Introduction to Microsoft security solutions

Beata Zalewa, Sierpniowe kolonie na chmurze Azure, NTHW, 19.08.2025

zalnet

About me

Security Architect

Consultant

MICROSOFT CERTIFIED TRAINER
Microsoft
MCT
Trainer
2023 - 2024

Microsoft Certified Trainer

AI & Cybersecurity Practitioner

&#@

Developer

Freelancer

Azure

Azure @ ❤

aws

Google Cloud

1 Husband

MOM

1 Daughter

2 Cats

2 Dogs

Crime stories

Photography

zalnet

in https://www.linkedin.com/in/beatazalewa/

✉ info@zalnet.pl

BLOG https://zalnet.pl/

Agenda

- Security management capabilities of Azure
- The security capabilities of Microsoft Sentinel
- Threat protection with Microsoft Defender XDR
- The function and identity types of Microsoft Entra ID
- The authentication capabilities of Microsoft Entra
- The access management capabilities of Microsoft Entra

Security management capabilities of Azure

Microsoft Defender for Cloud

A cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyberthreats and vulnerabilities.

Cloud security posture management (CSPM)

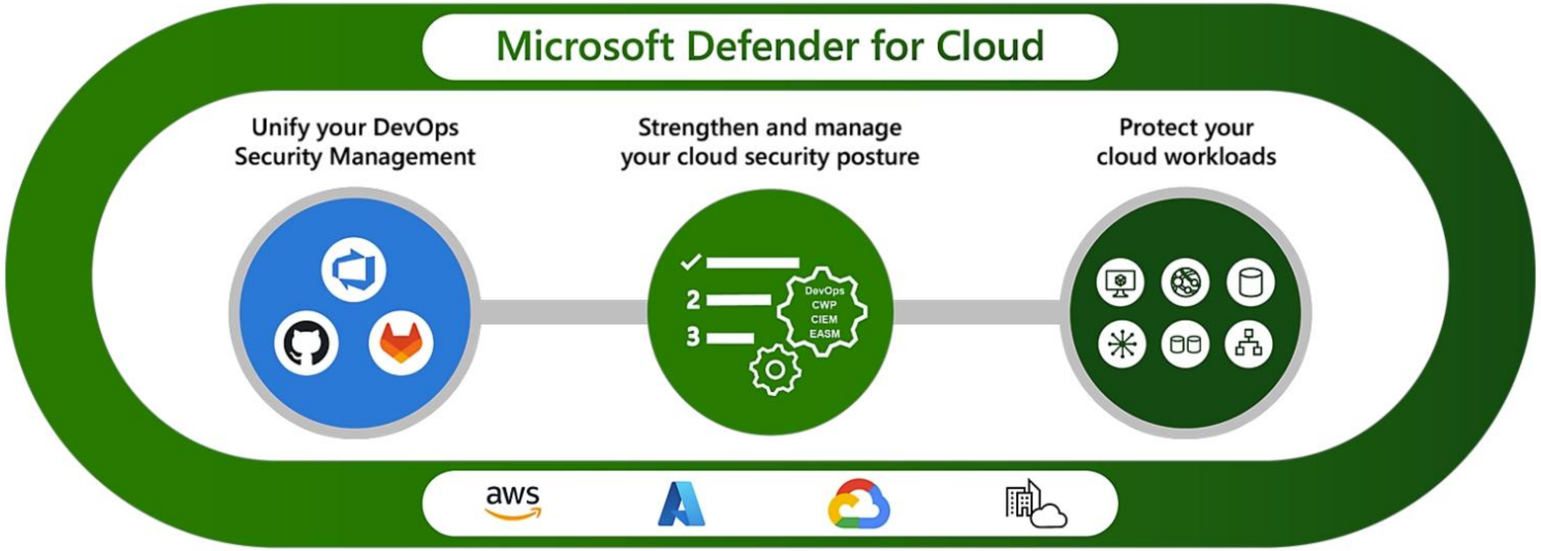
Surfaces actions that you can take to prevent breaches.

Cloud workload protection platform (CWPP)

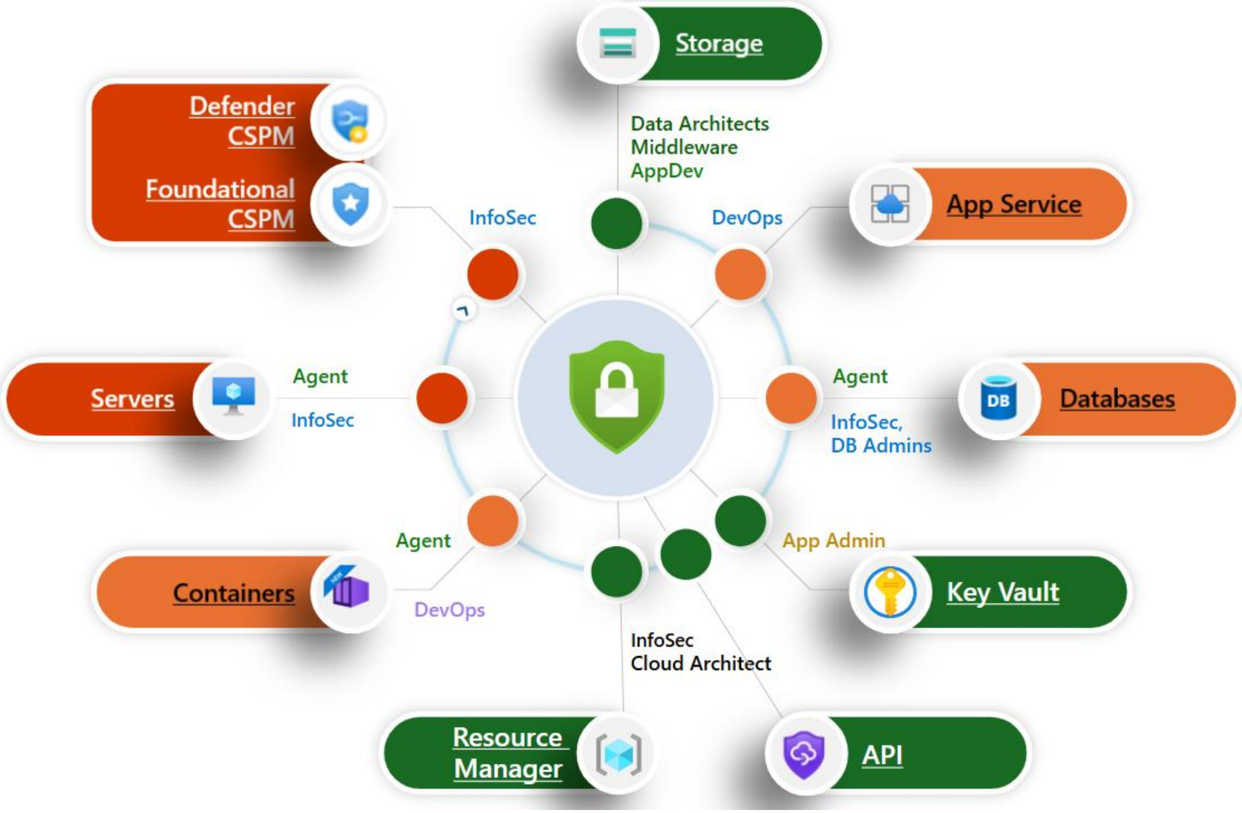
Specific protections for servers, containers, storage, databases, and other workloads.

Development security operations (DevSecOps)

Unifies security management at the code level across multicloud and multiple-pipeline environments.


Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
2
3
DevOps
CWP
CIEM
EASM
aws

Describe how security policies and initiatives improve cloud security posture



Security initiatives

- A collection of policies.
- Assigned to resources, subscriptions, and so on.

Microsoft cloud security benchmark (MCSB)

- Default security initiative in Defender for Cloud.
- Provides best practices and recommendations to improve the security of workloads, data, and services on Azure and other clouds.

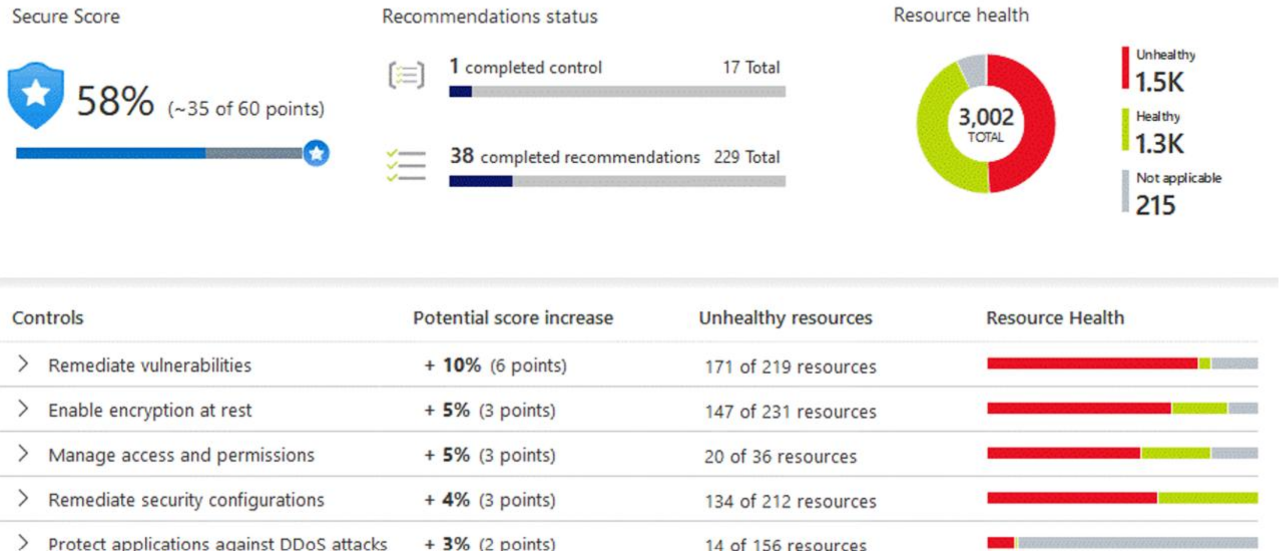
Microsoft Defender for Cloud

- Continually assesses your environment against MCSB and other security initiatives.

Cloud Security Posture Management (CSPM)

Visibility and recommendations

- Continually assesses your resources, subscriptions, and organization for security issues.
- Aggregates all the findings into a single secure score.
- Hardening recommendations on any identified security misconfigurations and weaknesses.
- Visibility and recommendations across your multicloud environment.
- Embeds capabilities of Microsoft Security Copilot on the recommendations page.



