



Zero Trust



Identity



Endpoints



Applications



Network



Infrastructure



Data

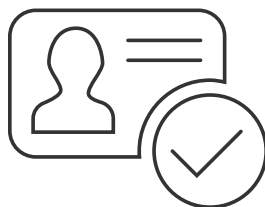
Identity, Endpoints, Applications, Network, Infrastructure and Data are important links in the end to end chain of the Zero Trust security model. The approach advocates protection at each layer, as they could be used as entry points or channels to leak sensitive information.

Zero Trust principles

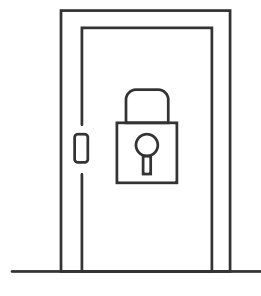
In the past, as an organization, you may have focused your defenses on protecting network access with on-premises firewalls and VPNs, assuming that everything inside the network was safe. But today, as data footprints have expanded to sit off-premises in the Cloud, or across hybrid networks, the Zero 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**.

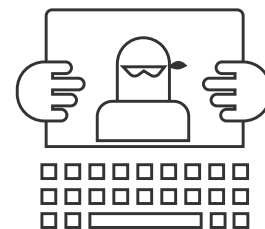
These principles are applied across a comprehensive control plane to provide multiple layers of defense.



