Zero Trust Essentials eBook

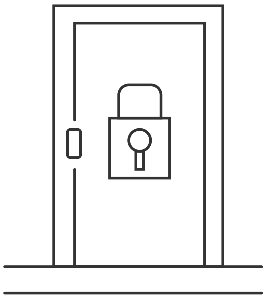
Identity, Endpoints, Applications, Network, Infrastructure and Data are important links in the end to end chain of the Zero Trust security model. The approach advocates protection at each layer, as they could be used as entry points or channels to leak sensitive information.

Zero Trust principles

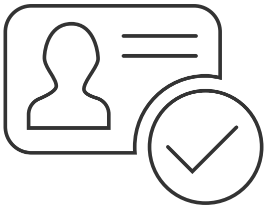
In the past, as an organization, you may have focused your defenses on protecting network access with on-premises firewalls and VPNs, assuming that everything inside the network was safe. But today, as data footprints have expanded to sit off-premises in the Cloud, or across hybrid networks, the Zero Trust security model has evolved to address a more holistic set of attack vectors.

Core to Zero Trust, are the principles of **verify explicitly, apply least privileged access** and **always assume breach.**

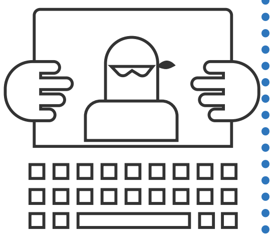
These principles are applied across a comprehensive control plane to provide multiple layers of defense.



Apply least privileged access

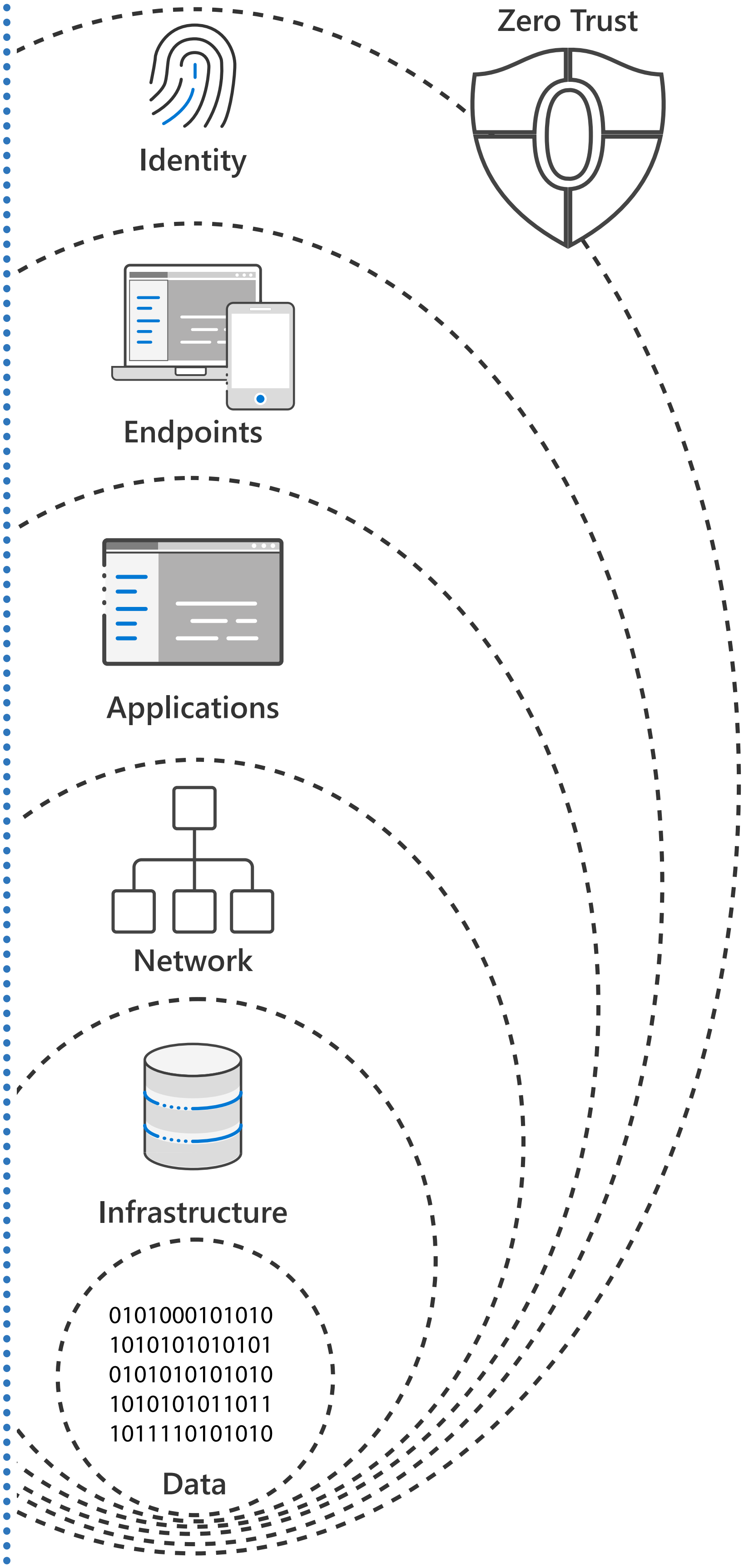


Verify explicitly



Always assume breach

Zero Trust security layers



Identity

Zero Trust starts with **identity**, verifying that only the people, devices and processes that have been granted access to your resources can access them.

Endpoints

Next comes asssessing the security compliance of device **endpoints** - the hardware accessing your data - including the IoT systems on the edge.

Applications

This oversight applies to your **applications** too, whether local or in the Cloud, as the software-level entry points to your information.

Network

Next, there are protections at the **network** layer for access to resources – especially those within your corporate perimeter.

Infrastructure

Followed by the **infrastructure** hosting your data on-premises and in the cloud. This can be physical or virtual, including containers and micro-services and the underlying operating systems and firmware.

Data

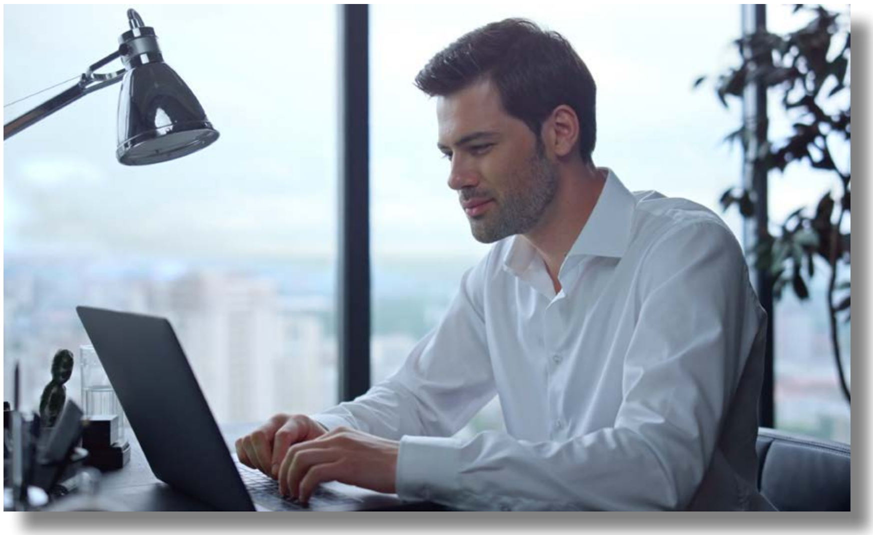
And finally, protection of the **data** itself across your files and content, as well as structured and unstructured data wherever it resides

