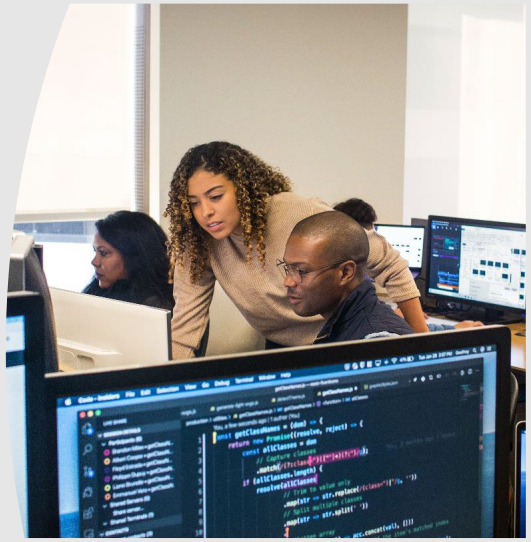
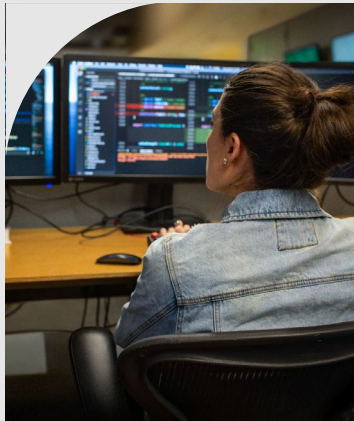
Microsoft Security

Top SaaS app use cases

Microsoft Defender for Cloud Apps





Contents

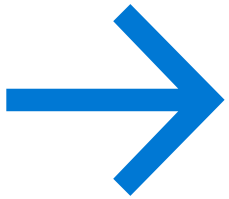
Introduction

Moving to the cloud requires a new approach to security. As you enable employees to work from virtually anywhere and from any device of their choice, your organizational access perimeters and boundaries change. Your new security controls need to adapt to this dynamic environment and be able to quickly respond to the constantly evolving threat landscape.

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. SaaS security combines fundamental app protection (discovery, information protection, anomaly detection) 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.

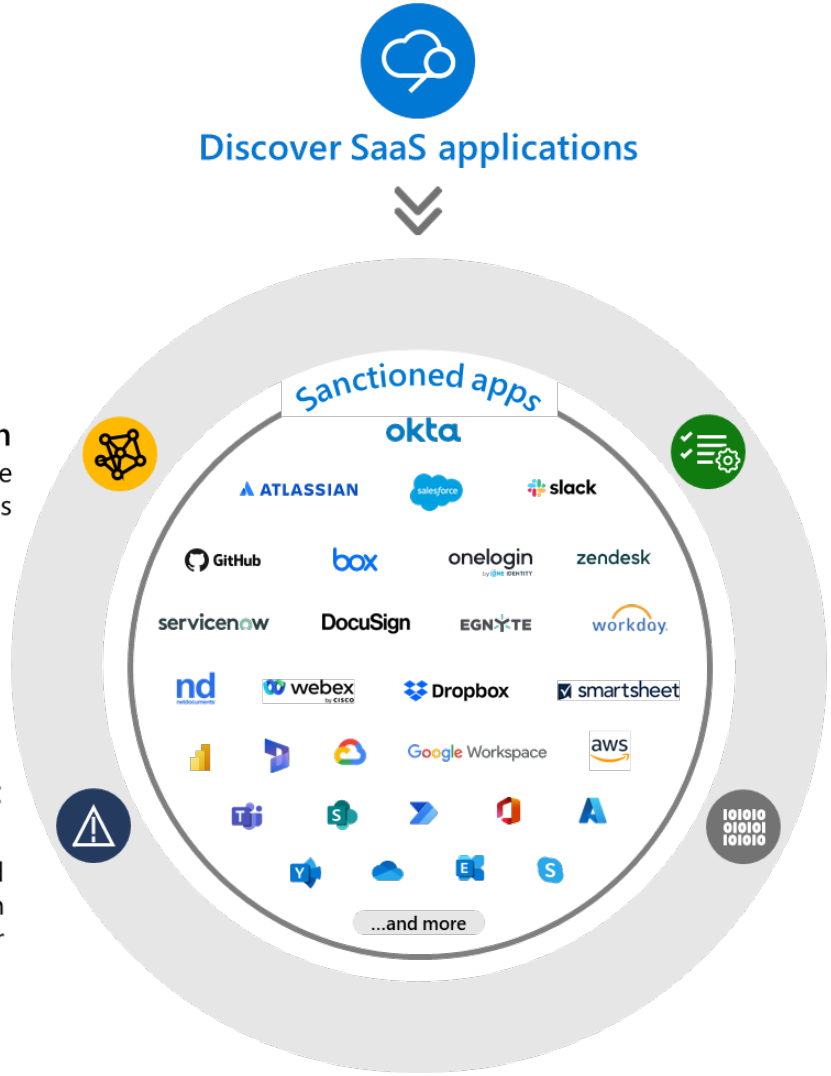
In this guide we share the top use cases for SaaS Security that we recommend as a baseline for a successful implementation to improve your cloud security.