Verify explicitly

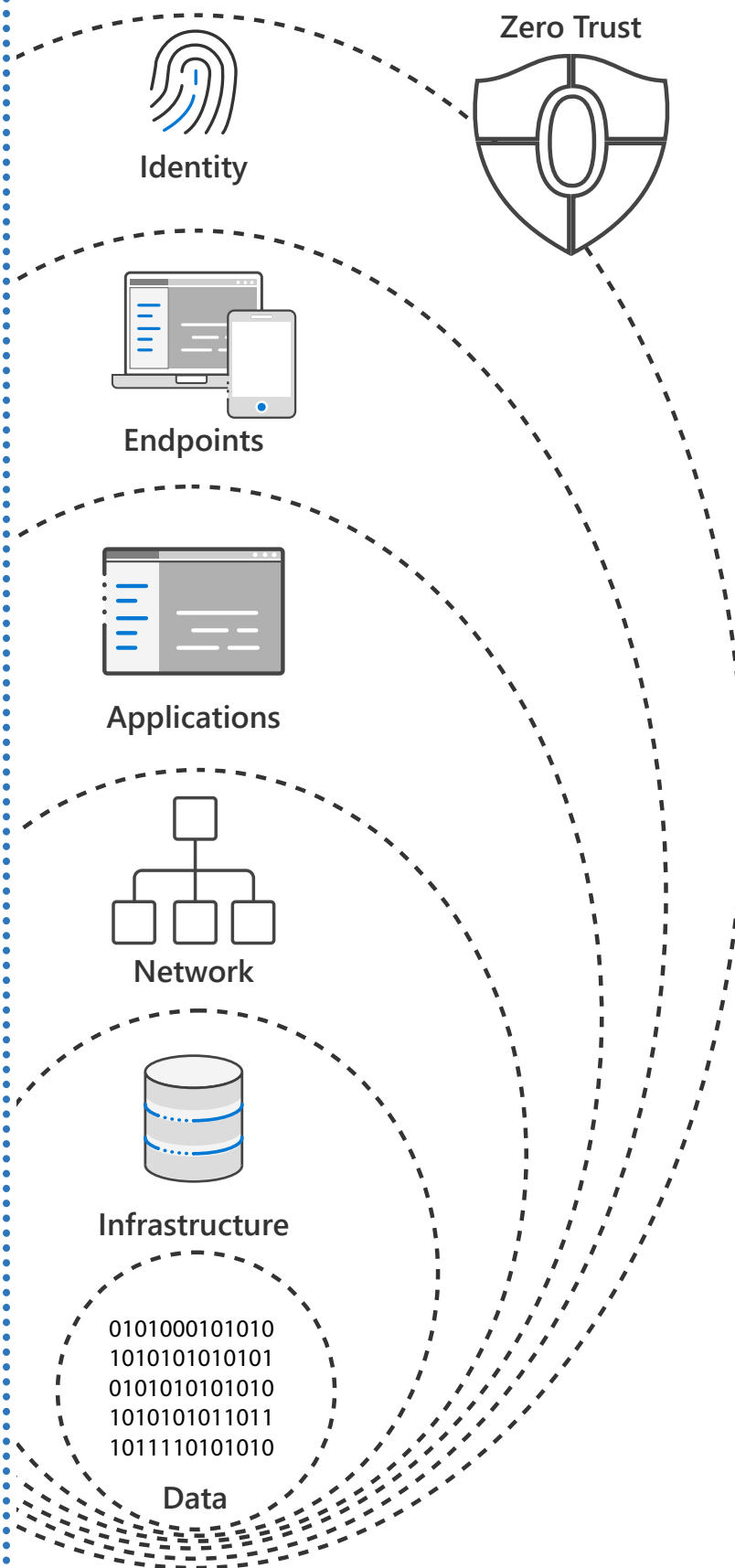


Apply least privileged access



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 assessing 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

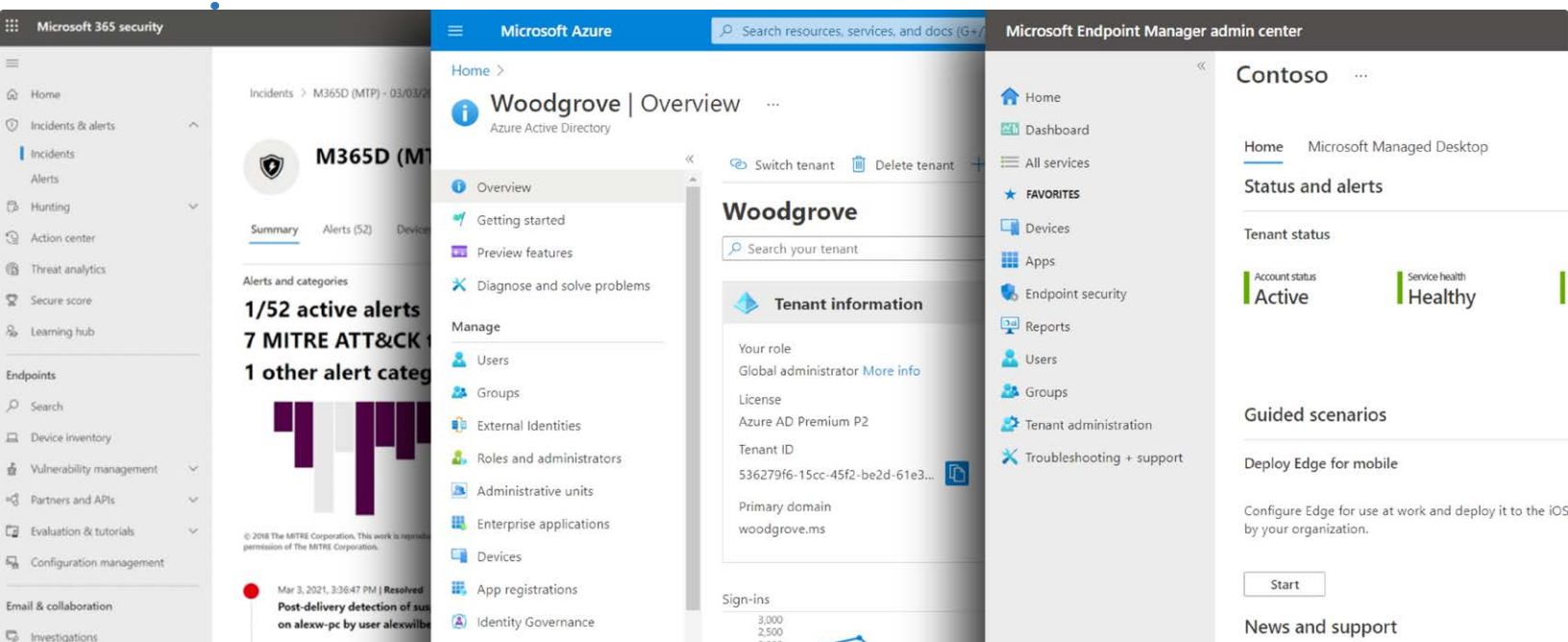
And finally, protection of the **data** itself across your files and content, as well as structured and unstructured data wherever it resides

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



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

Identity



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.