Secure Score

58% (~35 of 60 points)

Recommendations status

1 completed control 17 Total

38 completed recommendations 229 Total

Resource health

3,002 TOTAL

Unhealthy 1.5K

Healthy 1.3K

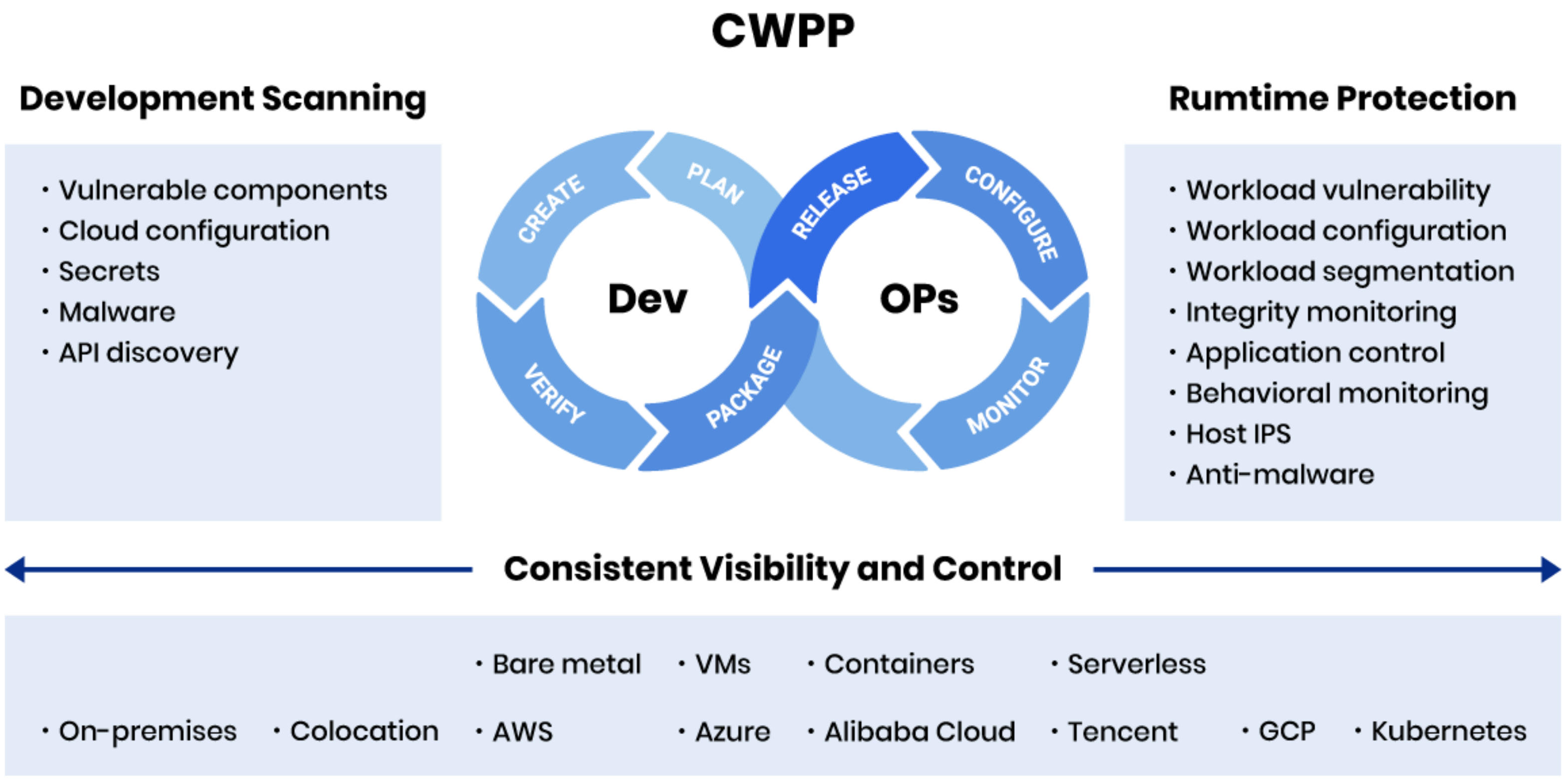
Not applicable 215

Controls	Potential score increase	Unhealthy resources	Resource Health
Remediate vulnerabilities	+ **10%** (6 points)	171 of 219 resources	
Enable encryption at rest	+ **5%** (3 points)	147 of 231 resources	
Manage access and permissions	+ **5%** (3 points)	20 of 36 resources	
Remediate security configurations	+ **4%** (3 points)	134 of 212 resources	
Protect applications against DDoS attacks	+ **3%** (2 points)	14 of 156 resources	

Cloud workload protection platform (CWPP)

CWPP plans offer enhanced security features for your workloads.

- Endpoint detection and response
- Vulnerability scanning
- Multicloud security
- Hybrid security
- Threat protection alerts
- Access and application controls



CWPP

Development Scanning

- Vulnerable components
- Cloud configuration
- Secrets
- Malware
- API discovery

Rumtime Protection

- Workload vulnerability
- Workload configuration
- Workload segmentation
- Integrity monitoring
- Application control
- Behavioral monitoring
- Host IPS
- Anti-malware

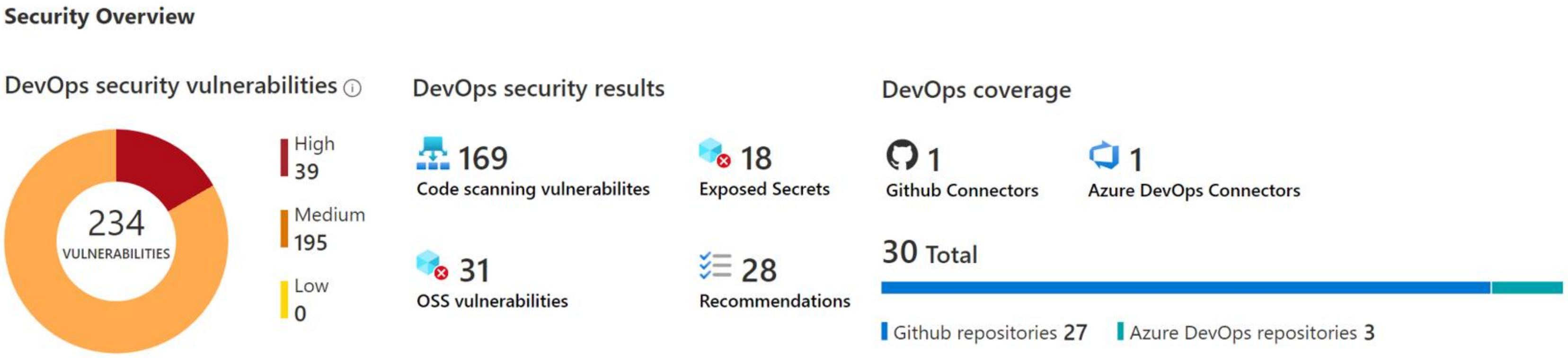
Consistent Visibility and Control

- Bare metal
- VMs
- Containers
- Serverless
- On-premises
- Colocation
- AWS
- Azure
- Alibaba Cloud
- Tencent
- GCP
- Kubernetes

Development security operations (DevSecOps)

Empowers security teams to manage DevOps security across multipipeline environments.

- Unified visibility into DevOps security posture.
- Strengthen configurations of cloud resources in the development life cycle.
- Prioritize remediation of critical issues in code.



Security Overview

DevOps security vulnerabilities

234
VULNERABILITIES

High
39

Medium
195

Low
0

DevOps security results

169
Code scanning vulnerabilites

18
Exposed Secrets

31
OSS vulnerabilities

28
Recommendations

DevOps coverage

1
Github Connectors

1
Azure DevOps Connectors

30 Total

Github repositories 27

Azure DevOps repositories 3

The security capabilities of Microsoft Sentinel

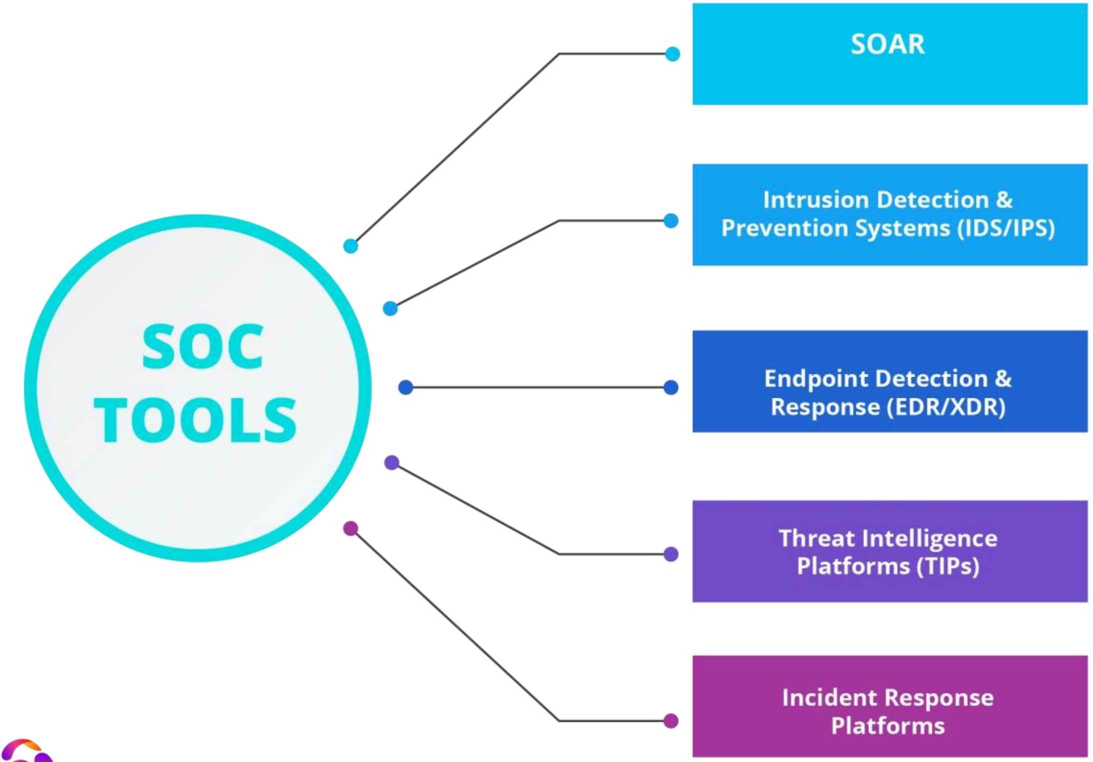
SIEM and SOAR

Security incident and event management (SIEM)

- Collects data from across the whole digital estate.
- Analyzes and looks for correlations or anomalies.
- Generates alerts and incidents.

Security orchestration automated response (SOAR)

- Takes alerts from many sources, such as SIEM systems.
- Triggers action-driven automated workflows and processes.
- Runs security tasks that mitigate the issue.


SOC TOOLS
SOAR
Intrusion Detection & Prevention Systems (IDS/IPS)
Endpoint Detection & Response (EDR/XDR)
Threat Intelligence Platforms (TIPs)
Incident Response Platforms

eventus™

Microsoft Sentinel threat detection and mitigation

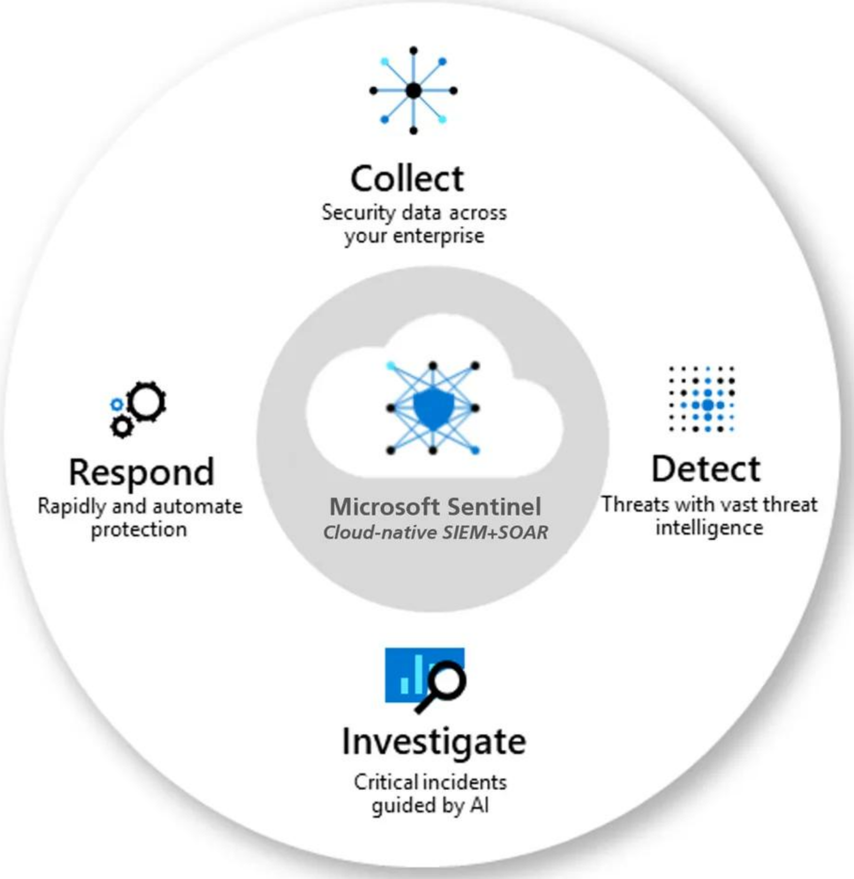
Collect data at scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.