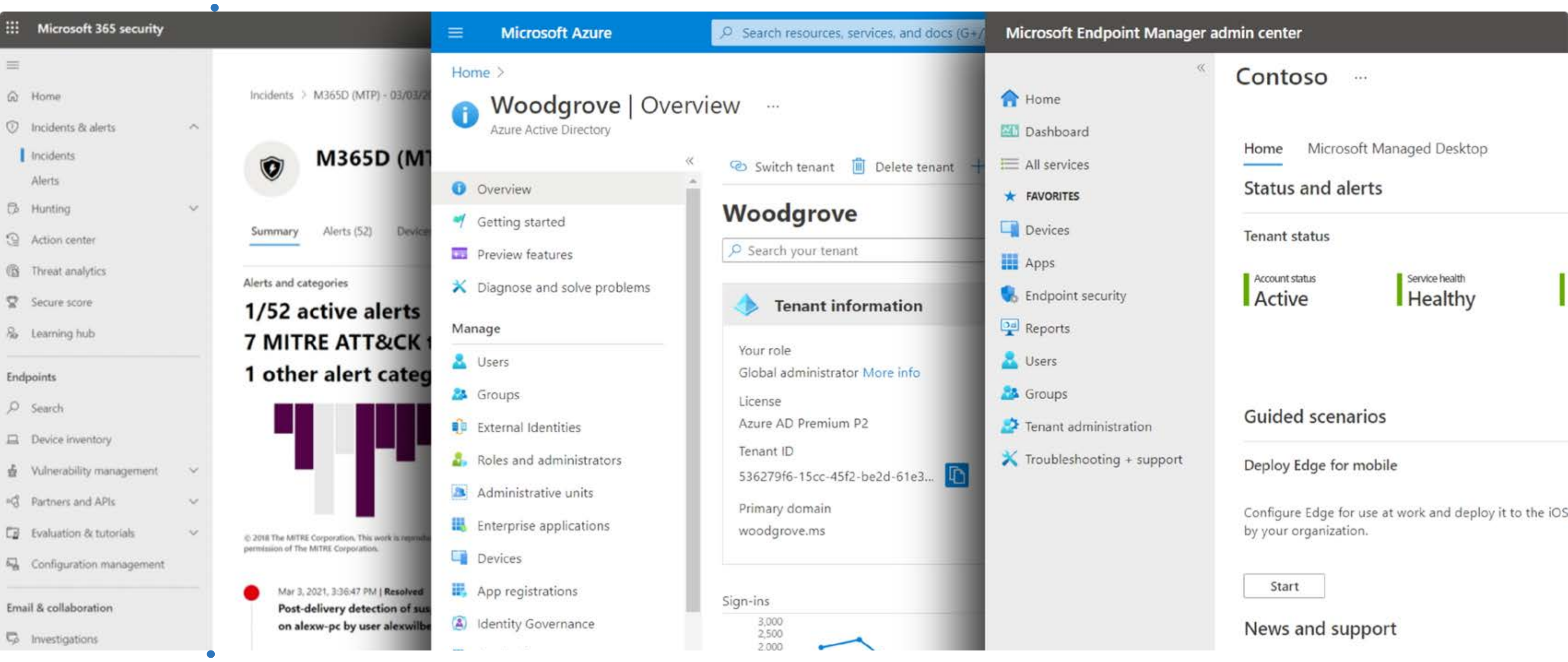
Microsoft’s approach to Zero Trust

Both Microsoft 365 and Azure are designed with Zero Trust as a core architectural principle. Protections span beyond the Microsoft cloud, to hybrid or even multi-cloud environments. Fundamental to Microsoft’s approach for Zero Trust is **not to disrupt end users**, but work behind the scenes to keep users secure and in their flow as they work.

The key here is end-to-end visibility and then bringing all this together with threat intelligence, risk detection and conditional access policies to reason over access requests and automate response across all of the Zero Trust layers of defense.

Keeping users protected but in their flow





Alerts and categories

1/52 active alerts

7 MITRE ATT&CK t

1 other alert categ

© 2018 The MITRE Corporation. This work is reprodu
permission of The MITRE Corporation.

Mar 3, 2021, 3:36:47 PM | Resolved
Post-delivery detection of sus
on alexw-pc by user alexwilbe

Your role
Global administrator More info

License
Azure AD Premium P2

Tenant ID
536279f6-15cc-45f2-be2d-61e3...

Primary domain
woodgrove.ms

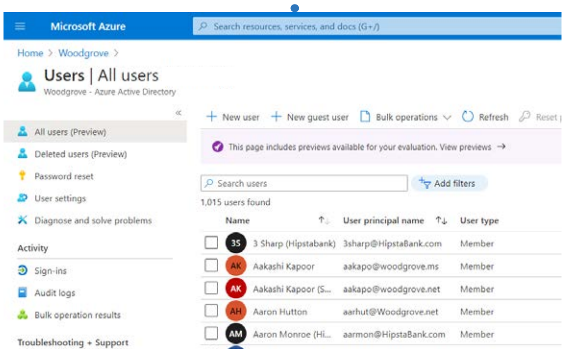
Account status
Active

Service health
Healthy

Configure Edge for use at work and deploy it to the iOS
by your organization.

Configuring Zero Trust with built-in and best-in-class controls

Identity



Users | All users

Woodgrove - Azure Active Directory

This page includes previews available for your evaluation. View previews →

1,015 users found

	Name	User principal name	User type
□	3S 3 Sharp (Hipstabank)	3sharp@HipstaBank.com	Member
□	AK Aakashi Kapoor	aakapo@woodgrove.ms	Member
□	AK Aakashi Kapoor (S...	aakapo@woodgrove.net	Member
□	AH Aaron Hutton	aarhut@Woodgrove.net	Member
□	AM Aaron Monroe (Hi...	aarmon@HipstaBank.com	Member

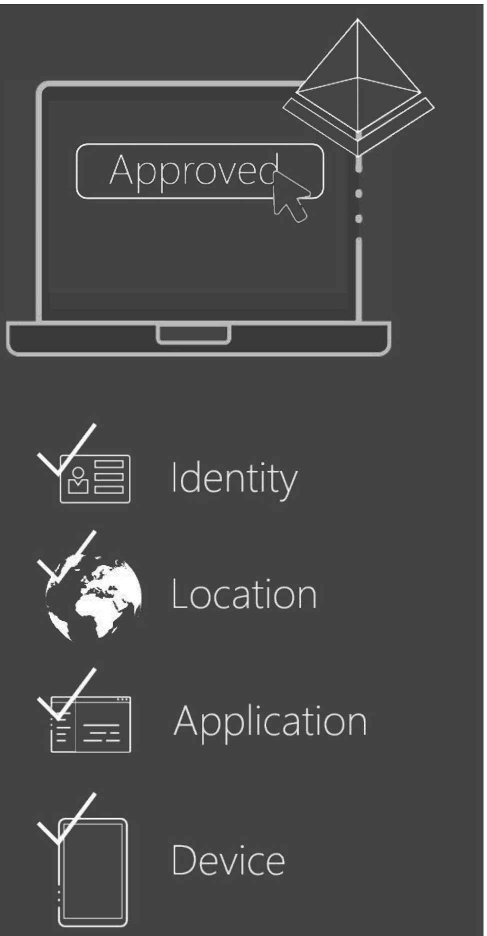
Users registered in Azure Active Directory

Azure Active Directory is the cloud identity service that assigns identity and conditional access controls for your people, the service accounts used for apps and processes, and your devices.

