Microsoft Security

Protect your SaaS apps with Microsoft Defender for Cloud Apps

SaaS App landscape

Microsoft's investment in a new approach to software as a service (SaaS) app protection is powered by security professionals' need for extra protection within cloud apps beyond the traditional scope of security.

59% 59% of security professionals find the SaaS sprawl challenging to manage

#1 Cloud misconfigurations are a top risk in security professionals' environments

55% 55% of IT and security professionals report that the top challenge in their SaaS environments is a lack of visibility into user activity and data, like OAuth data permissions

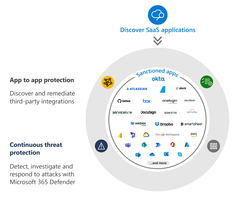
What is SaaS Security?

With an uptick in app usage and the breadth of applications being used combined with employees accessing company resources outside of corporate perimeters, better protection is needed. In addition, there have been new, and sophisticated, attack vectors on OAuth apps that require security teams to need visibility of the level of permissions and the type of data that these apps can access.

SaaS security combines fundamental app protection with modern ways to secure apps. Microsoft Defender for Cloud Apps offers **a holistic SaaS security approach** that delivers capabilities to address these new attack vectors across prevention and protection throughout the app usage lifecycle. Microsoft's unique approach helps security professionals easily start with SaaS security protection no matter where they are in their app protection journey.

Comprehensive SaaS Security

These new sets of capabilities, combined with fundamental app protection, encompass the Microsoft approach to holistic SaaS security and will help organizations modernize their strategy to effectively protect against app-based threats.



Discover SaaS applications

Defender for Cloud Apps shows the full picture of risks to your environment from SaaS app usage and resources, and gives you control of what's being used and when. Usage in SaaS apps has increased productivity as well as the opportunity for Shadow IT to exist in your organization.

With Microsoft's SaaS security protection, you gain control of shadow IT by providing easy ways to identify, assess, and manage application access.

- **Identify** - Using data based on an assessment of network traffic and an app catalog of more than 31,000 public cloud apps, Defender for Cloud Apps identifies apps accessed by users across your organization and provides details on which apps are really being used both on and off your corporate network.
- **Assess** - Evaluate those apps for more than 90 risk indicators allowing you to sort through the discovered apps and assess your orgs security and compliance posture.
- **Manage** - Set policies that monitor apps around the clock. If anomalous behavior happens, like unusual spikes in usage, you auto-alerted and guided to action.

SaaS Security Posture Management (SSPM)

SSPM surfaces misconfigurations and provides recommendations to strengthen app posture directly in Microsoft Secure Score. This allows organizations to secure the posture of their entire digital estate across apps, endpoints, resources, etc. We provide coverage for the most critical apps such as Microsoft 365, Salesforce, ServiceNow, Okta, GitHub, and more.

- **Seamless integration with the Defender for Cloud Apps connector experience:** If you have already connected any of these apps to Defender for Cloud, the new SSPM capabilities automatically light up without any additional deployment.
- **Alignment to best practices and benchmarks:** We recommend actions based on industry standards like the Center for Internet Security and follow best practices set by the specific app provider (for example, Salesforce Security Health Check).

Information protection

Defender for Cloud Apps integration with Microsoft Purview enables security teams to leverage over 300 out-of-the-box data classification types in their information protection policies. Microsoft provides an expansive suite of data loss protection capabilities to ensure your data is protected no matter where it is being accessed.

Defender for Cloud Apps connects to SaaS apps to scan for files containing sensitive data uncovering which data is stored where and who is accessing it. To protect this data, organizations can implement controls such as:

- Apply a sensitivity label
- Block downloads to an unmanaged device
- Remove external collaborators on confidential files

App-to-app Protection

Attacks involving OAuth applications have been on the rise. This open attack vector wasn't addressed with traditional app protection methods as organizations didn't realize the damage a compromised OAuth app could do. Protecting how apps interact with each other and having visibility into dormant apps is critical to comprehensive SaaS Security.

App Governance within Defender for Cloud Apps fills the need for OAuth app protection by providing security and policy management capabilities. Identified by Microsoft Azure Directory, organizations can gain visibility into unused apps, credentials, and expired credentials to govern apps being used and upkeep app hygiene.

Defense and signal integration with Microsoft XDR

Sophisticated attacks often cross modalities and, in the past, solutions addressed alerting security operations center teams by identifying anomalies like mass download activity, leaving these teams without enough context to prioritize threat anomaly investigations.

- **Integrating Microsoft 365 Defender:** The XDR technology correlates signals from the Microsoft Defender suite across endpoints, identities, email, and SaaS apps to provide incident-level detection, investigation, and powerful response capabilities like automatic attack disruption.
- **Full kill chain visibility:** Improves operational efficiency with better prioritization and shorter response times to ultimately protect the organization more effectively.

It is critical that you protect data and assets by implementing SaaS security principles in your security strategy while empowering users to stay productive.

Microsoft's unique approach helps security professionals easily start no matter where they are in their app protection journey. 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