Respond to incidents rapidly with built-in orchestration and automation of common security.

Microsoft Sentinel can now be accessed from the Microsoft Defender portal, which delivers Microsoft's unified security operations platform.


Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Microsoft Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI

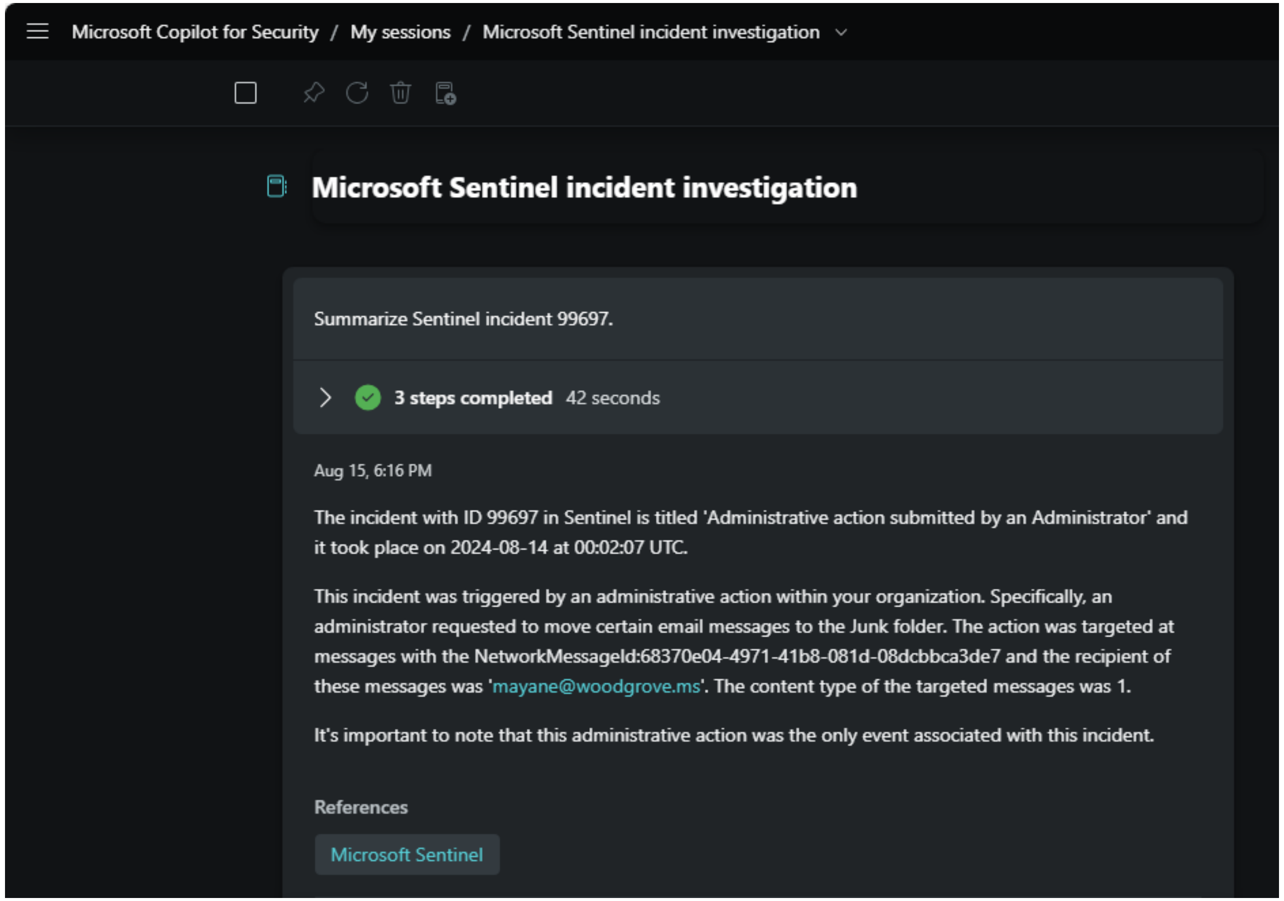
Microsoft Security Copilot integration with Microsoft Sentinel

Copilot plugins:

- Microsoft Sentinel
- Natural language to KQL for Microsoft Sentinel

Copilot integration supported through:

- Standalone experience
- Embedded experience in the Microsoft Defender Portal



Microsoft Copilot for Security / My sessions / Microsoft Sentinel incident investigation

Microsoft Sentinel incident investigation

Summarize Sentinel incident 99697.

3 steps completed 42 seconds

Aug 15, 6:16 PM

The incident with ID 99697 in Sentinel is titled 'Administrative action submitted by an Administrator' and it took place on 2024-08-14 at 00:02:07 UTC.

This incident was triggered by an administrative action within your organization. Specifically, an administrator requested to move certain email messages to the Junk folder. The action was targeted at messages with the NetworkMessageId:68370e04-4971-41b8-081d-08dcbbca3de7 and the recipient of these messages was 'mayane@woodgrove.ms'. The content type of the targeted messages was 1.

It's important to note that this administrative action was the only event associated with this incident.

References

Threat protection with Microsoft Defender XDR

Microsoft Defender XDR

An enterprise defense suite that natively coordinates detection, prevention, investigation, and response across your environment to provide integrated protection against sophisticated attacks.

The Defender includes:

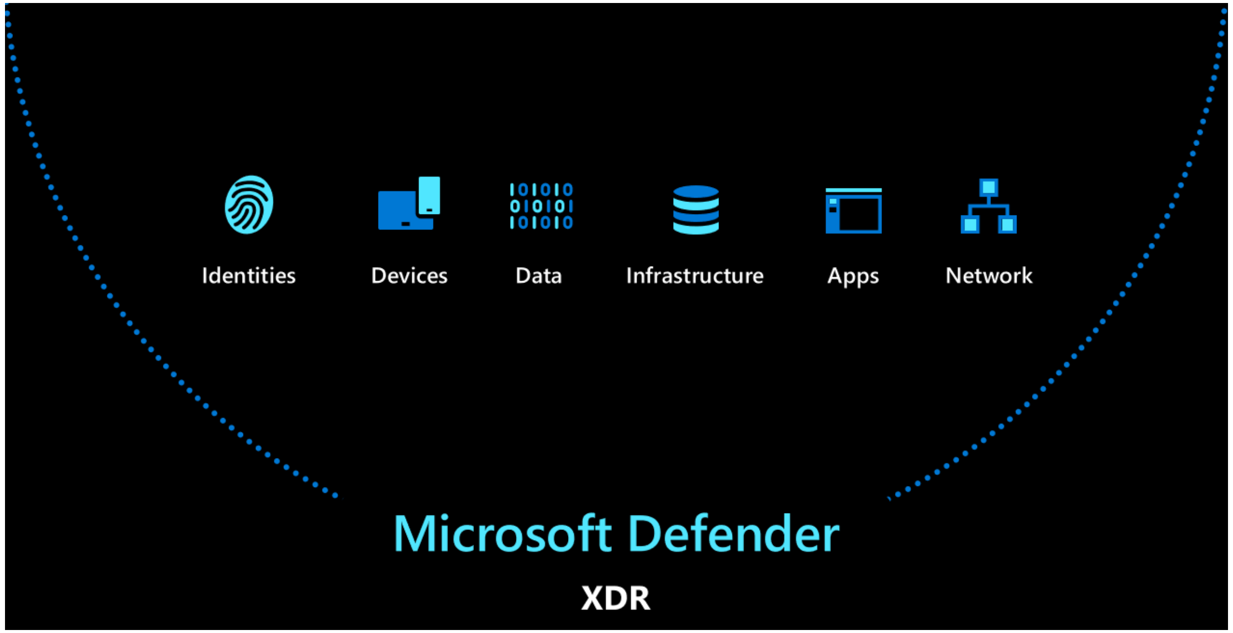
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management

Microsoft Defender XDR portal

- Delivers a unified security operations platform.
- Includes information and insights from Defender XDR, Microsoft Sentinel, and more.

Integration with Microsoft Security Copilot:

- Enabled through plugins
- Standalone and embedded experiences.



Microsoft Defender for Office 365

Seamless integration into your Office 365 subscription that provides protection against threats that arrive in email, links, attachments, or collaboration tools.

Prevent and detect

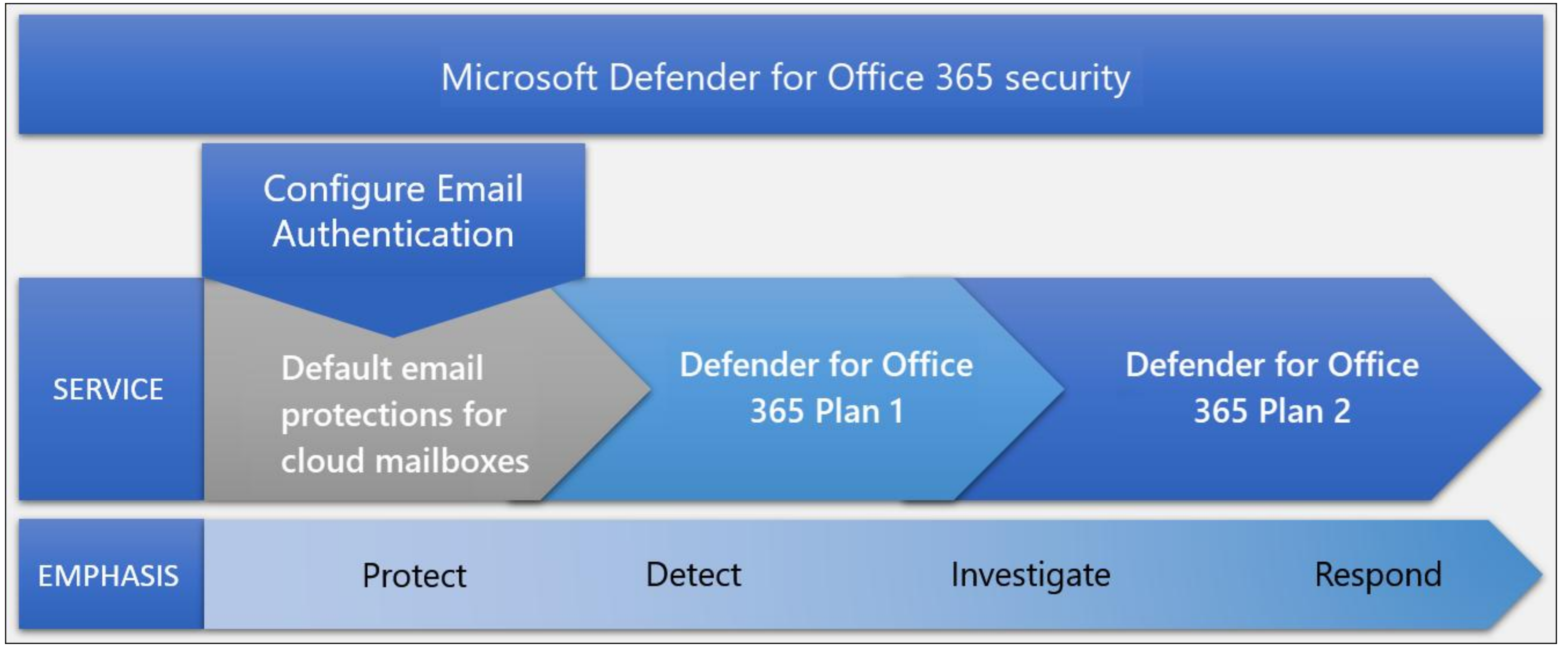
- Policies for anti-malware, anti-spam, anti-phishing
- Safe attachments
- Attack simulation training
- More…

Investigate

- Audit log search
- Message trace
- Explorer
- More..