Importantly beyond Microsoft services, Azure AD can provide a single identity control plane with common authentication and authorization services for all your apps and services, including popular SaaS apps, or line-of-business cloud and on-premises apps.

This prevents the use of multiple credentials and weak passwords across different services and helps you to universally apply strong authentication methods such as passwordless multi-factor authentication for your users. For example, biometric methods or a FIDO2 key.

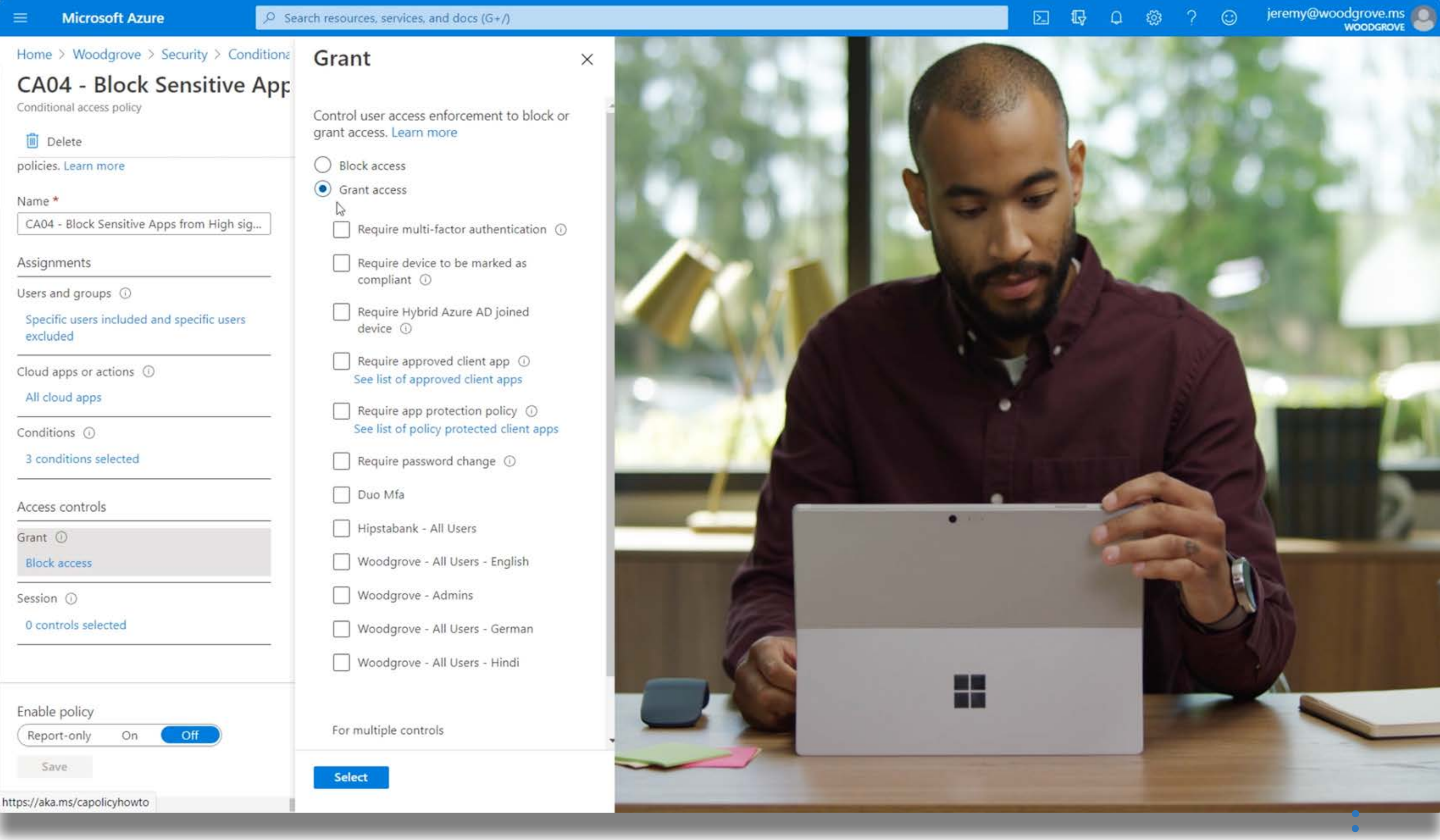
User authenticating with FIDO2 key



Conditional access

Also, to make the authentication process less intrusive to users, you can take advantage of real-time intelligence at sign-in with **Conditional Access** in Azure AD.

Conditional Access lets you set policies to assess the risk levels. This can be risk of the user or a sign-in, the device platform, the sign-in location, and apps, to make point-of-logon decisions and enforce access policies in real time to either block access and require password reset, grant access but require an additional authentication factor or limit it, for example, to view-only privileges.


Microsoft Azure

Search resources, services, and docs (G+/)

jeremy@woodgrove.ms
WOODGROVE

Home > Woodgrove > Security > Conditiona

CA04 - Block Sensitive App

Conditional access policy

Delete

policies. Learn more

Name *

CA04 - Block Sensitive Apps from High sig...

Assignments

Users and groups ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

3 conditions selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

Enable policy

Report-only | On | [✓ Off]

Save

https://aka.ms/capolicyhowto

Grant

Control user access enforcement to block or grant access. Learn more

○ Block access

● Grant access

□ Require multi-factor authentication ⓘ

□ Require device to be marked as compliant ⓘ

□ Require Hybrid Azure AD joined device ⓘ

□ Require approved client app ⓘ
See list of approved client apps

□ Require app protection policy ⓘ
See list of policy protected client apps

□ Require password change ⓘ

□ Duo Mfa

□ Hipstabank - All Users

□ Woodgrove - All Users - English

□ Woodgrove - Admins

□ Woodgrove - All Users - German

□ Woodgrove - All Users - Hindi

For multiple controls

Select

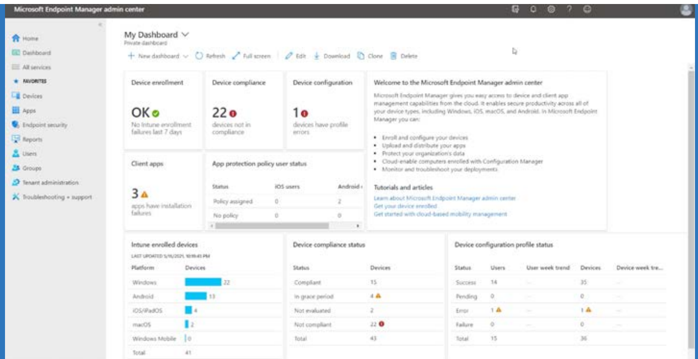
Granting or blocking access through Conditional Access policies

Endpoints

When users access resources including your data and apps, their endpoints may not be owned and managed by your organization. If endpoints are not up-to-date, or appropriately protected, they run the risk of data exfiltration from unknown apps or services.