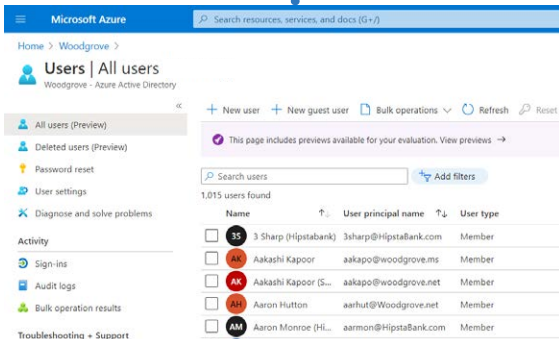
This prevents the use of multiple credentials and weak passwords across different services and helps you to universally apply strong authentication methods such as passwordless multi-factor authentication for your users. For example, biometric methods or a FIDO2 key.



User authenticating with FIDO2 key

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.



Users registered in Azure Active Directory



Identity



Location



Application



Device

Conditional access

Microsoft Azure

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

jeremy@woodgrove.ms

WOODGROVE

Home > Woodgrove > Security > Conditional Access

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

☐ Hipstabanck - 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

Home

Dashboard

All services

REPORTS

Devices

Apps

Endpoint security

Reports

Users

Groups

Device administration

Enrollment > support

My Dashboard

Private dashboard

New dashboard

Refresh

Full screen

Export

Download

Clone

Backup

Device enrollment

OK

No license enrollment failures last 7 days

Client apps

3

apps have installation failures

Intune enrolled devices

last status success, resource

Platform	Devices
Windows	21
Android	11
iOS/macOS	1
Windows Mobile	0
Total	41

Device compliance

22

devices not in compliance

App protection policy user status

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

Device configuration

1

devices have profile errors

• Enroll and configure your devices

• Update and distribute your apps

• Protect your organization's data

• Cloud-manage 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

Device compliance status

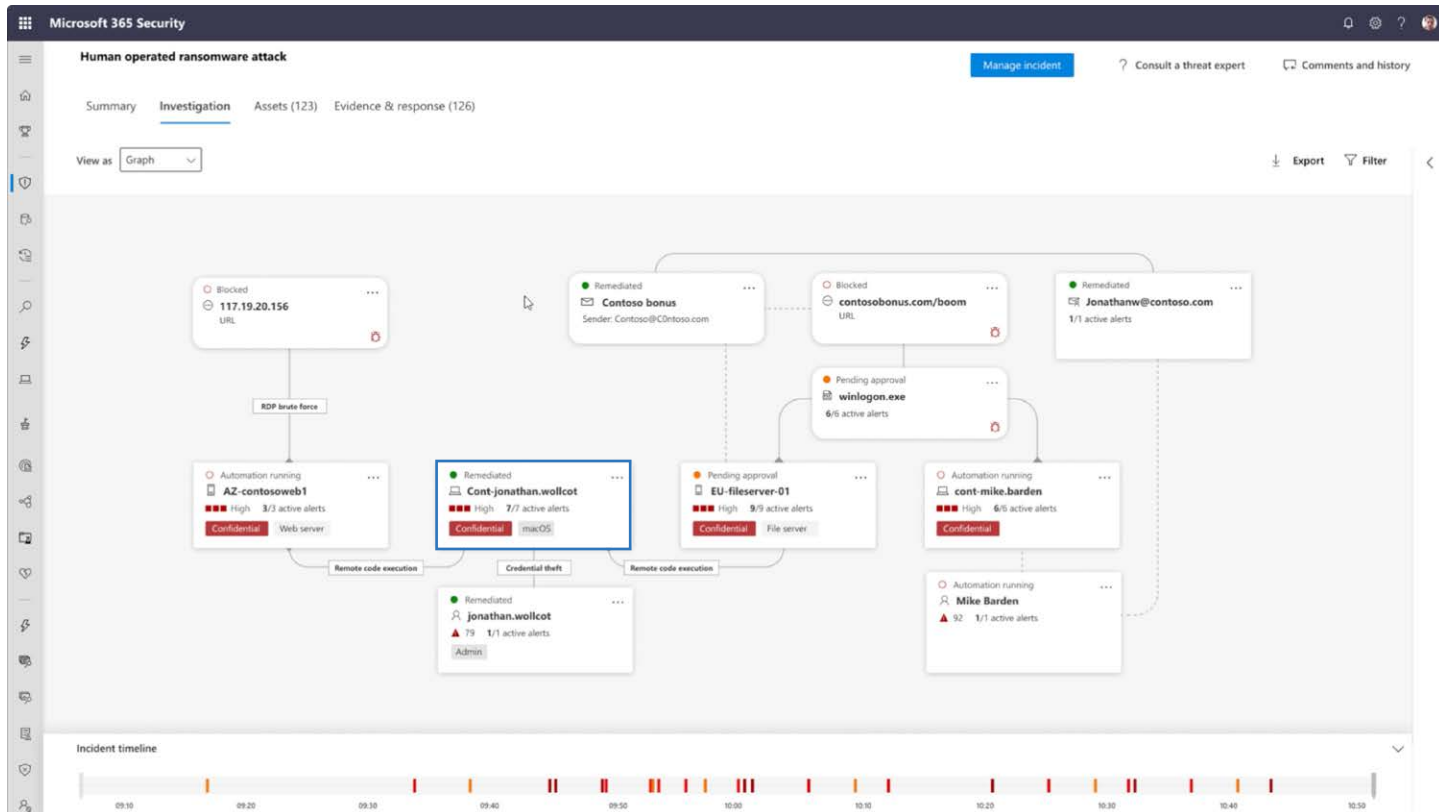
Status	Devices
Compliant	15
In grace period	4
Not evaluated	2
Not compliant	21
Total	42