The use cases can be leveraged as a starting point during a proof of concept, or as you're getting ready to deploy your SaaS Security solution solution and want to prioritize your deployment.



A comprehensive SaaS Security solution

Defender for Cloud Apps is a multimode SaaS Security solution. Get full visibility of your SaaS app landscape and take control of your apps with Microsoft Defender for Cloud Apps which combines SaaS security posture management, data loss prevention, app to app protection and integrated threat protection to ensure holistic coverage for your apps.



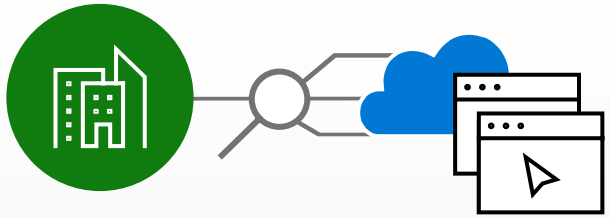
App to app protection
Discover and remediate third-party integrations

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

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

Information protection:
Sensitive data exposure
Governance file violation

Discover SaaS applications



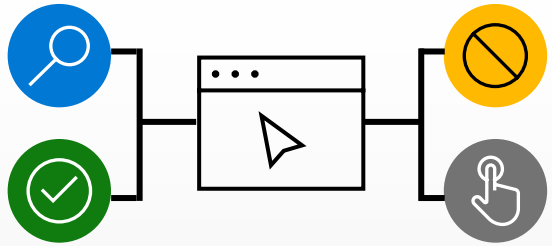
1. Shadow IT Discovery

Discover SaaS applications that are in use in your environment across our cloud app catalog containing more than 30,000 applications.

Requirements

Defender for Endpoint, Log Collector, Zscaler, iBoss, API Upload

Learn more about discovery and assessment



2. Shadow IT Assessment

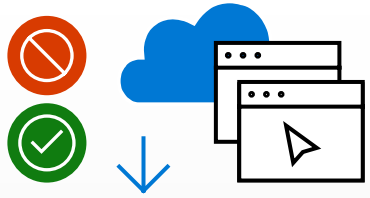
Categorize discovered SaaS apps and apply tags (Monitor, Sanctioned, Unsanctioned, or create your own).

Requirements

Defender for Endpoint, Log Collector, Zscaler, iBoss, API Upload

Learn more about discovered app filters and queries

Discover SaaS applications



3. Shadow IT enforcement

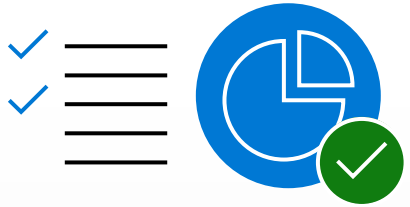
Govern discovered SaaS apps and block them manually or via discovery policies.

Requirements

Defender for Endpoint, ZScaler, iBoss, automate unsanctioned URLs by using API to retrieve the list of unsanctioned URLs

Learn more about discovered app governance

SaaS security posture management



4. SaaS security posture management

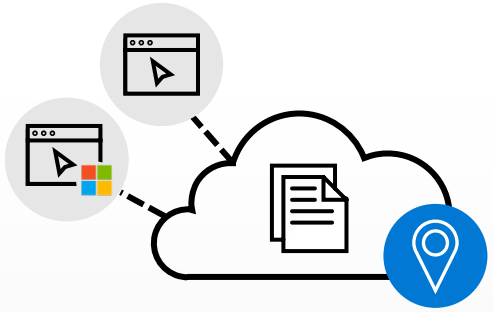
View misconfigurations in connected SaaS applications and get details from Microsoft Secure Score on how to proactively prevent the misconfigurations with links to vendor documentation.

Requirements

App connectors

Learn more about security posture management for SaaS apps

Information protection



5. Discover sensitive files at rest

View sensitive files that exist at rest in Microsoft and connected non-Microsoft SaaS apps.