Respond

- Zero-hour auto purge (ZAP)
- Automated investigation and response
- More…



Microsoft Defender for Office 365 security

Configure Email Authentication

SERVICE

Default email protections for cloud mailboxes

Defender for Office 365 Plan 1

Defender for Office 365 Plan 2

EMPHASIS

Protect

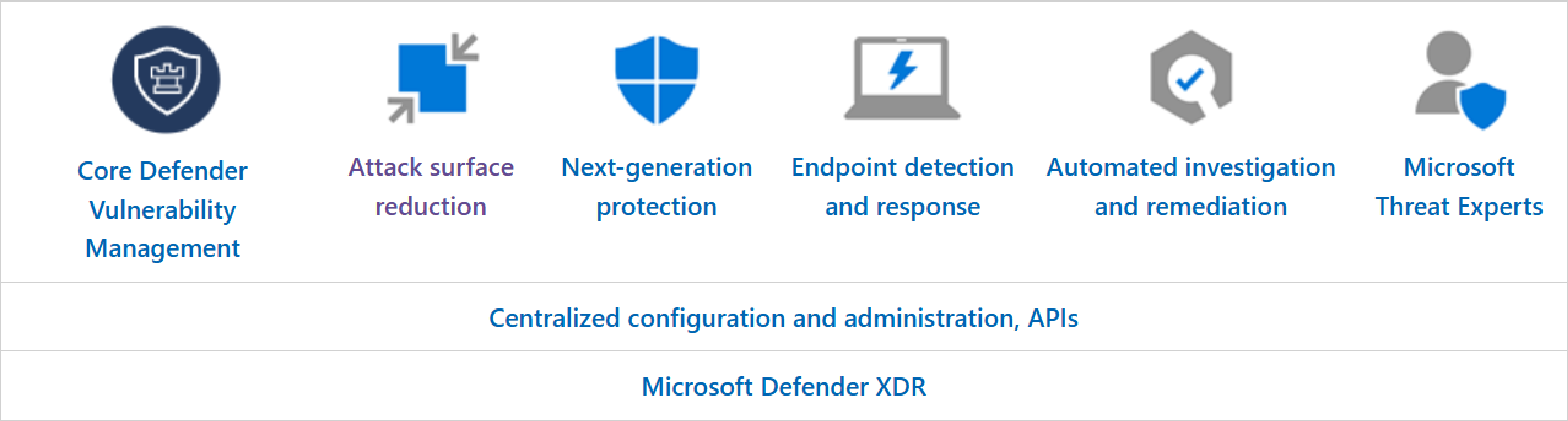
Detect

Investigate

Respond

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints.



Core Defender Vulnerability Management

Attack surface reduction

Next-generation protection

Endpoint detection and response

Automated investigation and remediation

Microsoft Threat Experts

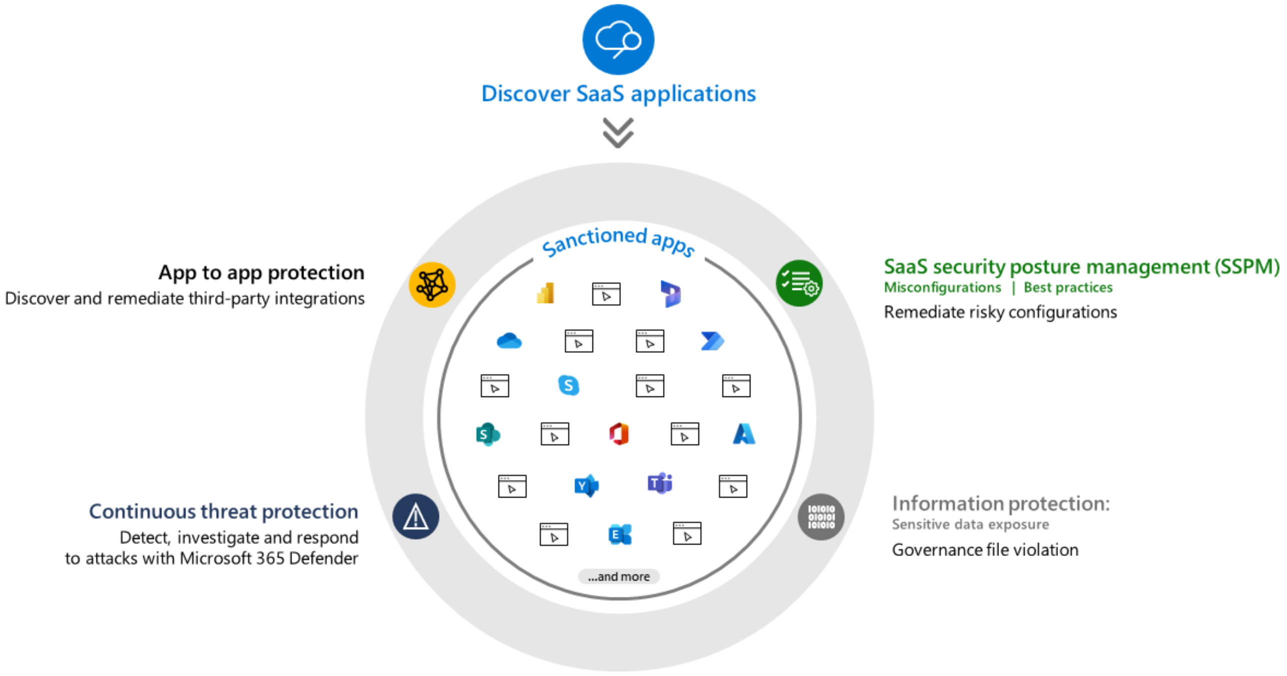
Centralized configuration and administration, APIs

Microsoft Defender XDR

Microsoft Defender for Cloud Apps

Provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

- Discover SaaS applications
- Information protection
- SaaS Security Posture Management (SSPM)
- Advanced threat protection
- App-to-app protection with app governance



Discover SaaS applications

Sanctioned apps

...and more

App to app protection
Discover and remediate third-party integrations

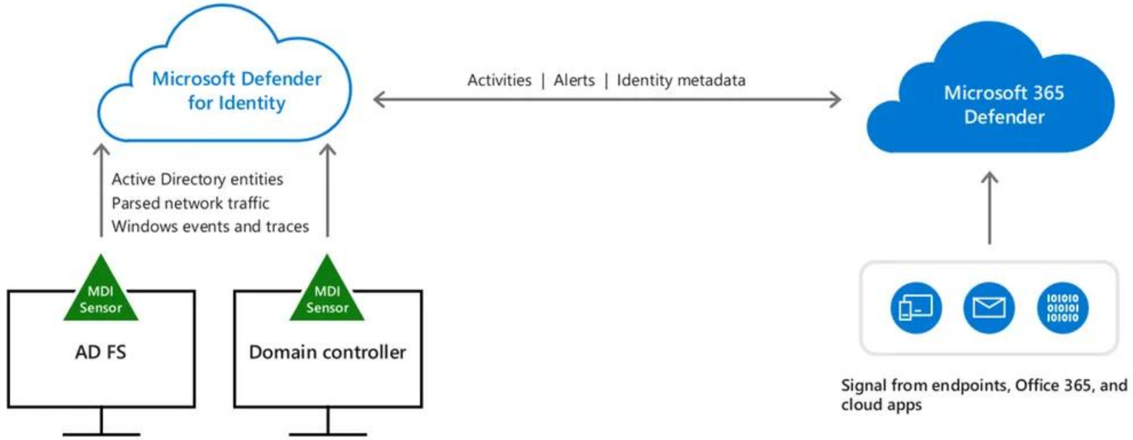
SaaS security posture management (SSPM)
Misconfigurations | Best practices
Remediate risky configurations

Continuous threat protection
Detect, investigate and respond to attacks with Microsoft 365 Defender

Information protection:
Sensitive data exposure
Governance file violation

Microsoft Defender for Identity

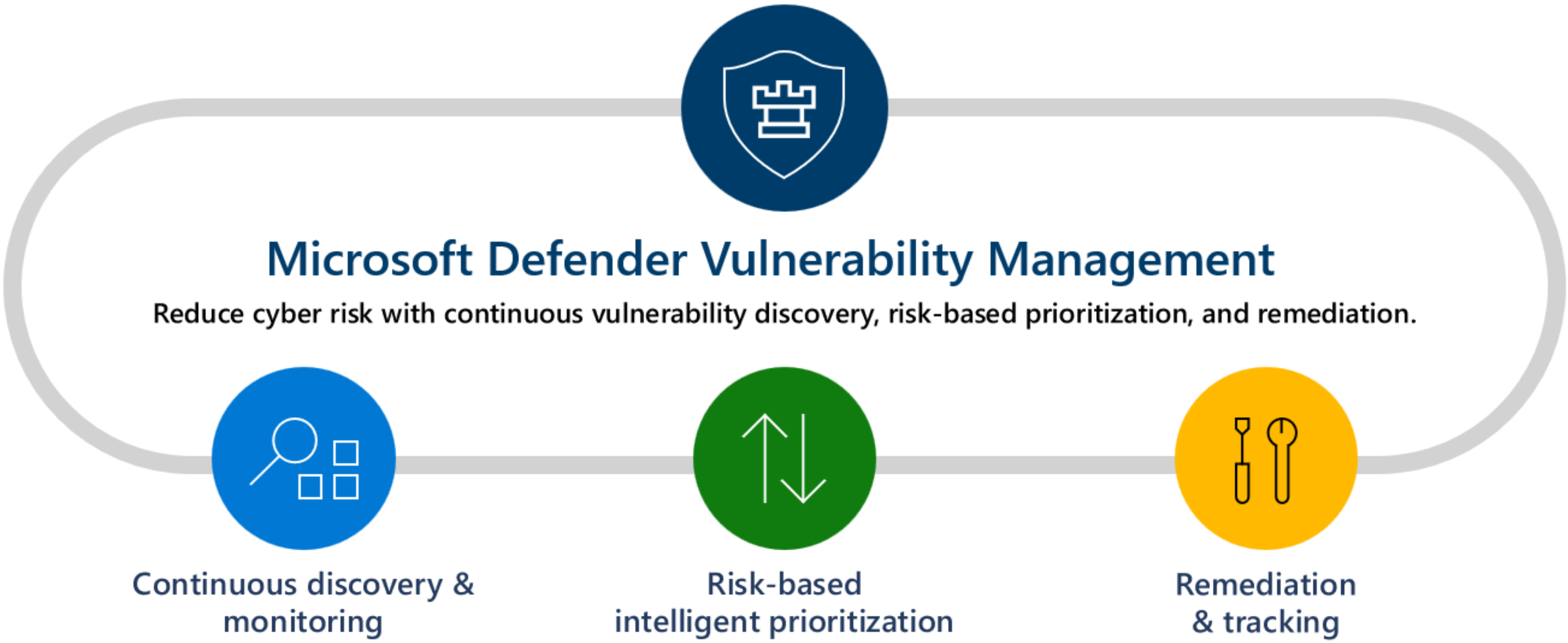
A cloud-based security solution that uses signals from your on-premises identity infrastructure servers to detect threats, like privilege escalation or high-risk lateral movement, and reports on easily exploited identity issues.