Device configuration profile status

Status	Users	Devices	Device week in...
Success	14	25	
Pending	0	0	
Error	1	1	
Failure	0	0	
Total	15	26	

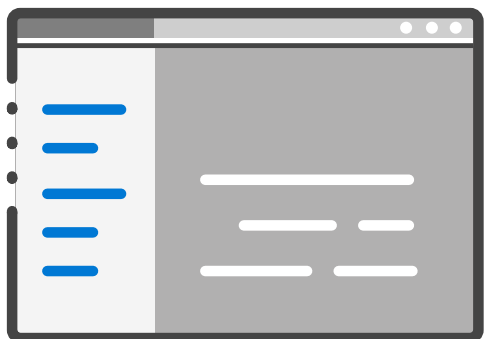
Microsoft Endpoint Manager gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types including Windows, iOS, macOS, and Android.

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

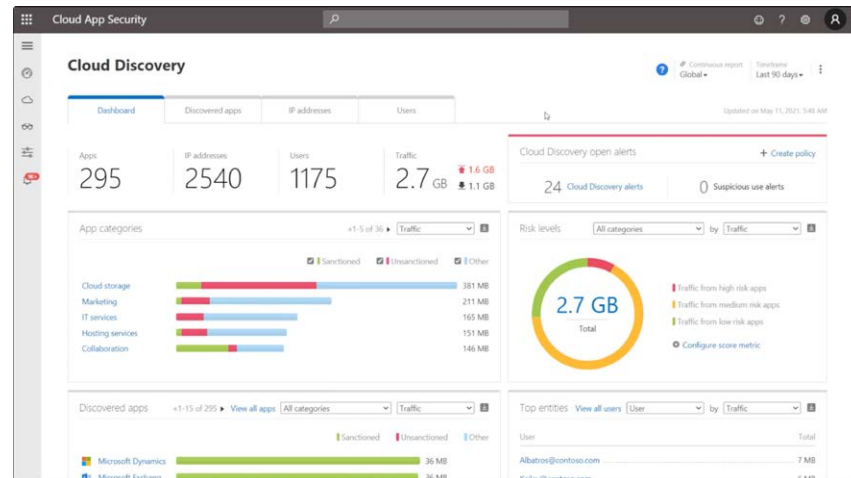
Applications



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

The screenshot shows the 'Discovered apps' page in Microsoft Cloud App Security. It displays a list of 1-20 of 295 discovered apps. The table includes columns for App, Score, Traffic, Upload, Transact, Users, IP address, Last seen, and Actions. The apps listed include RegisterCompass, Veeva, File Dropper, ChoiceStream, TWiN, CIGNEX, and Go4hosting.

App	Score	Traffic	Upload	Transact	Users	IP address	Last seen	Actions
RegisterCompass	2	9 MB	5 MB	141	94	71	Apr 14, 2021	
Veeva	2	10 MB	6 MB	144	96	70	Apr 14, 2021	
File Dropper	2	9 MB	5 MB	129	72	62	Apr 14, 2021	
ChoiceStream	2	9 MB	5 MB	131	97	65	Apr 14, 2021	
TWiN	3	9 MB	5 MB	125	94	58	Apr 14, 2021	
CIGNEX	3	8 MB	5 MB	128	94	68	Apr 14, 2021	
Go4hosting	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.