Requirements

App connectors

Learn more about DCS inspection

Learn more about Microsoft Purview integration

6. Protect data at rest

Apply policies to non-Microsoft apps to revoke files shared with too broad of an audience or alert when these files are detected or apply labels. Labels can also be applied to files in non-Microsoft applications along with some edge cases not covered in Purview.

Requirements

App connectors

Learn more about DLP

Information protection

7. Protect data in motion

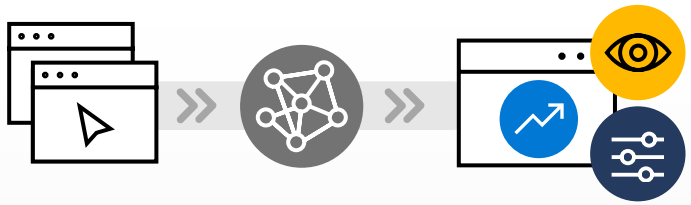
Apply policies to data moving between boundaries within a browser session using inline proxy. This provides the ability to block upload/download/copy/paste/apply label on unmanaged devices.

Requirements

Conditional Access app control, Azure Active Directory or third-party identity provider

Learn more about Conditional Access app control

Continuous threat protection



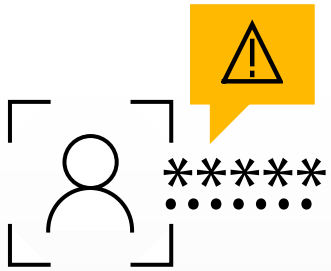
8. Record an audit trail

Capture an audit trail with correlated data across all your connected SaaS apps and apps flowing through inline controls which are aggregated into a single location with a common schema and enriched with signals from Microsoft Threat Intelligence.

Requirements

App connectors

Learn more about using the audit trail



9. Identify compromised accounts

Monitor user behaviors with machine learning capabilities and trigger alerts when suspicious activities happen, impossible travel, or define your own policies and automate resolutions with PowerAutomate. App Governance can perform similar activities for service principals and OAuth apps.

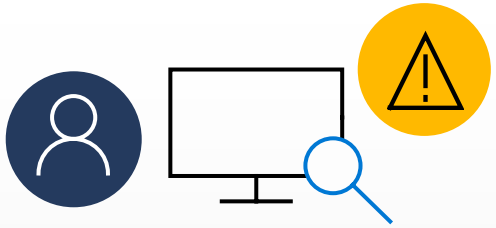
Requirements

App connectors, App Governance

Learn more about impossible travel detections

Learn more about threat protection policies

Continuous threat protection



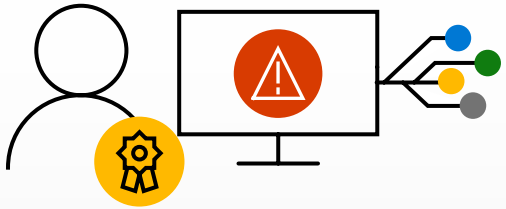
10. Detect threats from users inside your organization

Detect anomalous behavior from individual users such as mass download or repeated activities and automatically take action to suspend accounts.

Requirements

App connectors

Learn more about activity policies



11. Detect threats from privileged accounts

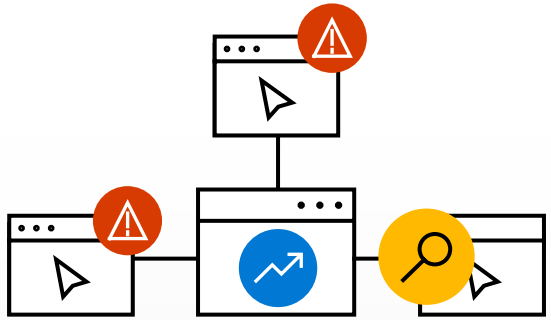
Detect anomalous behavior from individual users such as mass impersonation by a single user, login from new country with an admin account, or unusual activity from an MSSP admin.

Requirements

App connectors

Learn more about threat protection policies

Continuous threat protection



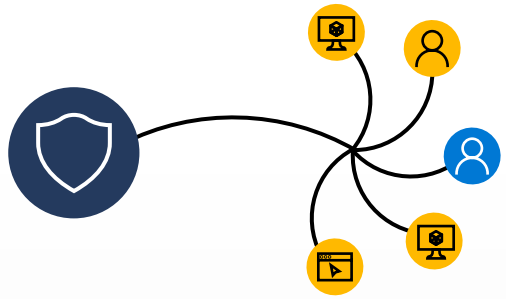
12. Hunt for threats across Microsoft 365 Defender

Use powerful KQL queries to hunt for audited activity in a common schema across all your connected SaaS applications along with the rest of the signals that are coming from other Microsoft 365 Defender products.