Using Microsoft Endpoint Manager, you can make sure that devices and their installed apps meet your security and compliance policy requirements, regardless of whether the device is owned by your organization or the user. This protection applies no matter where the device may be connecting from – whether that's inside the network perimeter, including over a VPN, on a home network, or the public internet.

Connecting from work, home, or public internet


Microsoft Endpoint Manager admin center

My Dashboard
Private dashboard

Device enrollment
OK ✓
No Intune enrollment failures last 7 days

Device compliance
22 ❗
devices not in compliance

Device configuration
1 ❗
devices have profile errors

Client apps
3 ⚠
apps have installation failures

App protection policy user status

Status	iOS users	Android
Policy assigned	0	2
No policy	0	0

Welcome to the Microsoft Endpoint Manager admin center

Microsoft Endpoint Manager gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types, including Windows, iOS, macOS, and Android. In Microsoft Endpoint Manager you can:

- Enroll and configure your devices
- Upload and distribute your apps
- Protect your organization's data
- Cloud-enable computers enrolled with Configuration Manager
- Monitor and troubleshoot your deployments

Tutorials and articles
Learn about Microsoft Endpoint Manager admin center
Get your device enrolled
Get started with cloud-based mobility management

Intune enrolled devices
LAST UPDATED 5/16/2021, 10:19:41 PM

Platform	Devices
Windows	22
Android	13
iOS/iPadOS	4
macOS	2
Windows Mobile	0
Total	41

Device compliance status

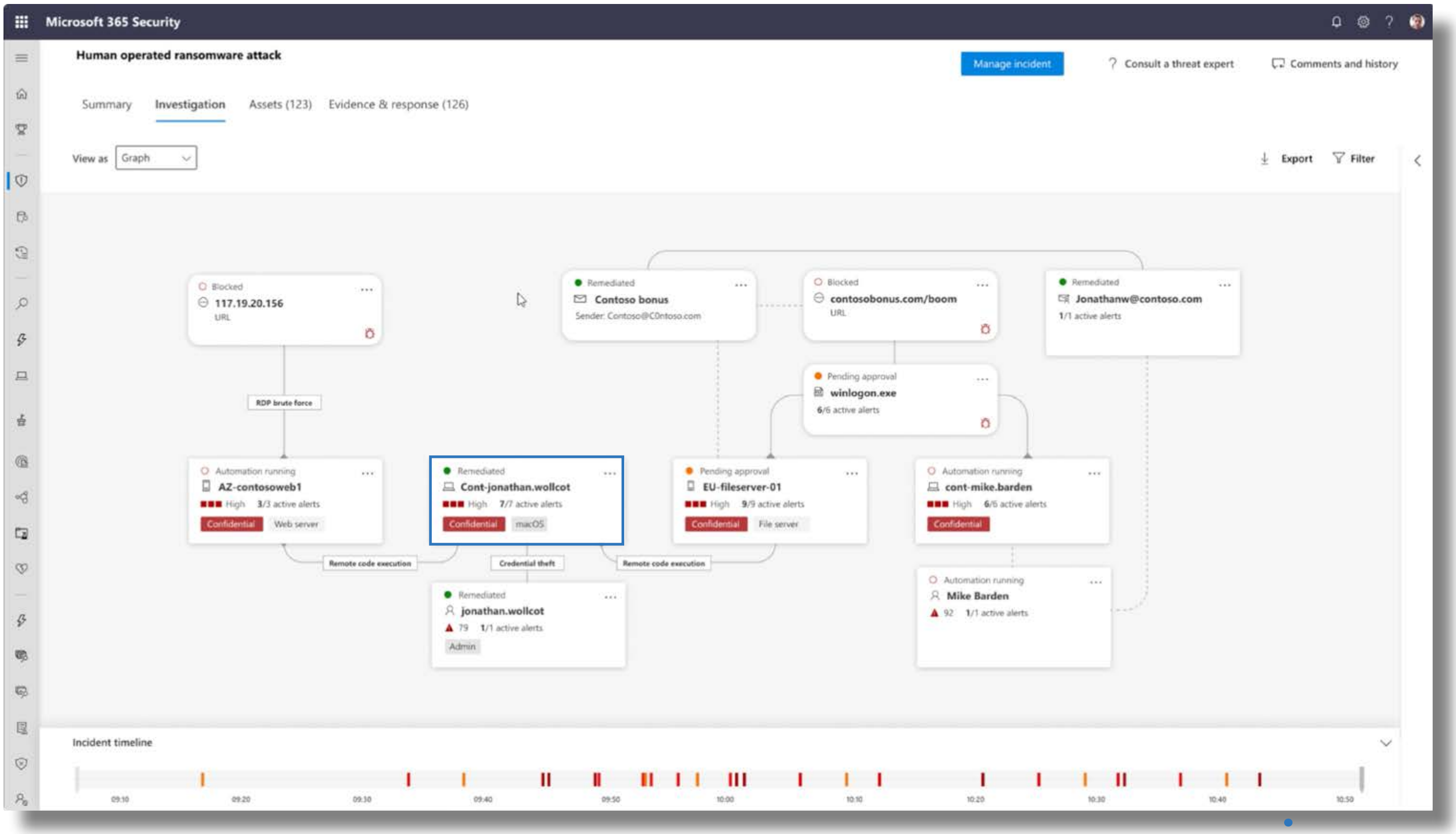
Status	Devices
Compliant	15
In grace period	4 ⚠
Not evaluated	2
Not compliant	22 ❗
Total	43

Device configuration profile status

Status	Users	User week trend	Devices	Device week tre...
Success	14	—	35	—
Pending	0	—	0	—
Error	1 ⚠	—	1 ⚠	—
Failure	0	—	0	—
Total	15		36	

Microsoft Endpoint Manager gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types including Windows, iOS, macOS, and Android.

Also, Microsoft Defender with its Extended Detection and Response or XDR management controls, can identify and contain breaches discovered on an endpoint and force the device back into a trustworthy state before it is allowed to connect back to resources.