Microsoft Defender for Identity
Activities | Alerts | Identity metadata
Microsoft 365 Defender
Active Directory entities
Parsed network traffic
Windows events and traces
MDI Sensor
AD FS
MDI Sensor
Domain controller
Signal from endpoints, Office 365, and cloud apps

- Software-based sensors installed on your on-premises identity infrastructure servers send signals to the Microsoft Defender for Identity service.
- Defender for Identity uses signals to provide identity threat detection and response (ITDR) that enables security pros to:
  - Proactively assess your identity posture
  - Detect threats, using real-time analytics and data intelligence
  - Investigate alerts and user activities
  - Remediate actions
- The Microsoft Defender portal provides security teams a unified security operations platform for investigating and responding to attacks.

Microsoft Defender Vulnerability Management

Delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.



Microsoft Defender Vulnerability Management

Reduce cyber risk with continuous vulnerability discovery, risk-based prioritization, and remediation.

Continuous discovery & monitoring

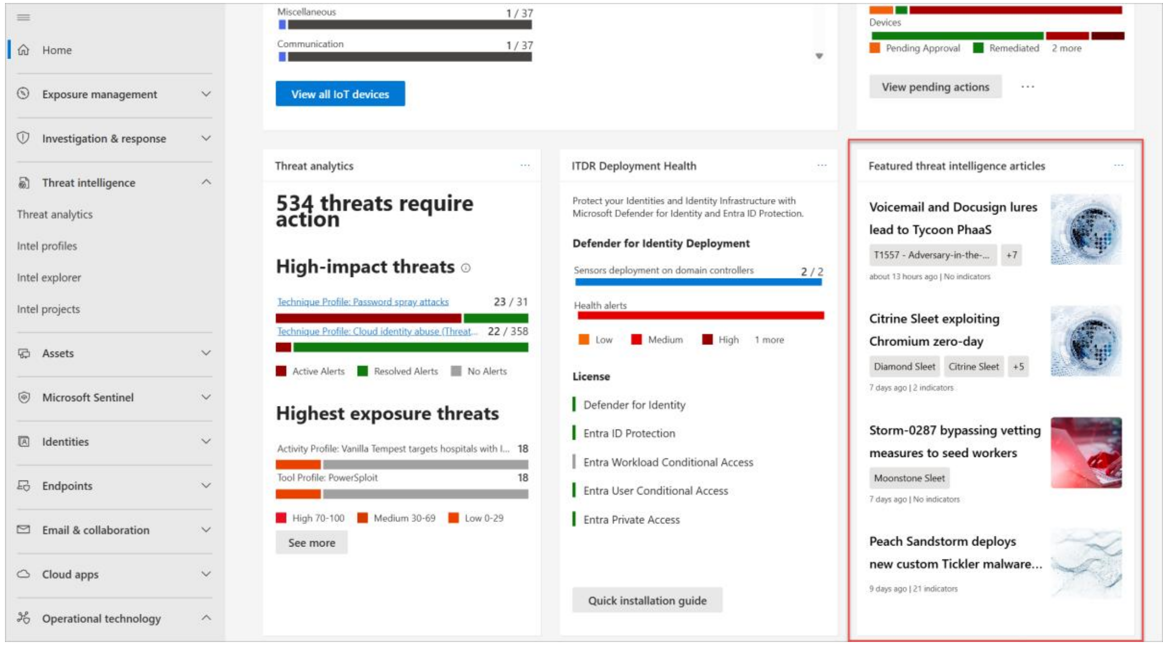
Risk-based intelligent prioritization

Remediation & tracking

Microsoft Defender Threat Intelligence

Aggregates and enriches critical threat intelligence data sources and is integrated with Microsoft Security Copilot to help security analyst as they triage, investigate, and remediate vulnerabilities in their organization.

- Threat analytics - Understand how emerging threats impact your organization's environment.
- Intel profiles - A definitive source of Microsoft's shareable knowledge on tracked threat actors, malicious tools, and vulnerabilities.
- Intel explorer - Where analysts can quickly scan new featured articles and perform search for intelligence gathering.
- Intel projects – Users can create projects that organize indicators of compromise (IOCs) from an investigation and contain associated artifacts and a detailed history.



Miscellaneous 1 / 37

Communication 1 / 37

Devices

🟧 Pending Approval 🟩 Remediated 2 more

Threat analytics

534 threats require action

High-impact threats

Technique Profile: Password spray attacks 23 / 31

Technique Profile: Cloud identity abuse (Threat... 22 / 358

🟥 Active Alerts 🟩 Resolved Alerts ⬜ No Alerts

Highest exposure threats

Activity Profile: Vanilla Tempest targets hospitals with I... 18

Tool Profile: PowerSploit 18

🟥 High 70-100 🟧 Medium 30-69 🟧 Low 0-29

ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Entra ID Protection.

Defender for Identity Deployment

Sensors deployment on domain controllers 2 / 2

Health alerts

🟧 Low 🟥 Medium 🟥 High 1 more

License

Defender for Identity

Entra ID Protection

Entra Workload Conditional Access

Entra User Conditional Access

Entra Private Access

Featured threat intelligence articles

Voicemail and Docusign lures lead to Tycoon PhaaS

T1557 - Adversary-in-the-... +7

about 13 hours ago | No indicators

Citrine Sleet exploiting Chromium zero-day

Diamond Sleet Citrine Sleet +5

7 days ago | 2 indicators

Storm-0287 bypassing vetting measures to seed workers

Moonstone Sleet

7 days ago | No indicators

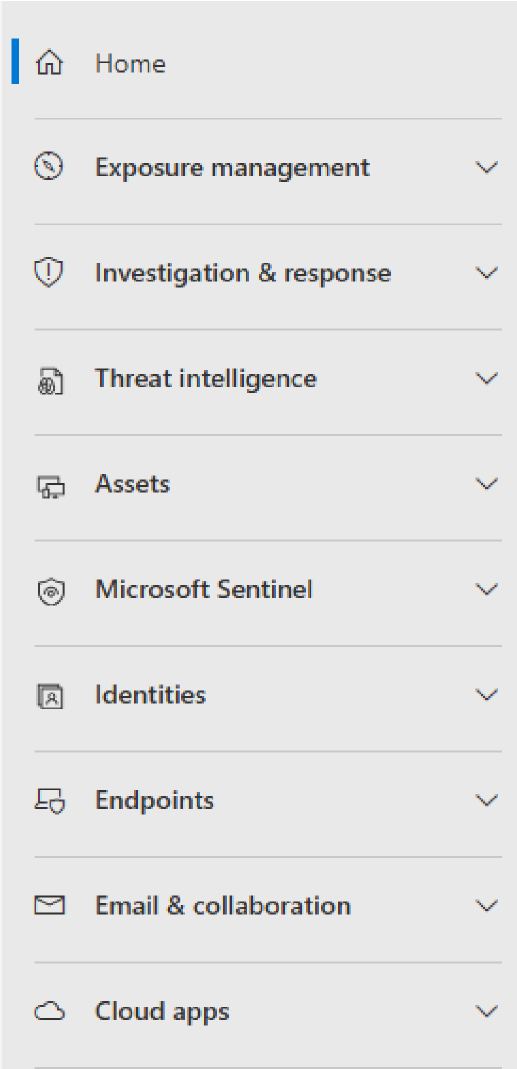
Peach Sandstorm deploys new custom Tickler malware...

9 days ago | 21 indicators

Microsoft Defender portal

The Microsoft Defender portal delivers a unified security operations platform

- The best of SIEM, XDR, posture management, and threat intelligence with advanced generative AI as a single platform.
- Combines protection, detection, investigation, and response to threats across your entire organization and all its components, in one place.

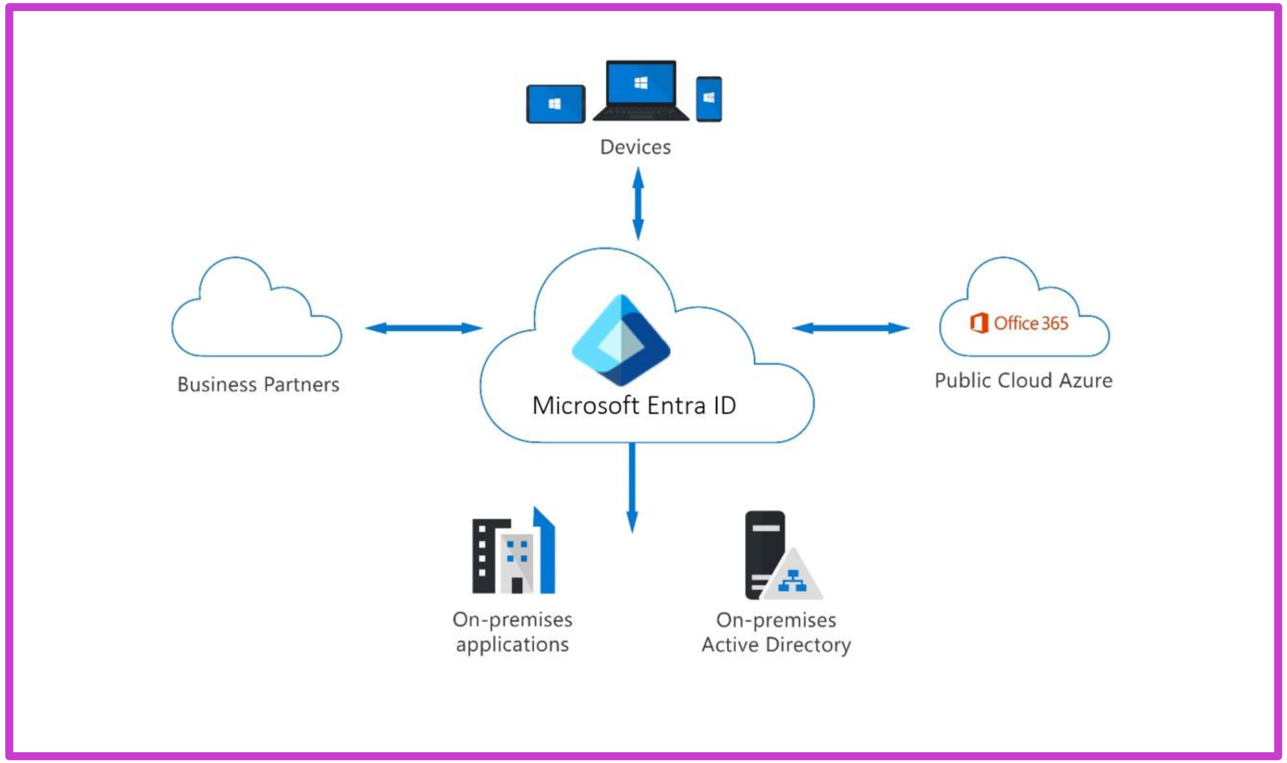


The function and identity types of Microsoft Entra ID

Microsoft Entra ID

Microsoft’s cloud-based identity and access management service.

- Organizations can enable their employees, guests, and others to sign in and access the resources they need.
- Provide a single identity system for their cloud and on-premises applications.
- Protect user identities and credentials to meet an organization’s access governance requirements.
- Subscribers to Azure services, Microsoft 365, or Dynamics 365 automatically have access to Microsoft Entra ID.
- Identity secure score.