Requirements

Microsoft 365 Defender Advanced Hunting

Learn more about Microsoft 365 Defender integration



13. View and triage incidents in Microsoft 365 Defender

Admins can view and triage multi-stage incidents that have been correlated across all of Microsoft 365 Defender and Azure Active Directory Identity Protection.

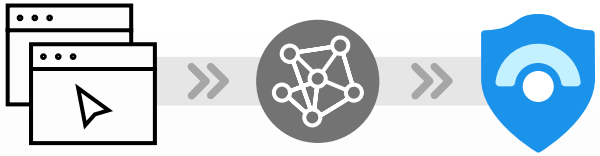
Requirements

Microsoft 365 Defender Incidents

Learn more about investigation and response in Microsoft 365 Defender

Learn more about incident response with Microsoft 365 Defender

Continuous threat protection



14. Send data to Microsoft Sentinel natively

Send enriched data from CloudAppEvents table to Sentinel for long term storage and hunting.

Requirements

App connectors, Microsoft 365 Defender Connector for Sentinel

Learn more about integration with Microsoft Sentinel

15. Send data to non-Microsoft SIEM solutions

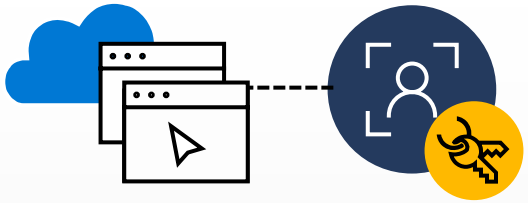
Send enriched data from CloudAppEvents table to EventHub or AzureStorage and consume downstream.

Requirements

App connectors, Microsoft 365 Defender Streaming API, EventHub, Azure Storage

Learn more about streaming advanced hunting data

App to app protection using App Governance



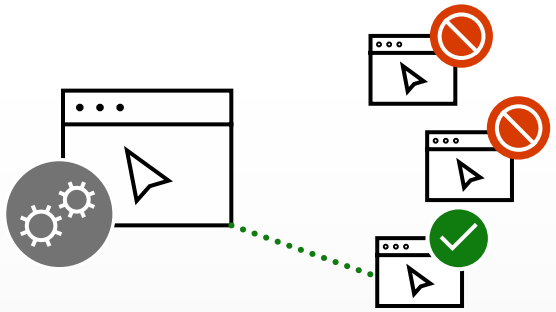
16. OAuth app consent discovery

Discover SaaS applications that have been consented to in your organization for first and third-party apps using app connectors. See app risk permission levels and which users have authorized the app.

Requirements

App connectors

Learn more about Security posture management for SaaS apps »



17. OAuth app registration discovery

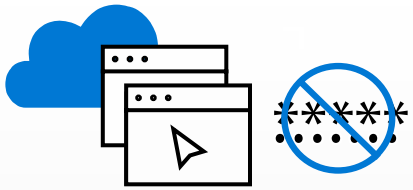
Discover SaaS applications that have been granted permissions in Microsoft Graph API. Also view apps that are overprivileged, apps accessing sensitive data, and volume of data being uploaded as well as anomaly detections powered by Microsoft threat intelligence.

Requirements

App Governance

Learn more about viewing your OAuth apps »

App to app protection using App Governance



18. OAuth app enforcement

Automatically revoke apps identified in OAuth policies and App Governance policies.

Requirements

App connectors, App Governance

Learn more about managing OAuth apps »

Learn more about getting started with app policies »

Resources

- **Visit our website:**
  Microsoft Defender for Cloud Apps | Microsoft Security
- **Check out our recent blog posts on Tech Community:**
  aka.ms/DefenderforCloudAppsBlogs
- **Access our documentation:**
  aka.ms/DefenderforCloudAppsdocs
- **Training:**

  Ninja show, part 1: Microsoft Defender for Cloud Apps Overview

  Ninja show, part 2: Microsoft Defender for Cloud Apps deep dive

  Ninja training short link
- **Quick overview:**
  aka.ms/DefenderforCloudAppsOverview
- **Want to know more about the App Governance capability?**

  aka.ms/AppGovernanceDocs

  aka.ms/AppGovernancePreview
- **Customer stories:**
  Global energy leader safeguards its digital transformation with automated App Governance