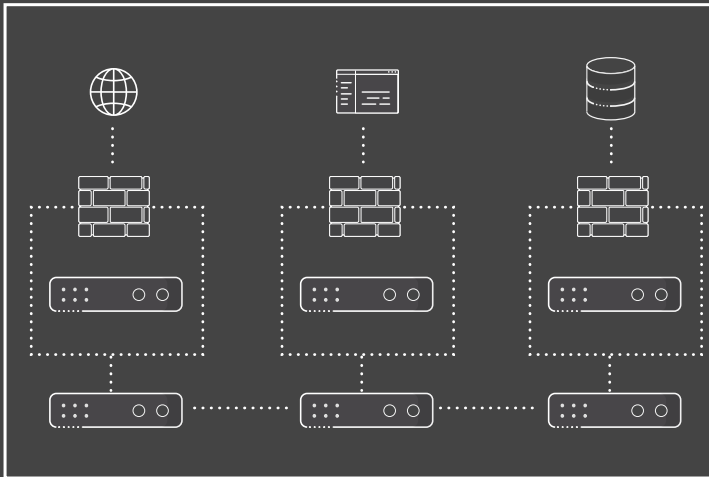
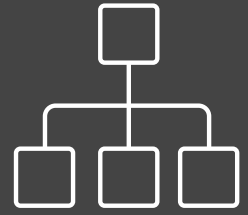
The policy tab in Microsoft Cloud App Security

The screenshot shows the 'Policies' page in Microsoft Cloud App Security. It displays a list of 1-20 of 107 policies. The table includes columns for Policy, Count, Severity, Action, and Modified. The policies listed include Approvers - Salesforce, BobB - Salesforce, BobB LOB App, Suspected DShadow attack, Suspected Golden Ticket usage, and Suspected Golden Ticket usage (time anomaly).

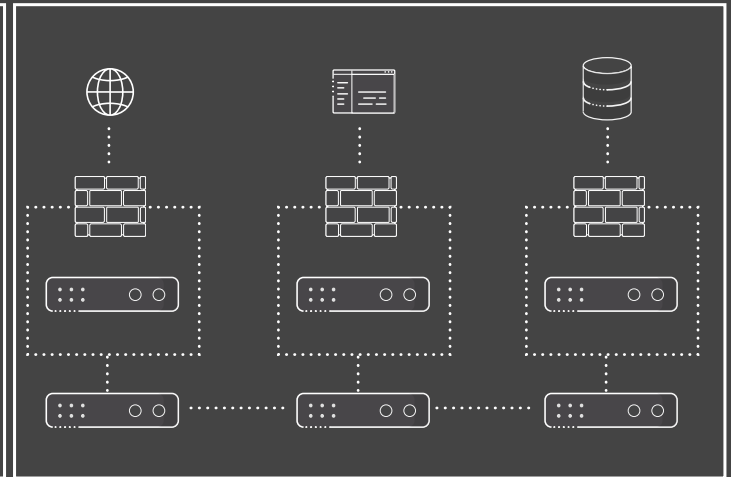
Policy	Count	Severity	Action	Modified
Approvers - Salesforce - Block download based on real-time content inspection	5 open alerts	High	Block	Mar 12, 2021
BobB - Salesforce - Block Activities based on real-time content inspection	0 open alerts	High	Block	Oct 15, 2019
BobB LOB App - Block Non-Compliant Devices (Disabled)	0 open alerts	High	Block	Apr 28, 2019
Suspected DShadow attack(DC replication request)	0 open alerts	High	Block	Jan 24, 2021
Suspected Golden Ticket usage (forged authorization data)	0 open alerts	High	Block	Jan 24, 2021
Suspected Golden Ticket usage (time anomaly)	0 open alerts	High	Block	Jan 24, 2021
Suspected DShadow attack(kerberos authentication)	0 open alerts	High	Block	Jan 24, 2021