Identity types

Human (user) identities

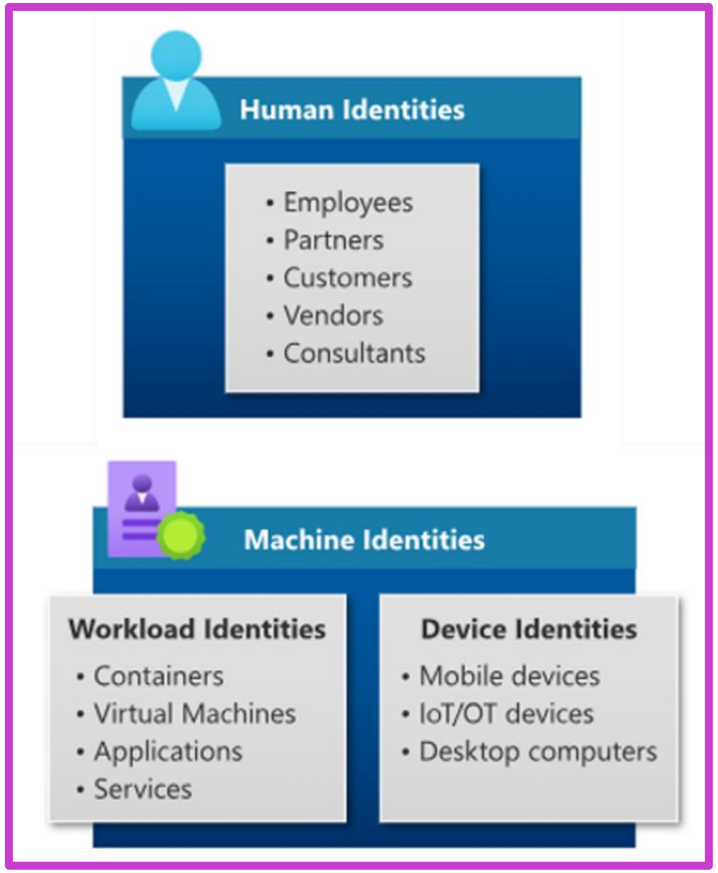
- Internal users – Employees.
- External users – Guests, partners, customers, and so on.

Workload identities (an identity assigned to an application or service)

- Service principal – Uses Microsoft Entra ID for identity and access functions; app developers manage credentials.
- Managed identities – A service principal managed in Microsoft Entra ID that eliminates the need for app developers to manage credentials.

Devices

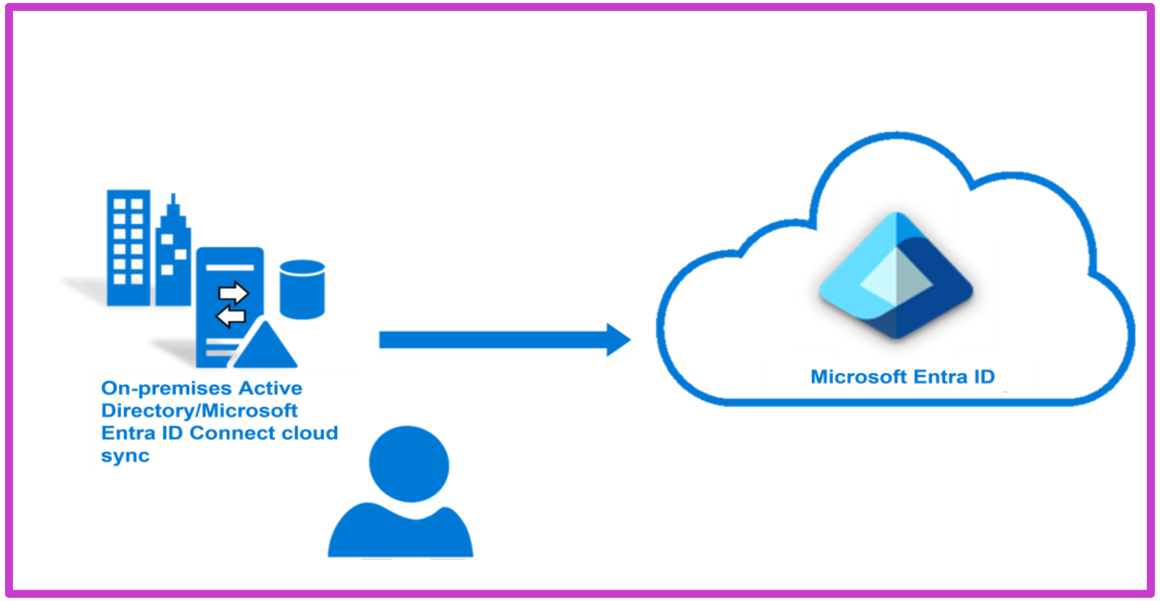
- Microsoft Entra ID registered – Support for bring your own device.
- Microsoft Entra ID joined – Device joined via an organizational account.
- Hybrid joined – Devices are joined to your on-premises Active Directory and Microsoft Entra ID, requiring organizational account to sign in.



Hybrid identity

What is a hybrid identity?

- A common user identity for authentication and authorization to on-premises and cloud resources.
- Hybrid identity is accomplished through:
  - Inter-directory provisioning – A user in Active Directory is provisioned into Microsoft Entra ID.
  - Synchronization – Identity information for your on-premises users and groups matches the cloud.
- Microsoft Entra ID Connect cloud sync – A method for provisioning and synchronization.


On-premises Active Directory/Microsoft Entra ID Connect cloud sync
Microsoft Entra ID

The authentication capabilities of Microsoft Entra

Authentication methods of Microsoft Entra

Passwords (primary auth)

Phone-based authentication

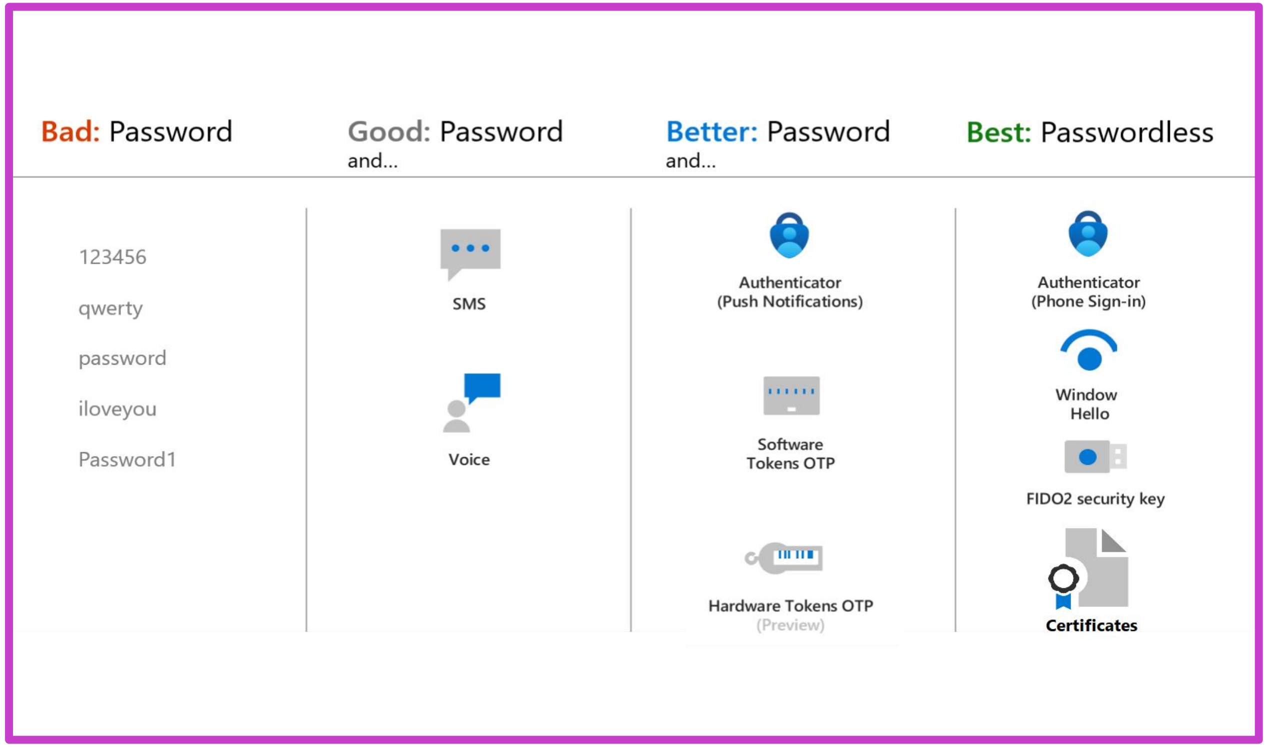
- SMS (primary and secondary auth)
- Voice (secondary auth)

OATH (secondary auth)

- Standard for how one-time password codes are generated
- SW tokens
- HW tokens

Passwordless (primary and secondary auth)

- Windows Hello
- Microsoft Authenticator
- FIDO2
- Certificates (primary auth)



Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456 qwerty password iloveyou Password1	SMS Voice	Authenticator (Push Notifications) Software Tokens OTP Hardware Tokens OTP (Preview)	Authenticator (Phone Sign-in) Window Hello FIDO2 security key Certificates

Multifactor authentication (MFA)

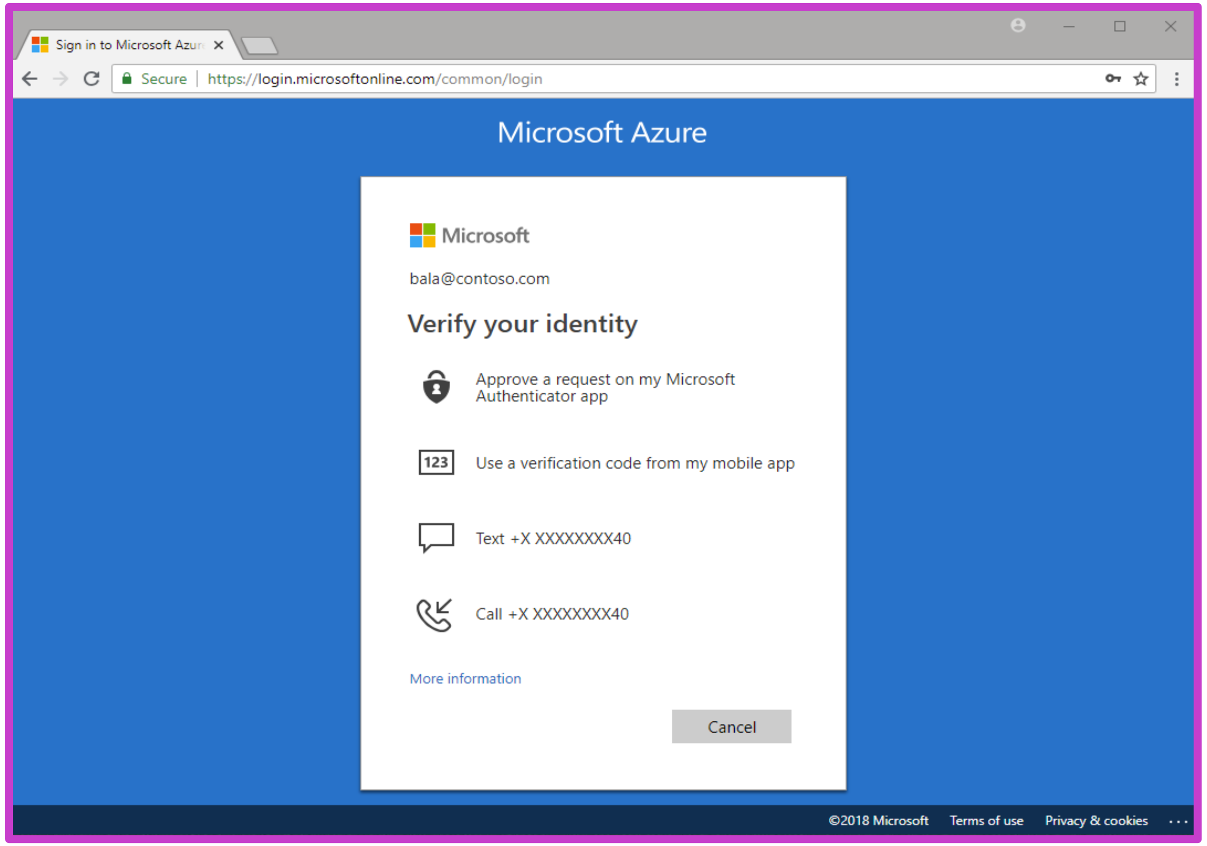
Dramatically improves the security of an identity, while still being simple for users.

