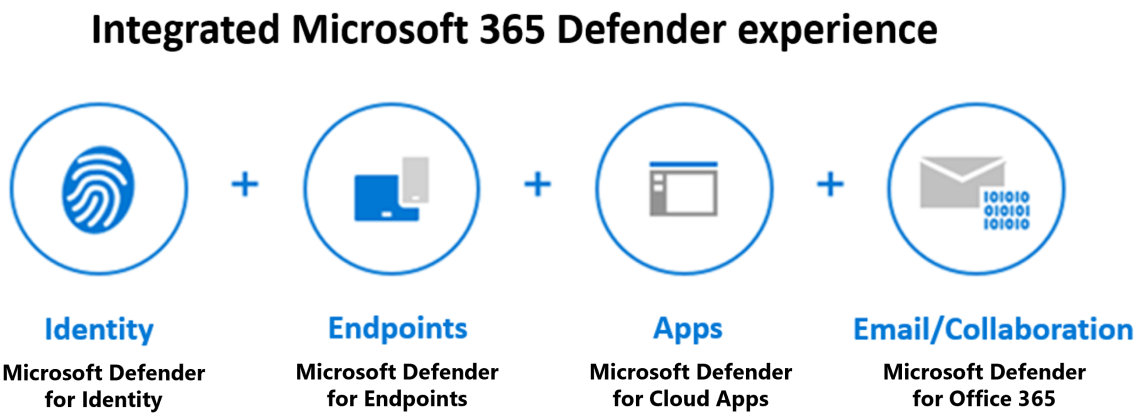
Threat protection with Microsoft 365 Defender



The 365 Defender suite protects:

- Identities with MS Defender or Identity and Aure AD Identity Protection
- Endpoints with MS Defender for Endpoint
- Applications with MS Defender for Cloud Apps
- Email and collaboration with MS Defender for O365

Defender for O365

Plan 1

- Safe attachments: checks email attachments for malicious content
- Safe links: Links scaned for each click. Safe link remains, but malicious are blocked
- Safe Attachments for SharePoint, OneDrive, Teams: Protects org when users collaborate and share files
- Anti-phishing protection: Detects attempts to impersonate users and internal or customer domains
- Real-time detections: Real time report allowing you to identify and analyse recent threats

Plan 2

- Threat trackers: provide latest intelligence on prevailing cyber issues and take countermeasures before there is an actual threat
- Threat explorer: real time report allows identification and analysis of recent threats
- Automated investigation and response (AIR): security playbooks that can be launched automatically when an alert is triggered, or manually
- Attack simulator: allows you to run realistic attack scenarios in your org to identify vulnerabilities. Can also be used to test policies and train employees.
- Hunt threats: query based threat hunting tool where you can export 30 days of raw data
- Investigate alerts and incidents: P2 customers have access to 365 Defender integration to efficiently detect, review, and respond to incidents and alerts.

Microsoft Defender for O365 is included in subscriptions such as M365 E5, O365 E5, O365 A5, and M365 Business Premium.

MS Defender for Endpoint

A platform designed to help enterprise networks protect endpoints. It includes:

- Threat & vuln management: A risk based approach to discovery, prioritisation, and remediation of endpoint vulns and misconfigs.
- Attack surface reduction: provides first line of defence in the stack by ensuring configuration settings are properly set and exploit mitigation techniques are applied.
- Next generation protection: Brings together ML, big data, and in depth threat resistance research.
- EDR - advanced attack detections near real time and actionable. Sec analysts can prioritise alerts, see full scope of breech and respond to remediate threats
- AIR - inspection algorithms and processes used by analysts (like playbooks) to examine alerts and take quick action to resolve breeches.
- MS Threat Experts: managed threat hunting service provides SOCs with monitoring and analysis tools to ensure threats don't get missed
- Management and APIs: provide APIs to integrate with other solutions

Defender for Cloud Apps

MS Defender for Cloud Apps is a Cloud Access Security Broker (CASB) - a cross SaaS solution that operates as an intemediary between a cloud user and the cloud provider.

What is a CASB?

A gatekeeper to broker real-time access between enterprise users and the cloud resources they use regardless of location or device.

- Visibility: Detect cloud services and app use and provide visibility into Shadow IT
- Threat protection: Monitor user activities for naomalous behaviours and control access to resources through acess controls
- Data security: Identify, classify, and control sensitive info
- Compliance: assess the compliance of cloud services

Defender for Cloud Apps framework

- Discover and control the user of Shadow IT: Identify cloud apps, IaaS, and PaaS services used by org and assesss risk levels. 25,000 SaaS apps against over 80 risks
- Protect against cyberthreats and anomalies: Detect unusual behaviour across cloud apps to identify ransomeare, compromised users, or rogue applications
- Protect sensitive info anywhere in cloud
- Assess cloud apps compliance: see if cloud apps meet relevant comp reqs. Prevent leaks to non-comp apps and limit access to regulated data

Defender for Cloud Apps functionality

- Cloud Discovery maps and identifies your cloud environment and the cloud apps your org uses.
- Sanction and un-sanction apps by using cloud apps catalogue (over 25,000)
- App connectors to integrate MS and non-MS cloud apps
- Conditional access App Control Protection provides real-time visibility and control over access and activities.
- Use policies to detect risky behaviour, violations, or suspicious data points

O365 Cloud App Security

A subset of MS Defender for Cloud Apps providing enhanced visibility and control for O365. It includes threat detection based on user logs, discovery of shadow It for apps with similar functionality to O365 offerings.

MS Defender for Identity

A cloud based security solution that uses on-prem AD data (called signals) to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions at the org.

Monitor and profile user behaviour and activities

MS Defender for Identity monitors and analyses user activites and info across your network including permissions and group memberships and creates a behavioural baseline for each user.

Protect user identities and reduce the attack surface

Provides insights on identity configs for suggesting security best practices to reduce attack surface.

For hybrid envs where AD FS is present, Defender for Identity protects it by detecting on-prem attacks and providing visibility into authentication events generated by AD FS.

Identify suspicious activities and advanced attacks across the cyberattack kill-chain

Normally attacks are launched against any accessibly entity (e.g. low privileged user). Attacks move laterally until the attacker can access valuable assets. Defender for Identity identifies these threates through the entire chain:

- Reconnaissance
- Compromised credentials
- Lateral movements
- Domain dominance

Investigate alerts and user activities

Designed to reduce general alert onise by only provider relevant and important ones in a simple attack timeline.

MS365 Defender Portal

MS365 Defender Portal coordinates detection, prevention, invesgitation, and response across endpoints, identities, email, applications all together in one central place designed to meet the needs of security teams.

Different roles see different cards that are more meaningful to their day-to-day jobs:

- Identities - Monitor the identities in your org and keep track of suspicious and risky behaviour
- Data - Track user activity that could lead to unauthorised data disclosure
- Devices - Get up-to-date info on alerts, breach activity and other threats
- Apps - Gain insight into how cloud apps are being used in your org

Incidents and alerts

MS365 services and apps create alerts when they detect a suspicious or malicious event or identity, which are automatically agregated by M365 Defender.

- All alerts related to incident
- All users identified to be a part of or related to incident
- All mailboxes identified to be a part of or related to incident
- All automated investigations triggered by alerts in the incident
- All supported evidence and response

Threat analytics

Analytics dashboard highlights reports that are most relevant to your org. Includes latest threats, high impact threats, and high exposure threats. Selecting specific threat from dashboard provides analytics report with more detailed information.

Secure Score

One of the tools in M365 Defender portal and is a representation of the company's security posture