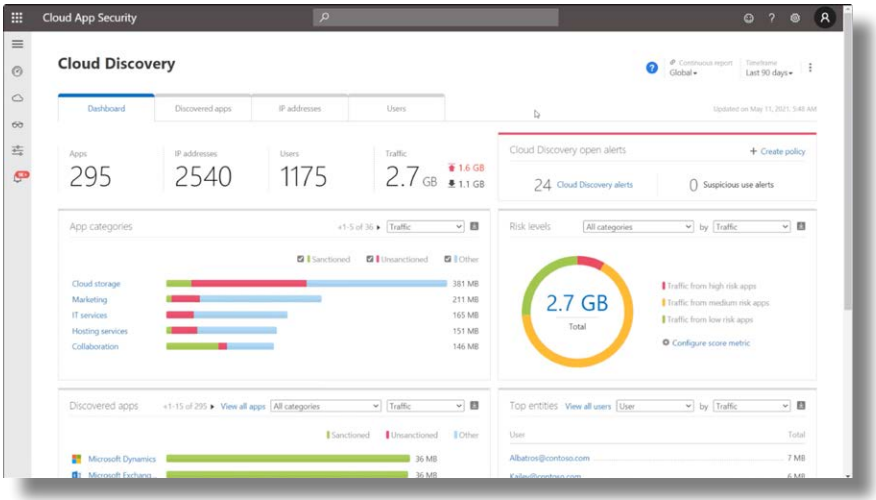
Containing a breach on a device endpoint with Microsoft Defender

Applications

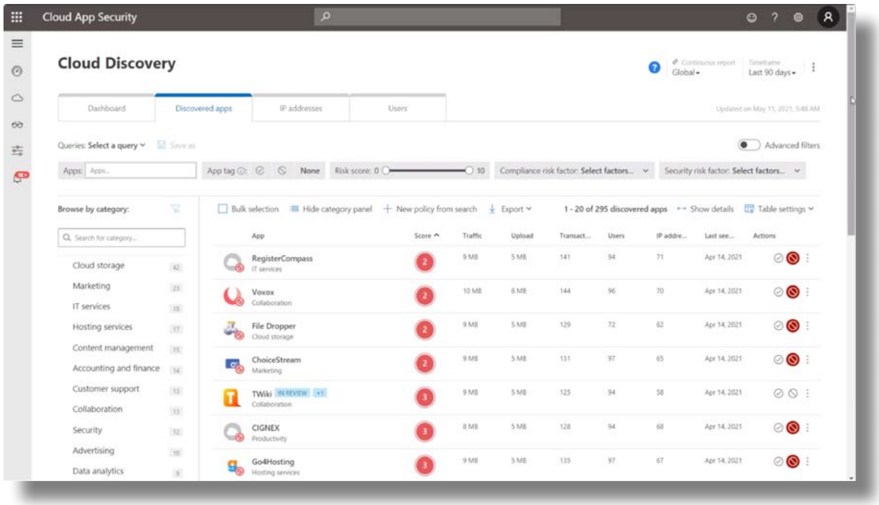
There are several ways that we help you to apply Zero Trust protections to your applications. We have already looked at the benefits of Azure AD as the single entity provider for authenticated sign-in, as well as the use of conditional access. These recommendations also apply to your cloud and local apps that connect to cloud-based services.

Additionally, Microsoft Endpoint Manager can be used to configure and enforce policy management for both desktop and mobile apps, including browsers. For example, you can prevent work related data from being copied and used in personal apps.

Knowing which apps are used within your organization is critical to mitigating new vulnerabilities. This includes apps acquired by individuals and teams, often referred to as Shadow IT. With its catalog of more than 17,000 apps, Microsoft Cloud App Security (MCAS) can discover and manage Shadow IT services.



Microsoft Cloud App Security dashboard



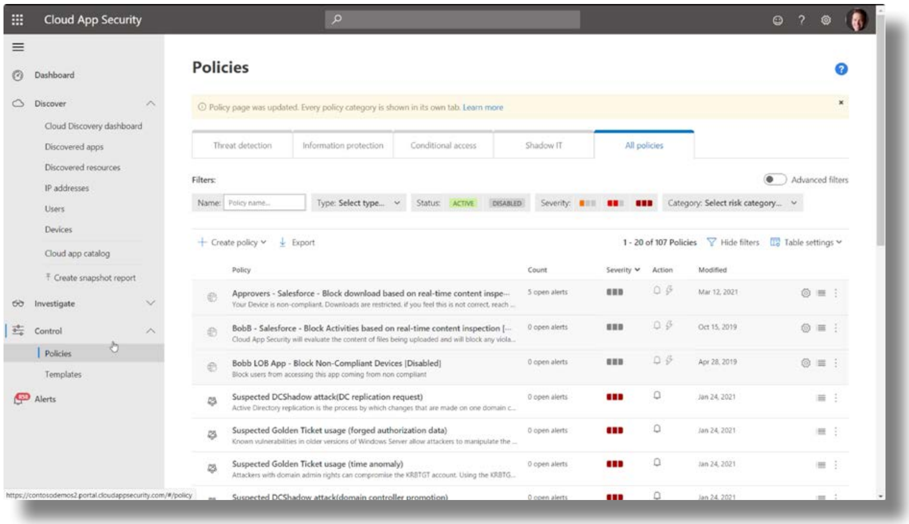
Category	
Cloud storage	42
Marketing	23
IT services	18
Hosting services	17
Content management	15
Accounting and finance	14
Customer support	13
Collaboration	13
Security	12
Advertising	10
Data analytics	9

App	Score	Traffic	Upload	Transact...	Users	IP addre...	Last see...	Actions
RegisterCompass IT services	2	9 MB	5 MB	141	94	71	Apr 14, 2021	
Voxox Collaboration	2	10 MB	6 MB	144	96	70	Apr 14, 2021	
File Dropper Cloud storage	2	9 MB	5 MB	129	72	62	Apr 14, 2021	
ChoiceStream Marketing	2	9 MB	5 MB	131	97	65	Apr 14, 2021	
TWiki IN REVIEW +1 Collaboration	3	9 MB	5 MB	125	94	58	Apr 14, 2021	
CIGNEX Productivity	3	8 MB	5 MB	128	94	68	Apr 14, 2021	
Go4Hosting Hosting services	3	9 MB	5 MB	135	97	67	Apr 14, 2021	

Cloud Discovery in Microsoft Cloud App Security

You can then set policies against your security requirements to scope how information may be accessed or shared by these services. For example, you can use policies to block actions within a cloud app, such as downloading confidential files, or discussing sensitive topics while using unmanaged devices.