MFA requires more than one form of verification

- Something you know.
- Something you have.
- Something you are.

Security defaults

- Requires all users to complete MFA as needed.
- Forces administrators to use MFA.
- Enforces MFA for all users.



Sign in to Microsoft Azure
Secure
https://login.microsoftonline.com/common/login
Microsoft Azure
Microsoft

bala@contoso.com

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

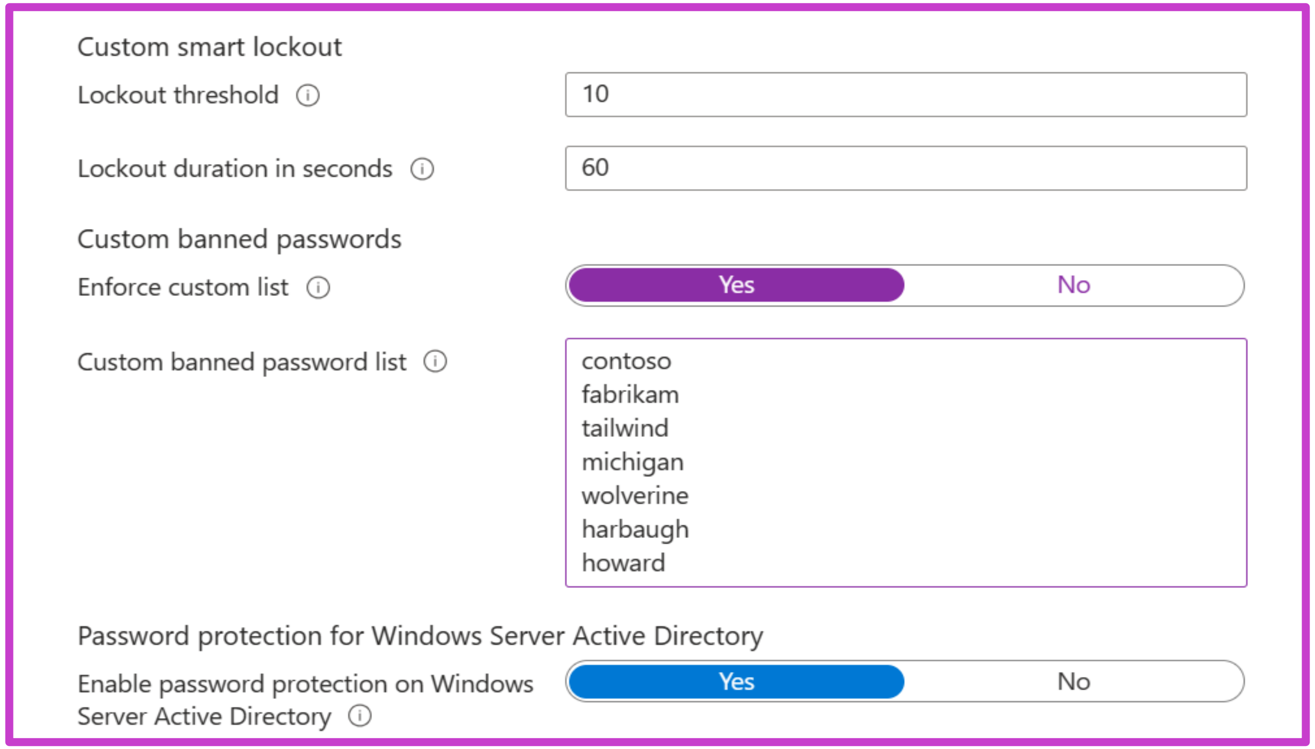
Text +X XXXXXXXX40

Call +X XXXXXXXX40

Password protection and management capabilities

Reduce the risk of users setting weak passwords:

- Global banned password list.
- Custom banned password lists.
- Protecting against password spray.
- Integrates with an on-premises Active Directory environment.



Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ [✓ Yes] No

Custom banned password list ⓘ

contoso
fabrikam
tailwind
michigan
wolverine
harbaugh
howard

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ [✓ Yes] No

The access management capabilities of Microsoft Entra

Conditional Access

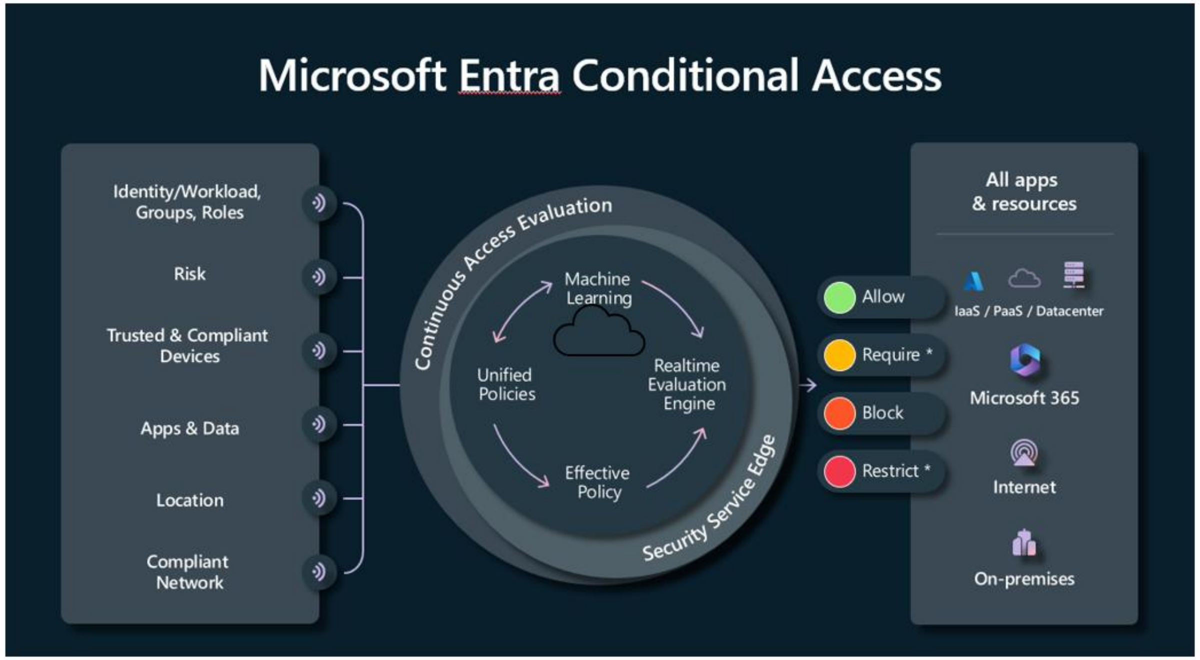
At their simplest, Conditional Access (CA) policies are if-then statements.

Assignments determine which signals to use

- Users, groups, workload identities, directory roles.
- Cloud apps or actions.
- Sign-in and user risk detection.
- Device or device platform.
- IP location.
- More…

Access controls determine how a policy is enforced

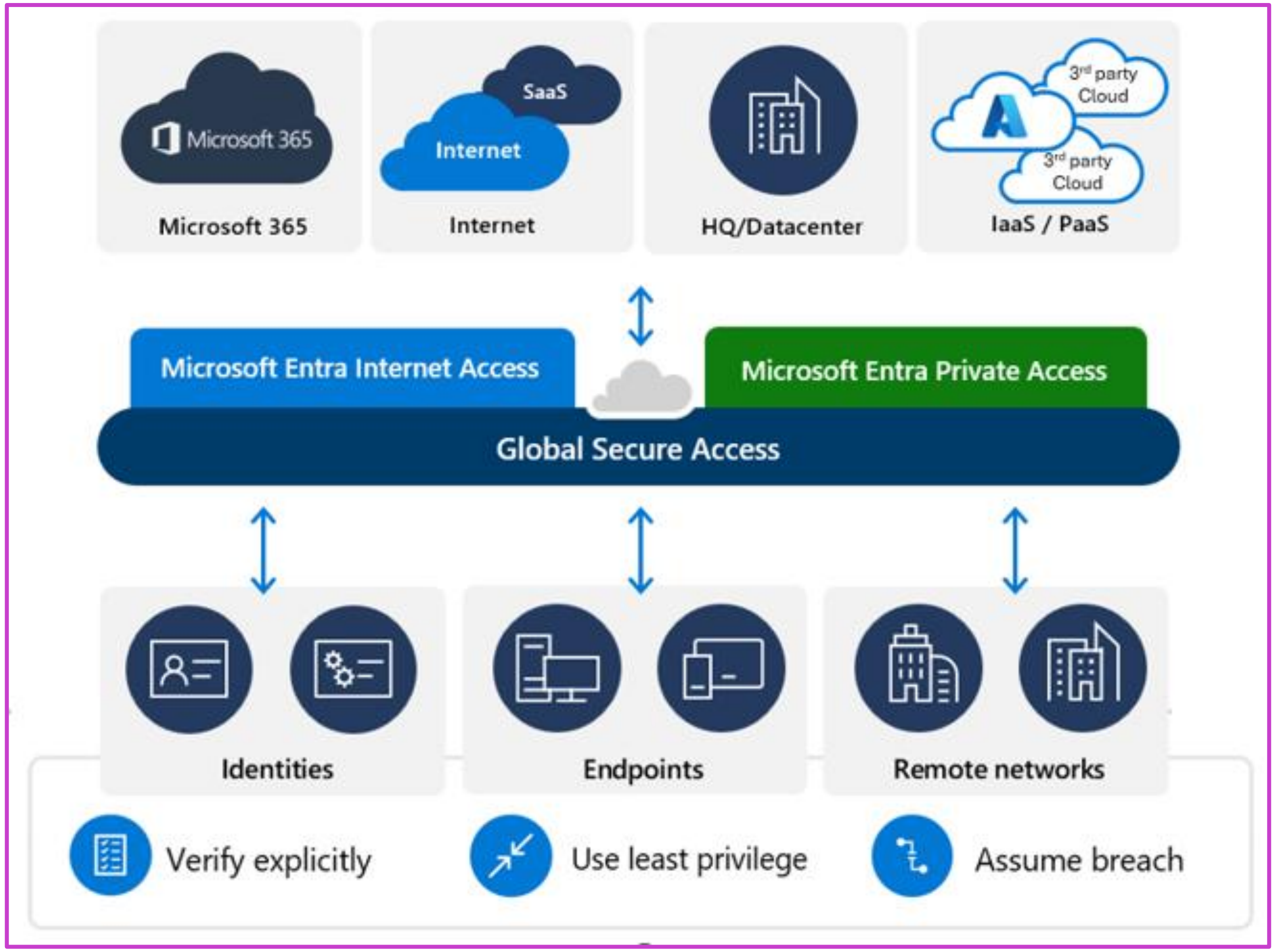
- Block access.
- Grant access – Require one or more conditions to be met before granting access.
- Session control – Enable a limited experience.



Microsoft Entra Global Secure Access

GSA converges **Zero Trust network, identity, and endpoint access controls** to secure access to any app or resource, from any location, device, or identity.