Network

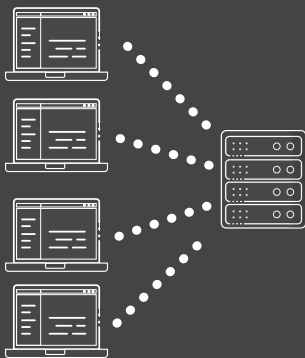
The network is the fourth layer in the Zero Trust security model. With modern architectures and hybrid services spanning on-premises and multiple cloud services, virtual networks – or VNETs – and VPNs, we give you a number of controls, starting with: **1. Network Segmentation** to limit the blast radius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



Microsegment 1



Microsegment 2

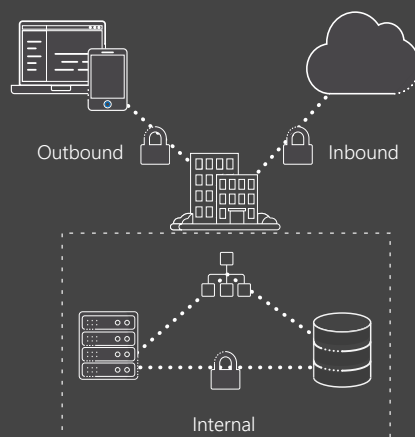


DDoS Attack



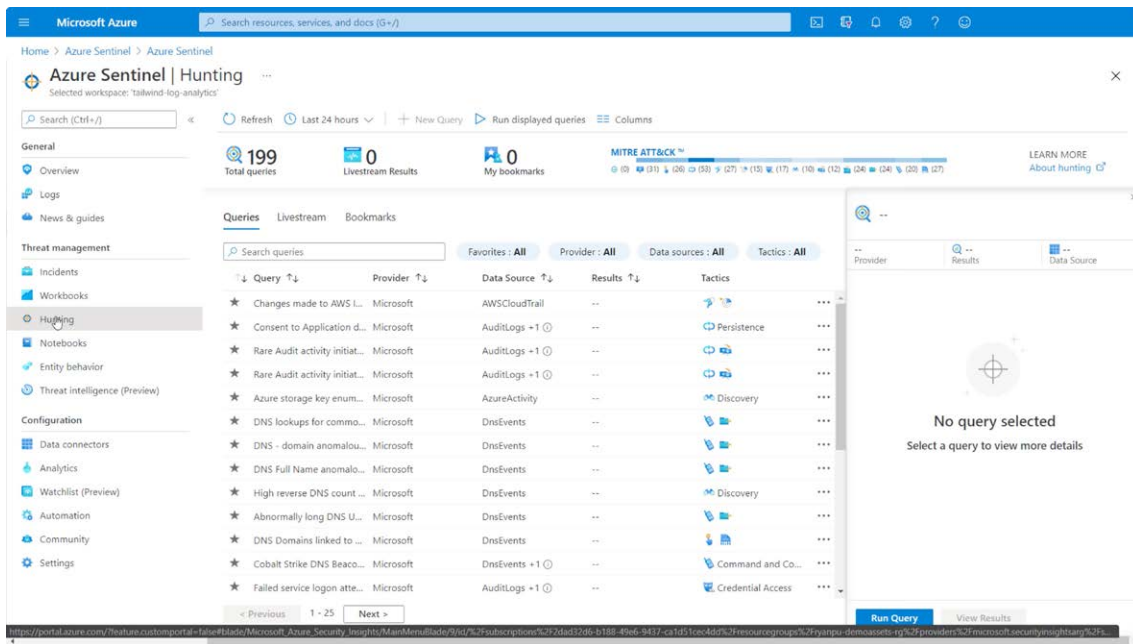
Brute force attack

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**



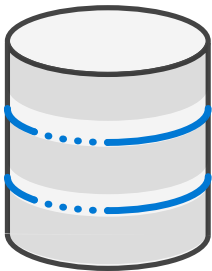
3. Encryption for all network traffic, whether it's internal, inbound or outbound

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.