The policy tab in Microsoft Cloud App Security

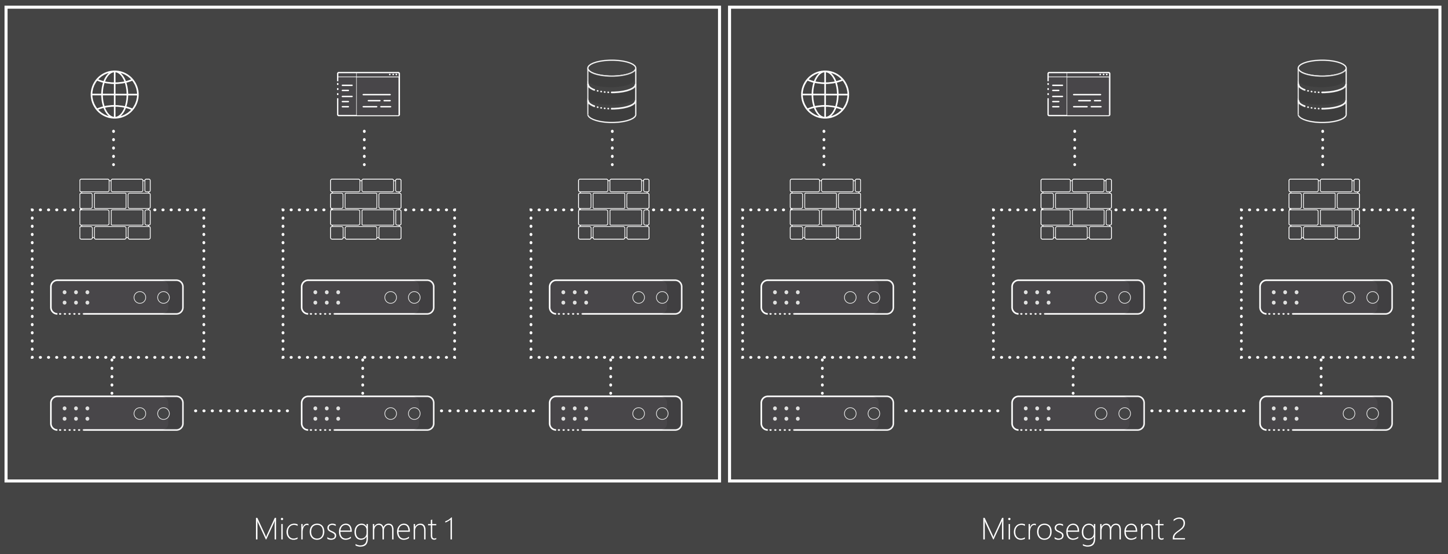


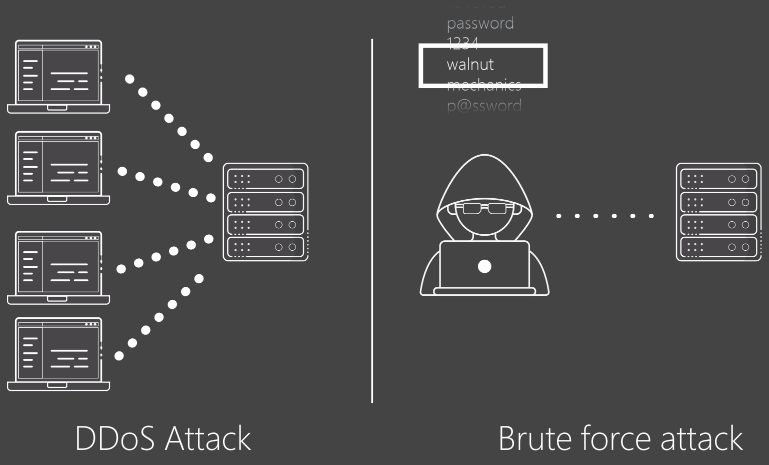
Policy page was updated. Every policy category is shown in its own tab. Learn more

Policy	Count	Severity	Action	Modified
Approvers - Salesforce - Block download based on real-time content inspe... Your Device is non-compliant. Downloads are restricted. if you feel this is not correct, reach ...	5 open alerts			Mar 12, 2021
BobB - Salesforce - Block Activities based on real-time content inspection [... Cloud App Security will evaluate the content of files being uploaded and will block any viola...	0 open alerts			Oct 15, 2019
Bobb LOB App - Block Non-Compliant Devices [Disabled] Block users from accessing this app coming from non compliant	0 open alerts			Apr 28, 2019
Suspected DCShadow attack(DC replication request) Active Directory replication is the process by which changes that are made on one domain c...	0 open alerts			Jan 24, 2021
Suspected Golden Ticket usage (forged authorization data) Known vulnerabilities in older versions of Windows Server allow attackers to manipulate the ...	0 open alerts			Jan 24, 2021
Suspected Golden Ticket usage (time anomaly) Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTG...	0 open alerts			Jan 24, 2021
Suspected DCShadow attack(domain controller promotion)	0 open alerts			Jan 24, 2021

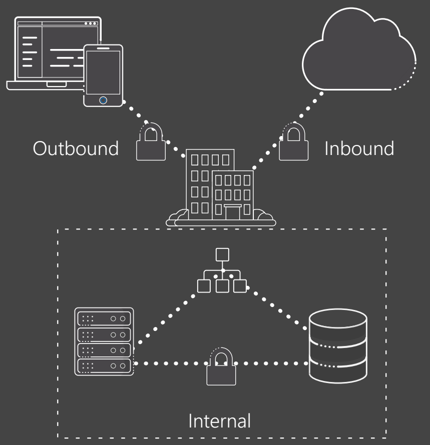
Network

The network is the fourth layer in the Zero Trust security model. With modern architectures and hybrid services spanning on-premises and multiple cloud services, virtual networks – or VNETs – and VPNs, we give you a number of controls, starting with: **1. Network Segmentation** to limit the blast radius and lateral movements of attacks on your network.



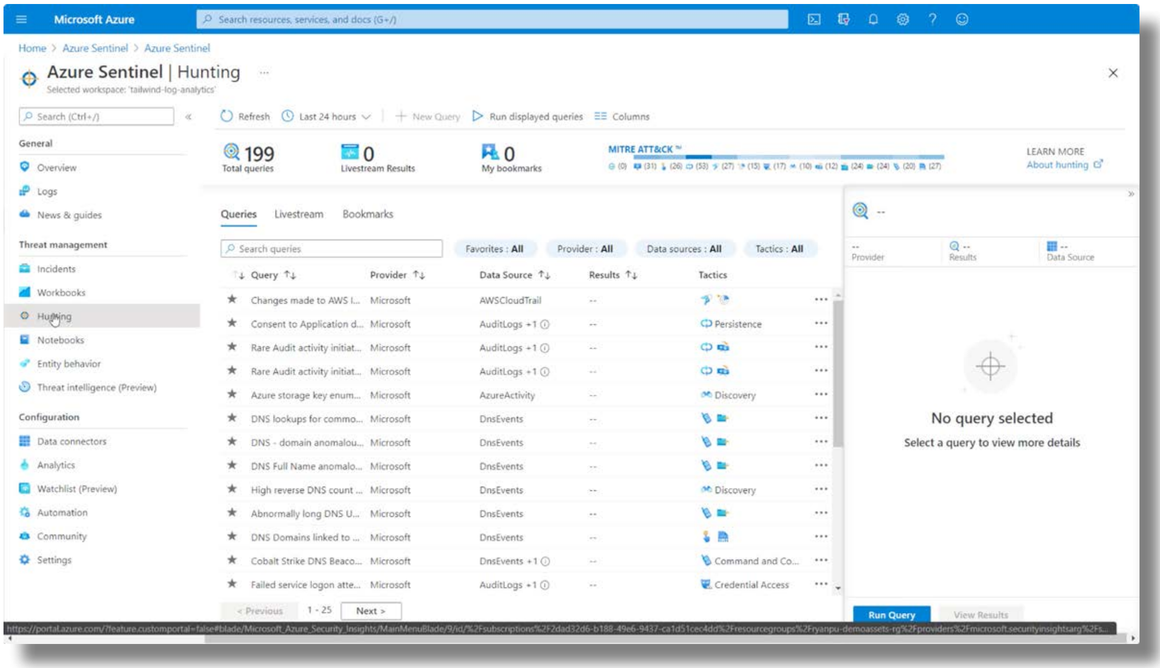


2. Threat protection to harden the network perimeter from things like DDoS or brute force attacks, **then the ability to quickly detect and respond to incidents**



3. Encryption for all network traffic, whether it's internal, inbound or outbound

Microsoft offers several solutions to help secure your network, including Azure Firewall and Azure DDoS Protection to protect your Azure VNET resources. Importantly, Microsoft's XDR and SIEM solution, comprising Microsoft Defender and Azure Sentinel, help you quickly identify and contain security incidents.