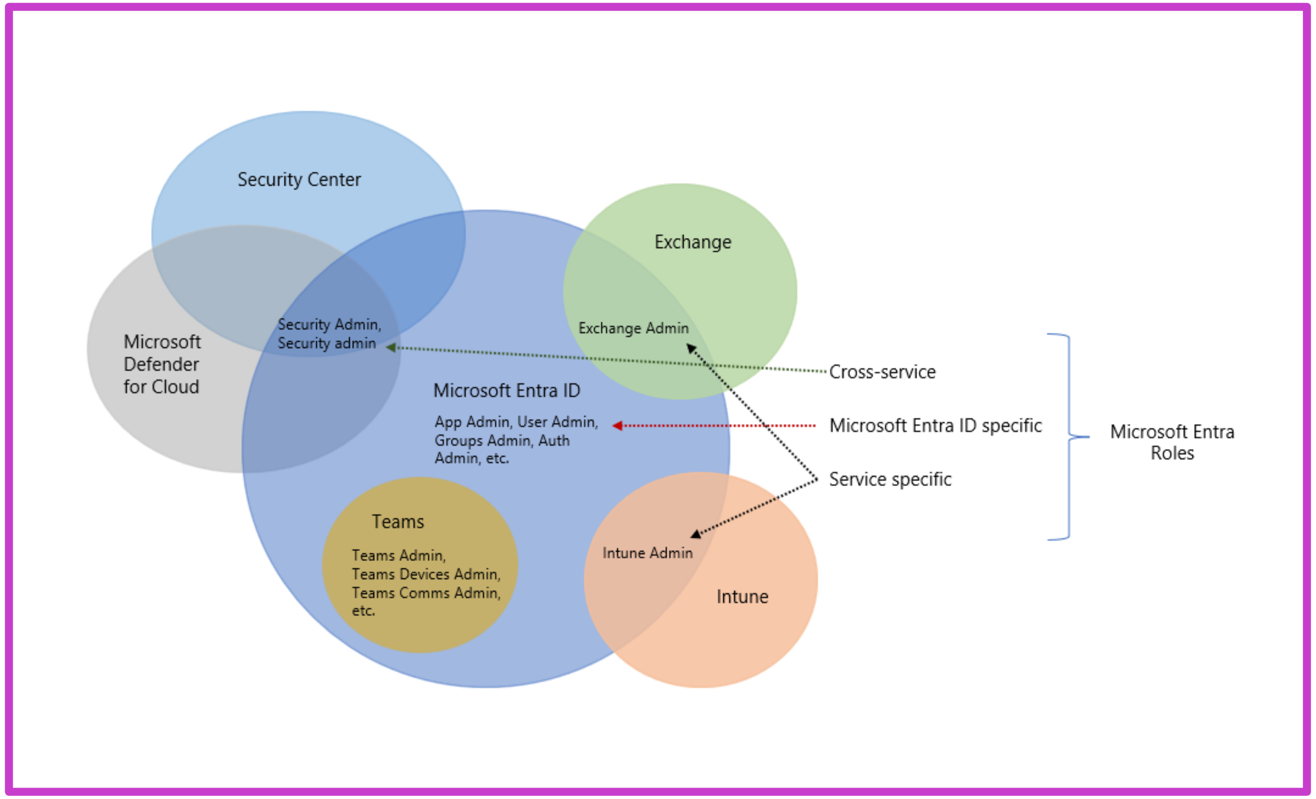
- **Microsoft Entra Internet Access** secures access to SaaS applications, including Microsoft Services, and public internet apps.
- **Microsoft Entra Private Access** provides your users secure access to your private, corporate resources.



Microsoft Entra roles and role-based access control (RBAC)

Microsoft Entra ID roles control permissions to manage Microsoft Entra resources.

- Built-in roles.
- Custom roles.
- Categories of Microsoft Entra roles:
  - Microsoft Entra specific
  - Service-specific
  - Cross service
- Only grant the access users need.


Security Center
Exchange
Microsoft Defender for Cloud
Security Admin, Security admin
Exchange Admin
Cross-service
Microsoft Entra ID
App Admin, User Admin, Groups Admin, Auth Admin, etc.
Microsoft Entra ID specific
Microsoft Entra Roles
Service specific
Teams
Teams Admin, Teams Devices Admin, Teams Comms Admin, etc.
Intune Admin
Intune

Identity governance in Microsoft Entra

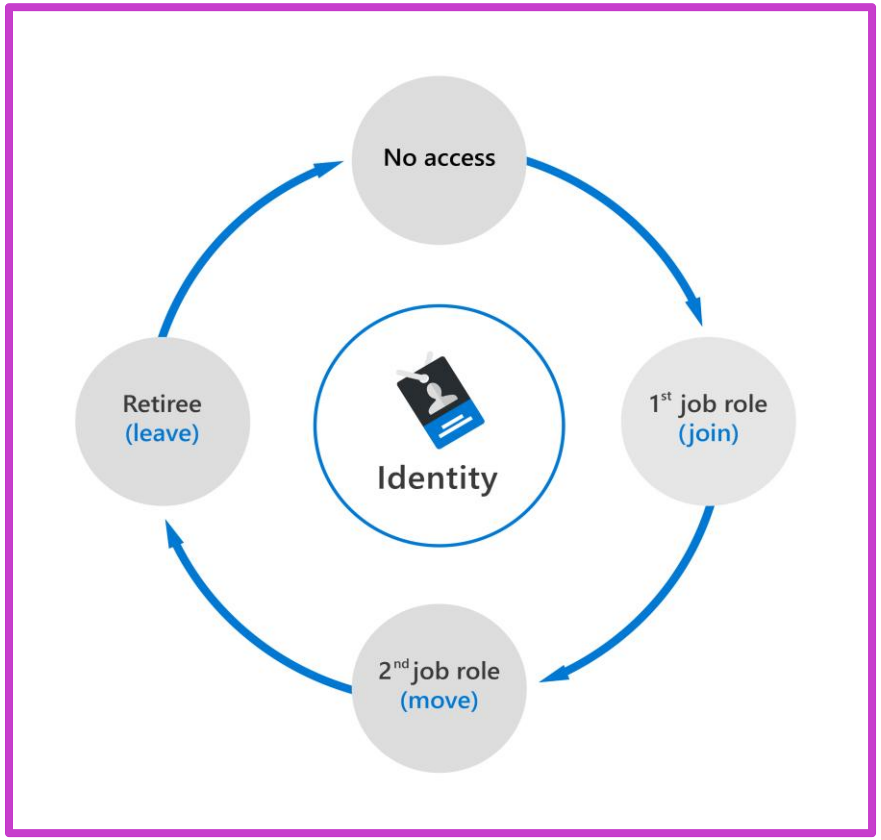
The right people have the right access to the right resources.

The tasks of Microsoft Entra identity governance

- Govern the identity life cycle.
- Govern access life cycle.
- Secure privileged access for administration.

Identity life cycle

- Join: A new digital identity is created.
- Move: Update access authorizations.
- Leave: Access may need to be removed.



Privileged Identity Management (PIM)

PIM enables you to manage, control, and monitor access to important resources in your organization.

1. Just in time, providing privileged access only when needed, and not before.
2. Time-bound, by assigning start and end dates that indicate when a user can access resources.
3. Approval-based, requiring specific approval to activate privileges.
4. Visible, sending notifications when privileged roles are activated.
5. Auditable, allowing a full access history to be downloaded.

Microsoft Entra Identity Protection

Detect

- User risk
- Sign-in risk

Investigate

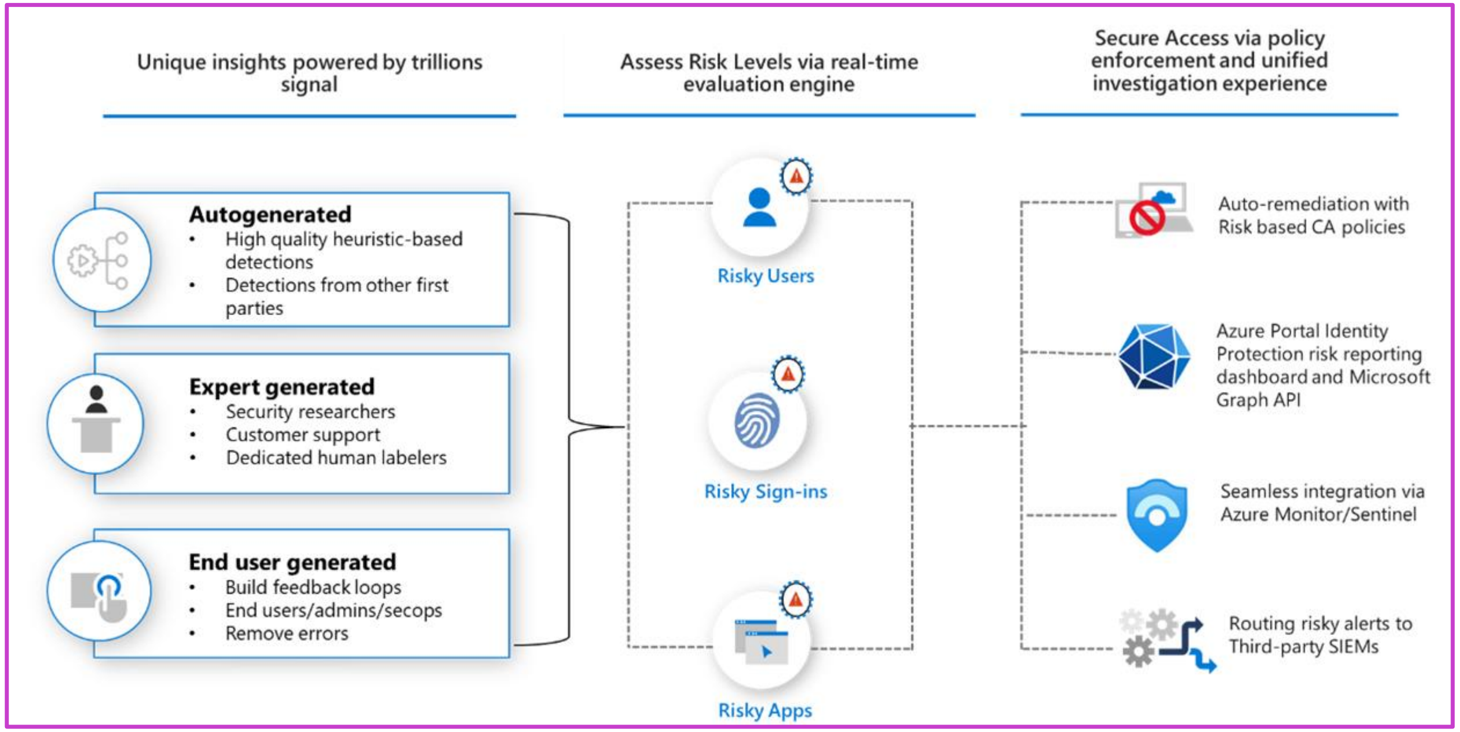
- Risk detections report
- Risky sign-ins report
- Risky users report (embeds Copilot)
- Risky workload identities report

Remediate

- Automated remediation
- Manual remediation

Export

- Export risk detection data to first and third-party utilities for further analysis.



Unique insights powered by trillions signal

Autogenerated
- High quality heuristic-based detections
- Detections from other first parties

Expert generated
- Security researchers
- Customer support
- Dedicated human labelers

End user generated
- Build feedback loops
- End users/admins/secops
- Remove errors

Assess Risk Levels via real-time evaluation engine

Risky Users

Risky Sign-ins

Risky Apps

Secure Access via policy enforcement and unified investigation experience

Auto-remediation with Risk based CA policies

Azure Portal Identity Protection risk reporting dashboard and Microsoft Graph API

Seamless integration via Azure Monitor/Sentinel

Routing risky alerts to Third-party SIEMs

Stale poszukuję nowych możliwości i ekscytujących wyzwań. Jeśli chcesz się ze mną skontaktować, proszę, skorzystaj z poniższych kanałów:

zalnet
BEATA ZALEWA

Email: info@zalnet.pl

LinkedIn: https://www.linkedin.com/in/beatazalewa/

Blog: https://zalnet.pl/pl/blog/

X: https://x.com/beatazalewa

GitHub - slajdy: https://github.com/beatazalewa/Conferences/

Github – linki:

https://github.com/beatazalewa/Sierpniowe-kolonie-na-chmurze-Azure-2025/