Microsoft Security

Microsoft Defender for Cloud Apps

Threat Protection

Protection against cyberthreats—with insights from trillions of signals and state of the art data correlation

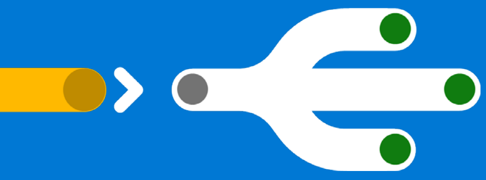
Threats are becoming ever more complex and persistent, traversing email and messaging apps to applications, identities, and infrastructure. To understand and contain an attack, defenders need intelligent, automated, integrated security to close gaps in detection and response and give them back time to get more proactive.

The challenge of securing your environment

Bad actors are using increasingly creative and sophisticated attacks

The digital estate offers a very broad surface area that is difficult to secure

Intelligent correlation of signals is difficult, time-consuming, and expensive



Why Microsoft?

Integrating Microsoft Defender for Cloud Apps with your endpoint security systems, or with your SIEM, gives you the ability to use cloud discovery beyond your organization’s network or secure web gateways. With the combined user and device information, you can identify risky users or devices, manage application usage, and investigate further endpoint activities as it relates to cloud usage.

Key threats in the cloud

Insider threats

Detect and protect against internal users with malicious intent

Compromised accounts

Combat advanced attackers that leverage compromised user credentials

Malware

Detect malware in existing cloud storage and block new malware from being uploaded

Data exfiltration

Detect unusual flows of data to cloud sources outside of your organization

Privileged users

Detect abnormal behavior of privileged user accounts to limit the damage

OAuth app permissions

Identify risky OAuth apps with high permissions levels and revoke access tokens

Comprehensive Threat Protection for your cloud apps

Built-in Threat Protection policies

More than 20 out-of-the-box policies that alert you on some of the most common cloud threats such as impossible travel, impersonation activities or ransomware detection

Malware Detonation

Intelligent heuristics identify potentially malicious files and detonate them in a sandbox environment—for existing and newly uploaded files

Customize policies to alert and remediate

Customize what you want to be alerted on to minimize noise and configure automatic remediation

Prioritized investigation of alerts

Overview of the users who likely pose the greatest risk to the organization and are recommended for immediate review, with a unified view of identity threats across on-premises and cloud

Get behavioral analytics and anomaly detection

The anomaly detection policies of Microsoft Defender for Cloud Apps provide out-of-the-box user and entity behavioral analytics (UEBA) and machine learning (ML), so you are ready from the outset to run advanced threat detection across your cloud environment. Because they're automatically enabled, the new anomaly detection policies immediately start the process of detecting and collating results, targeting numerous behavioral anomalies across your users and devices connected to your network. Additionally, the policies expose more data from the Defender for Cloud Apps detection engine, to help you speed up the investigation process and contain ongoing threats.

Anomalies are detected by scanning user activity. The risk is evaluated by looking at over 30 different risk indicators, grouped into risk factors, as follows:

Risky IP address	Login failures	Admin activity	Inactive accounts	Location	Impossible travel	Device and user agent	Activity rate

Develop and deploy your security plan with Microsoft Defender for Cloud Apps today

Microsoft Defender for Cloud Apps

Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that gives you visibility into your cloud apps and services, provides sophisticated analytics to identify and combat cyberthreats and enables you to protect your data and control how it travels.

aka.ms/defender-for-cloud-apps

Microsoft Defender for Cloud

Strengthen your cloud security posture and compliance state. Monitor and help protect workloads across your multi-cloud and hybrid environments.

aka.ms/defender-for-cloud

Microsoft Sentinel

Standing watch, by your side. Intelligent security analytics for your entire organization. See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise.

aka.ms/MicrosoftSentinel

Microsoft Defender for Endpoint Plan 2

Defender for Endpoint Plan 2 is a unified endpoint security platform for protection, detection, investigation and response. Defender for Endpoint protects endpoints from cyber-threats; detects advanced attacks and data breaches, automates security incidents and improves security posture.

aka.ms/MDEp2OpenTrial

This material is provided for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESSED OR IMPLIED.