	Query	Provider	Data Source	Results	Tactics
★	Changes made to AWS I...	Microsoft	AWSCloudTrail	--	
★	Consent to Application d...	Microsoft	AuditLogs +1	--	Persistence
★	Rare Audit activity initiat...	Microsoft	AuditLogs +1	--	
★	Rare Audit activity initiat...	Microsoft	AuditLogs +1	--	
★	Azure storage key enum...	Microsoft	AzureActivity	--	Discovery
★	DNS lookups for commo...	Microsoft	DnsEvents	--	
★	DNS - domain anomalou...	Microsoft	DnsEvents	--	
★	DNS Full Name anomalo...	Microsoft	DnsEvents	--	
★	High reverse DNS count ...	Microsoft	DnsEvents	--	Discovery
★	Abnormally long DNS U...	Microsoft	DnsEvents	--	
★	DNS Domains linked to ...	Microsoft	DnsEvents	--	
★	Cobalt Strike DNS Beaco...	Microsoft	DnsEvents +1	--	Command and Co...
★	Failed service logon atte...	Microsoft	AuditLogs +1	--	Credential Access

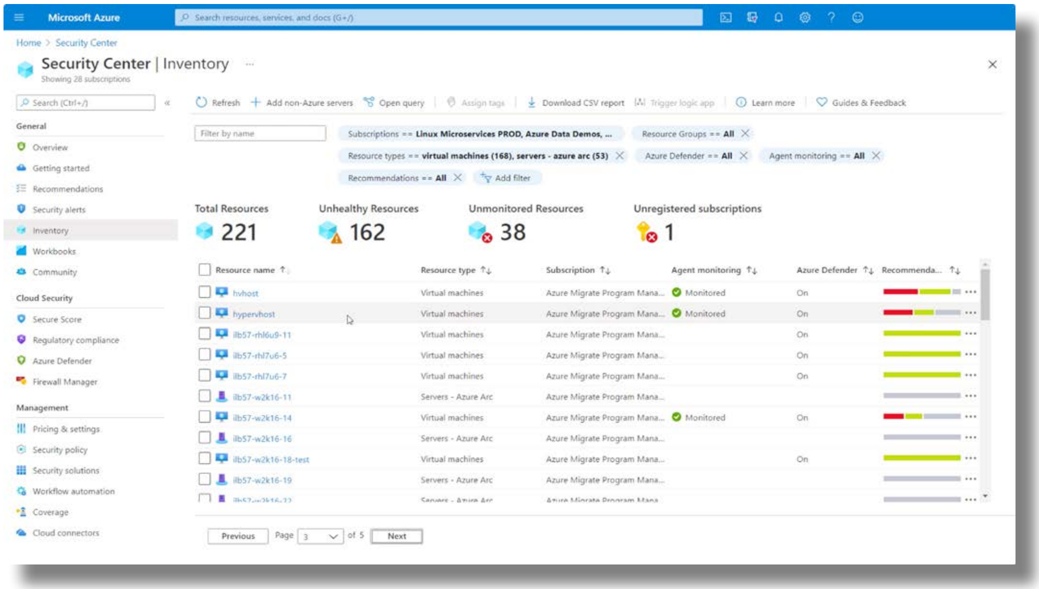
https://portal.azure.com/?feature.customportal=false#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/9/id/%2Fsubscriptions%2F2dad32d6-b188-49e6-9437-ca1d51cec4dd%2Fresourcegroups%2Fryanpu-demoassets-rg%2Fproviders%2Fmicrosoft.securityinsightsarg%2Fs...

Post-breach hunting in Azure Sentinel

Infrastructure

The most important consideration with infrastructure is around configuration management and software updates so that all deployed infrastructure meets your security and policy requirements.

Here for cloud resources, Azure landing zones, blueprints and policies ensure that newly deployed infrastructure meets compliance requirements. And the Azure Security Center along with Log Analytics helps with configuration and software update management for your on-premises, cross-cloud and cross-platform infrastructure.



Resource name	Resource type	Subscription	Agent monitoring	Azure Defender	Recommenda...
hvhost	Virtual machines	Azure Migrate Program Mana...	Monitored	On	
hypervhost	Virtual machines	Azure Migrate Program Mana...	Monitored	On	
ilb57-rhl6u9-11	Virtual machines	Azure Migrate Program Mana...		On	
ilb57-rhl7u6-5	Virtual machines	Azure Migrate Program Mana...		On	
ilb57-rhl7u6-7	Virtual machines	Azure Migrate Program Mana...		On	
ilb57-w2k16-11	Servers - Azure Arc	Azure Migrate Program Mana...			
ilb57-w2k16-14	Virtual machines	Azure Migrate Program Mana...	Monitored	On	
ilb57-w2k16-16	Servers - Azure Arc	Azure Migrate Program Mana...			
ilb57-w2k16-18-test	Virtual machines	Azure Migrate Program Mana...		On	
ilb57-w2k16-19	Servers - Azure Arc	Azure Migrate Program Mana...			
ilb57-w2k16-22	Servers - Azure Arc	Azure Migrate Program Mana...			

Azure Security Center monitoring of your resources in Azure, on-premises, or across-clouds using Azure Arc

Monitoring is critical for the detection of vulnerabilities, attacks and anomalies. Microsoft Defender with Azure Sentinel provides depth and breadth threat protection for multi-cloud workloads enabling automated detection and response.

Data

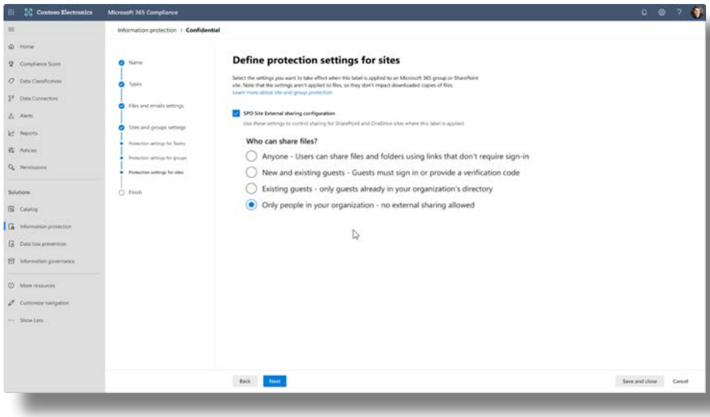
0100100100100100100100100100100100100101110101100101000100100100100010010
1001001010001001001001011101001001010010101010010101010010010010010111010
001111001010101101011110100101010100001010010100101011101010100101001010001
0100100101010100100101011111001010101011100010010010001000001010101011101 0
01001010101010101010100101010010101010101001010101010010101010010101010100

At the end of the day Zero Trust is all about understanding and then applying the right controls to protect your Data.

