recommended safeguard. This is a good opportunity to stack a third-party security tool like **Novacoast novaSOC** for vulnerability management across software applications. novaSOC is a multi-tenant solution that can integrate with your PSA tool to provide alerting capabilities. novaSOC creates an inventory of every application installed and references published common vulnerability and exposure (CVEs). If a security update is published, an alert/ticket will be generated for an admin.

CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

UPSELL OPPORTUNITY: CLOUD APP SECURITY $3.50/USER/MONTH

- **Discover and control the use of shadow IT**: Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, then assess the risk levels and business readiness of more than 16,000 SaaS apps against more than 80 risks. Start managing these apps and services to ensure security and compliance.
- **Protect sensitive information anywhere in the cloud:** Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real-time across all your cloud apps.
- **Protect against cyberthreats and anomalies:** Detect unusual behavior across cloud apps to identify ransomware and compromised users or rogue applications, analyze high-risk usage, and automatically remediate to limit the risk to your organization.
- **Assess the compliance of your cloud apps:** Assess if your cloud apps meet relevant compliance requirements including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps and limit access to regulated data.



CIS CONTROLS WITH MICROSOFT

OVERVIEW & BUSINESS CASE

CIS CONTROL 19: INCIDENT RESPONSE AND MANAGEMENT



Description: *"Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems."*

Discovery Questions to Ask (Internal to MSP):

- How do we triage incidents that come through from our clients?
- What is our time to acknowledge (TTA) for certain types of events?
- What is our average time to remediate (TTR)?
- How many incidents have automated remediation versus manual?
- How many incidents cause escalations between our support tiers?
- Are roles and responsibilities defined when an incident occurs both internally and with the client?
- Are we consistent with how we respond when a client opens a ticket?
- Do we have incident categories 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?
- Does our organization ever do a retroactive meeting, both internally and at the client site, for certain incidents or breaches?
- How do we document lessons we have learned from previous incidents?
- Do new users to our company have easy access to this information if they search for it?
- What metrics do we want to track for incident response?

CIS CONTROLS WITH MICROSOFT

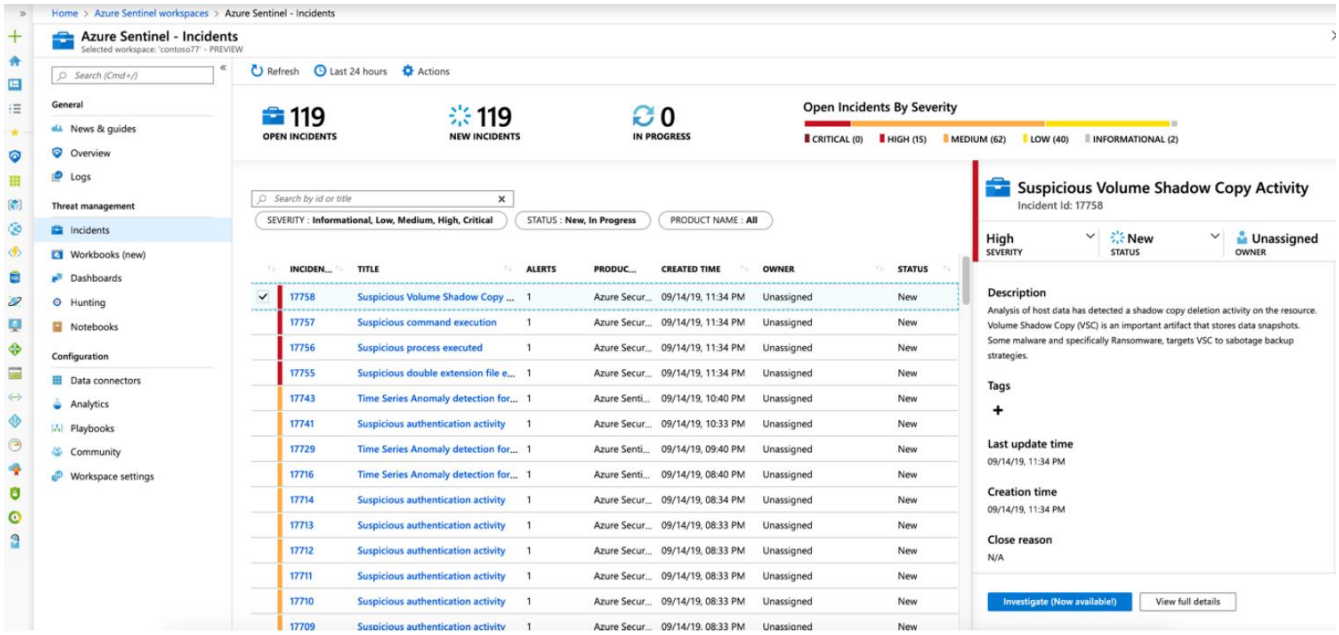
OVERVIEW & BUSINESS CASE

OVERVIEW

A strategy for procedures, reporting, responsibilities, containment, and communications needs to be in place *before* an incident occurs. Being able to manage, contain, and recover from a cybersecurity attack is essential in your practice as an IT professional. Proper documentation needs to be in place for both known vulnerabilities and incidents so that you are able to scale your business to new technicians who join the company. After defining your policies for incident response and the metrics you want to track, periodic scenario-based training should be conducted to increase efficiencies.

