Microsoft Security

Protect your SaaS apps with Microsoft Defender for Cloud Apps

Securing SaaS apps is more challenging than ever in the era of AI and complex modern attacks. Your SaaS security approach must evolve.

80% Enterprises will be using Generative AI apps or deploy Generative AI-enabled apps by 2026.[1]

#1 Cloud misconfigurations are a top risk in security professionals' environments.[2]

130 Average number of apps used in an organization in 2022, up 18% from 2021.[3]

Microsoft Defender for Cloud Apps

SaaS security combines fundamental app protection with modern ways to secure apps. Microsoft Defender for Cloud Apps offers **a holistic approach to SaaS security** across prevention and protection throughout the app usage lifecycle. Microsoft's unique approach empowers security teams to effectively **secure AI apps** with advanced prevention and protection capabilities against AI-related threats.

SaaS app discovery & posture management

SaaS threat protection

App to app protection

Security for AI apps

Information Protection

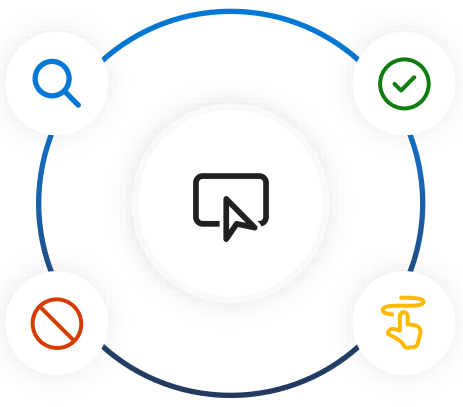
Sanctioned apps

okta, zendesk, ATLASSIAN, servicenow, salesforce, DocuSign, Google Workspace, aws, slack, EGNYTE, miro, workday, GitHub, nd, box, webex, asana, Dropbox, onelogin, smartsheet, ...and more

SaaS app discovery & posture management

Defender for Cloud Apps gives you full picture of risks associated with SaaS app usage and resources within your environment. You can gain control of what's being used and when to help you manage shadow IT by providing easy ways to **identify, assess, and manage** application access.

SaaS app posture management surfaces misconfigurations and provides recommendations to strengthen app posture directly in Microsoft Secure Score. We provide coverage for the most critical apps such as Microsoft 365, Salesforce, ServiceNow, Okta, GitHub, and more.

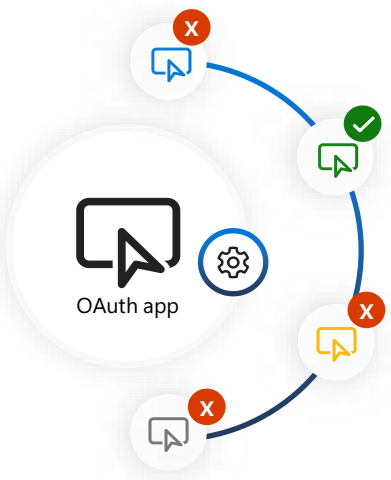


SaaS threat protection

Sophisticated attacks often cross modalities. Defender for Cloud Apps is part of **Microsoft's unified security operations** platform which correlates signals from Microsoft Defender XDR and 3rd party via Microsoft Sentinel (SIEM) to provide incident-level detection, investigation, and powerful response capabilities like automatic attack disruption.

App-to-app protection

Defender for Cloud Apps provides OAuth app protection by providing security and policy management capabilities. Identified by Microsoft Entra ID, organizations can gain visibility into unused apps, credentials, and expired credentials to govern apps being used and upkeep app hygiene.



Security for AI apps

Defender for Cloud Apps allows you to discover **over 400 GenAI** apps, understand the risks with the ready-to-use risk assessments evaluating over **40 risk factors**, and set controls accordingly to mitigate the risks.

It helps you detect and remediates threats from suspicious interactions with Copilot for Microsoft 365, such as accessing sensitive files via Copilot from comprised user accounts or risky IPs.

Information protection

Defender for Cloud Apps integrates with Microsoft Purview to provide intelligent detection and control of sensitive information across their SaaS apps. Any data loss prevention (DLP) alerts are automatically correlated within the XDR experience for easy prioritization of incidents that include sensitive data.

Get started with Microsoft Defender for Cloud Apps

Learn how to protect your organization's apps across the SaaS app management lifecycle through a set of simple steps and best practices:

- Explore Microsoft Defender for Cloud Apps
- Visit our Tech Community blog
- Check out our best practices guide

1. Gartner® Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026
2. Top 7 SaaS Security Risks (and How to Fix Them), 2022
3. 2023 State of SaaSOps study, BetterCloud