We give you the controls to limit data access only to the people and processes that need it. The policies you set, along with real-time monitoring, can then restrict or block the unwanted sharing of sensitive data and files.

For example, with Microsoft Information Protection, you can automate labeling and classification of files and content.

Policies are then assigned to labels to trigger protective actions, such as encryption or limiting access, restricting third party apps and services and much more.



Information protection > Confidential

Define protection settings for sites

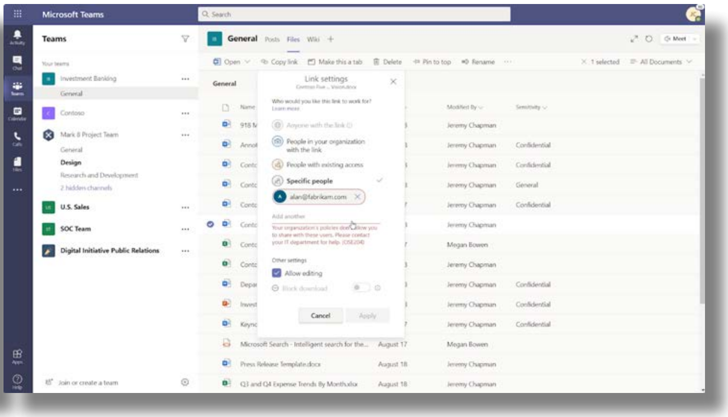
Select the settings you want to take effect when this label is applied to an Microsoft 365 group or SharePoint site. Note that the settings aren't applied to files, so they don't impact downloaded copies of files.
Learn more about site and group protection

☑ SPO Site External sharing configuration
Use these settings to control sharing for SharePoint and OneDrive sites where this label is applied

Who can share files?

○ Anyone - Users can share files and folders using links that don't require sign-in
○ New and existing guests - Guests must sign in or provide a verification code
○ Existing guests - only guests already in your organization's directory
● Only people in your organization - no external sharing allowed

Setting information protection controls in the Microsoft 365 compliance center



Link settings

Who would you like this link to work for?
Learn more

○ Anyone with the link
○ People in your organization with the link
○ People with existing access
● Specific people ✓

alan@fabrikam.com

Add another

Your organization's policies don't allow you to share with these users. Please contact your IT department for help. (OSE204)

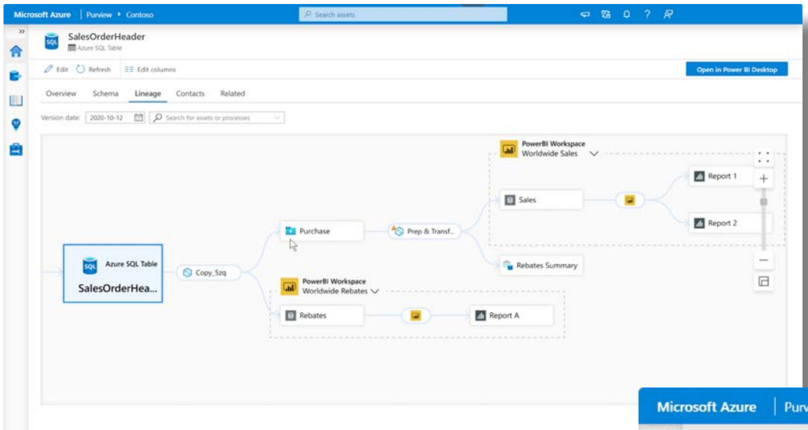
Other settings
☑ Allow editing
○ Block download

Name		Modified By	Sensitivity
918 M		Jeremy Chapman	
Anno		Jeremy Chapman	Confidential
Conto		Jeremy Chapman	Confidential
Conto		Jeremy Chapman	General
Conto		Jeremy Chapman	Confidential
Conto		Jeremy Chapman	
Conto		Megan Bowen	
Conto		Jeremy Chapman	
Depar		Jeremy Chapman	Confidential
Invest		Jeremy Chapman	Confidential
Keyno		Jeremy Chapman	Confidential
Microsoft Search - Intelligent search for the...	August 17	Megan Bowen	
Press Release Template.docx	August 18	Jeremy Chapman	
Q3 and Q4 Expense Trends By Month.xlsx	August 18	Jeremy Chapman	

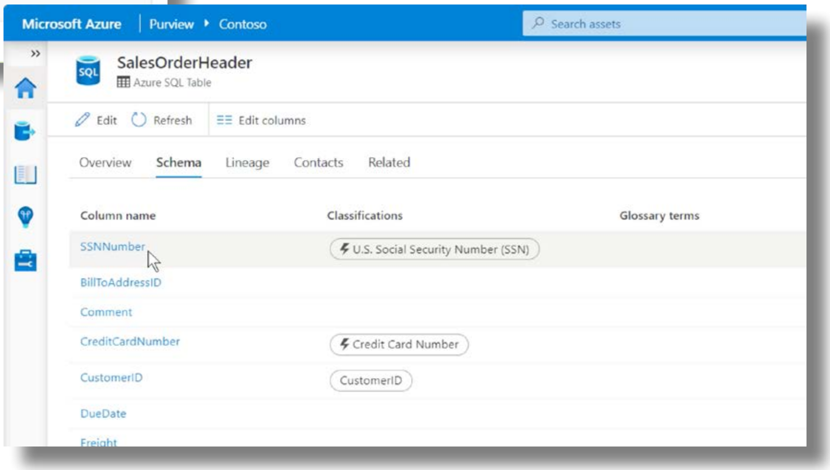
Example of a policy being enforced as user tries to share content

Azure Purview

For data outside of Microsoft 365, Azure Purview automatically discovers and maps the data sitting across your Azure data sources, on-premises, and SaaS data sources; it works with Microsoft Information Protection to help you to classify your sensitive information.



Azure Purview data lineage map



Column name	Classifications	Glossary terms
SSNNumber	U.S. Social Security Number (SSN)	
BillToAddressID		
Comment		
CreditCardNumber	Credit Card Number	
CustomerID	CustomerID	
DueDate		
Freight		

Classification of sensitive information in Azure Purview

Additional Resources

Moving to a Zero Trust security model doesn't have to be all-or-nothing. We recommend using a phased approach, closing the most exploitable vulnerabilities first.

For hands-on demonstrations of the tools for implementing the Zero Trust security model across the six layers of defense, watch our Microsoft Mechanics series at **aka.ms/ZeroTrustMechanics**.

You can also learn more at **aka.ms/zerotrust**.