Post-breach hunting in Azure Sentinel

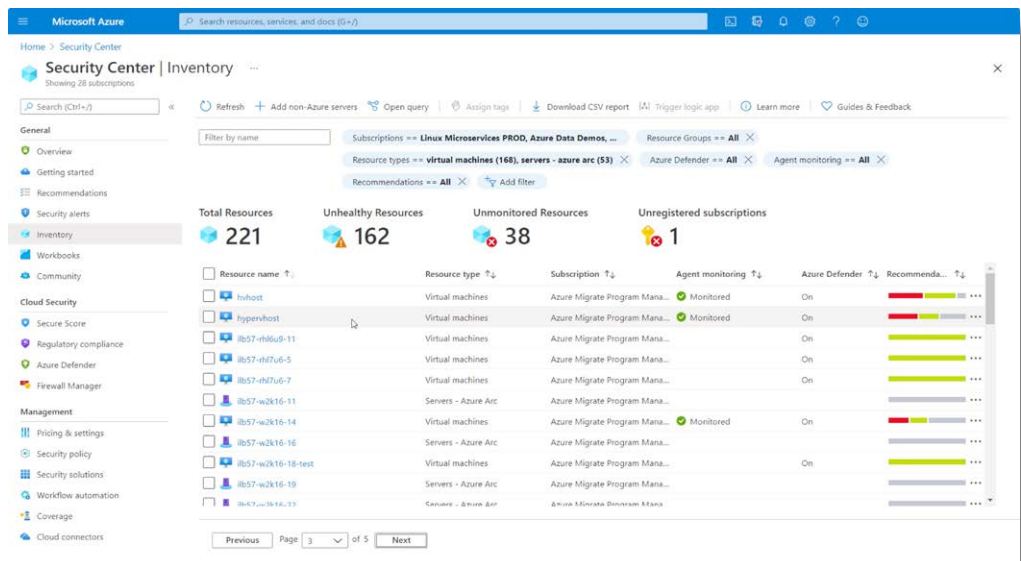
Infrastructure



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.

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

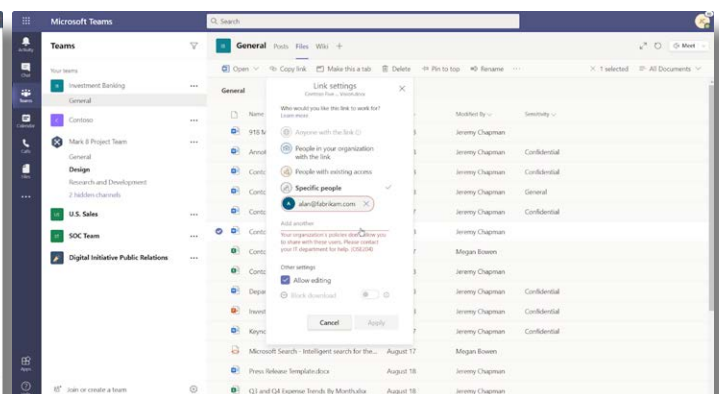


Data

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

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

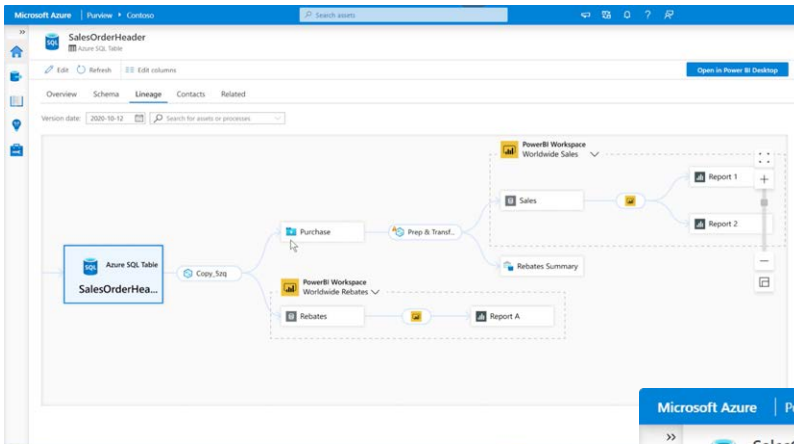
Policies are then assigned to labels to trigger protective actions, such as encryption or limiting access, restricting third party apps and services and much more.



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

A screenshot of the Azure Purview interface showing the 'Schema' view for the 'SalesOrderHeader' table. The table is an 'Azure SQL Table'. The 'Schema' tab is selected, showing a list of columns and their classifications. The columns are: SSNNumber, BillToAddressID, Comment, CreditCardNumber, CustomerID, DueDate, and Freight. The 'SSNNumber' column is highlighted, showing its classification as 'U.S. Social Security Number (SSN)'. The 'CreditCardNumber' column is classified as 'Credit Card Number', and 'CustomerID' is classified as 'CustomerID'.

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.