UPSELL OPPORTUNITY: AZURE SENTINEL

Azure Sentinel is Microsoft's security information event management (SIEM) and security orchestration automated response (SOAR) solution. Sentinel allows you to connect all of your security sources (not just Microsoft) and consolidates the data in one location. It has automated investigation, detection, and response capabilities to minimize the number of alerts you respond to. Pricing for Azure Sentinel is based on the volume of data ingested for analysis. Click here for the pricing calculator.



OVERVIEW & BUSINESS CASE

Recommended Baseline Safeguards:

- 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.
- Make sure roles and responsibilities are clearly defined and communicated for an incident.
- Review ticket correspondence and ensure consistent messaging and procedures are enforced.
- Select metrics you would like to track for incident response. Recommended metrics are time to acknowledge, time to resolution, incidents remediated automated vs manual, and escalations between support tiers.
- Review how Microsoft's solution fits in your security stack. Classify incidents based on severity and periodically review against the changing security landscape.
- Review your process for how you document new vulnerabilities and threats that emerge in the companies you manage.
- Ensure that you define how to contain each type of incident that can occur.
- Start conducting retroactive meetings internally for larger incidents (if you are not already) and document steps you are going to take to avoid mistakes or oversights in the future.

OVERVIEW & BUSINESS CASE

CIS CONTROL 20: PENETRATION TESTS AND RED TEAM EXERCISES

Description: *"Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker."*

Discovery Questions to Ask (Internal to MSP):

- Do we conduct regular penetration test?
- How can we test the ease of attack for known vulnerabilities across the organization?

Overview:

After an organization has taken the time to implement all the policies, procedures, and technical safeguards to protect their company, the next logical step is to perform periodic penetration tests against the company. Attackers often look to exploit the gap of defined internal defenses and the continued maintenance of those defenses. Penetration test should be conducted with a clear scope and rules for engagement in a well-defined contract. Penetration testers usually look for vulnerabilities that can be defined in an organization and demonstrate how effectively or ineffectively they held up through various attacks. Red Team exercises take a comprehensive approach across the full spectrum of organization;s policies, processes, and defenses in order to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels.[1] Penetration tests and Red Team exercises should be performed by mature organizations. The results provided should improve overall business practices and security posture.

OVERVIEW & BUSINESS CASE

NEXT STEPS

We hope this guide has provided you some guidance on mapping Microsoft 365 Business solutions to the CIS Controls and brought some considerations around your existing cybersecurity policies. Understanding these solutions should help you prioritize which safeguards you need to put in place. Here are some targeted next steps:

1. Start with Compliance!

The upsell angle of these solutions needs to focus on compliance. Almost every organization is accessing and sharing data in an insecure manner. Asking clients about data loss from personal cell phones can be very eye-opening, whether or not they fall under compliance regulations. Help clients understand where they are exposed and evaluate the cost of a breach or data loss. For businesses under compliance regulations, this becomes even more critical from the standpoint of an audit or violations and fines due to a data breach. As a trusted business advisor, you become very sticky with clients when you can focus on a certain market segment and apply these compliance controls.

2. Implement Intune, Conditional Access, and ATP

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 MAM policies can immediately protect corporate data on mobile devices which is a massive security risk today. These policies do not require the device to be enrolled in the MDM solution. Users will be prompted to use a managed app like Outlook to access data. With MAM in place, you can monitor, encrypt, and remotely wipe corporate data.

Conditional access allows you to be "IT heroes" by allowing access to data and applications in a secure manner without inhibiting productivity. Create custom policies that cover security gaps in today's workplace. Evaluate the most critical applications based on business data and create policies that protect that data both on and off your network.

ATP policies for safe links and safe attachments can be set up in a short amount of time and add a great layered approach for your security solution.

Overview & Business Case

3. *Phased Rollout of Solutions*

If you do upsell your client to Microsoft 365 Business, it doesn't make sense to roll out all solutions in the stack at once. It would be incredibly taxing to your internal staff and you will reduce employee adoption and 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 the policy that provides the highest safeguard with the least amount of burden to the company.
3. Define the scope of users, groups, devices, and applications to which the policies would be applied.
4. Roll out the policy to pilot users (the champions of the organization).
5. Gather their feedback and adjust accordingl.
6. Create a communication plan for broad deployment and 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 phased approach is a great way to project manage the solutions to your clients, while understanding and maximizing your own internal bandwidth for implementation, and creating documentation that you can use as a template for every one of your clients. Over time you should have baseline policies that you apply to every company and the feedback you receive for improvements should reduce with each iteration.

OVERVIEW & BUSINESS CASE

REFERENCES

1. CIS Controls, Version 7.1
   Center for Internet Security
   April 2019
   https://workbench.cisecurity.org/files/2312

2. Small Businesses Turn to Managed Service Providers for Security
   Informa Tech
   March 2019
   https://www.darkreading.com/cloud/small-businesses-turn-to-managed-service-providers-for-security/d/d-id/1334259

3. Version 1.0 Center for Internet Security® Risk Assessment Method
   Center for Internet Security, Chris Cronin
   April 2018
   https://learn.cisecurity.org/cis-ram

4. 7 Ransomware Statistics MSPs Should Know
   Datto, CHRIS BRUNAU
   February 2020
   https://www.datto.com/blog/7-key-statistics-on-the-state-of-ransomware

5. How Microsoft Measures Effectiveness of Malware & Phish Catch for Office 365 *Microsoft, Debraj Ghosh*
September 2018
https://techcommunity.microsoft.com/t5/security-privacy-and-compliance/how-microsoft-measures-effectiveness-of-malware-amp-phish-catch/ba-p/263248

6. The Global Risks Report 2020
World Economic Forum
January 2020
http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf