Appendix A: App connectors available in Microsoft Cloud App Security (MCAS) as of 25 May 2020

- Amazon Web Services
- Azure
- Box
- Cisco Webex
- Dropbox
- G Suites
- Google Cloud Platform
- Office 365
- Okta
- Salesforce
- ServiceNow
- Workday

Appendix B: Log collectors available In Microsoft Cloud App Security (MCAS) as of 25 May 2020

- Blue Coat
- Blue Coat ProxySG - Access log (W3C)
- Barracuda
- Barracuda - Web App Firewall (W3C)
- Barracuda - F-Series Firewall
- Barracuda - F-Series Firewall Web Log Streaming
- Check Point
- Check Point (CSV)
- Check Point - SmartView Tracker
- Check Point (XML)
- Check Point Syslog
- Cisco
- Cisco ASA Firewall
- Cisco FWSM
- Cisco IronPort WSA
- Cisco Cloud Web Security
- Meraki - URLs log
- Cisco ASA FirePOWER
- Cisco IronPort WSA II
- Cisco IronPort WSA III
- Cisco FirePower 64
- Clavister
- Clavister NGFW (Syslog)
- ContentKeeper
- ContentKeeper Secure Internet Gateway
- Corrata
- Corrata
- Dell SonicWALL

- SonicWALL
- Digital Arts
- Digital Arts i-FILTER
- Forcepoint
- Forcepoint Web Security Cloud
- Forcepoint LEEF
- Fortinet
- Fortinet FortiGate
- FortiOS
- Iboss
- Iboss Secure Cloud Gateway
- Juniper
- Juniper SRX
- Juniper SRX SD
- Juniper SRX Welf
- Juniper SSG
- McAfee
- McAfee Web Gateway
- Microsoft
- Microsoft Forefront Threat Management Gateway (W3C)
- Palo Alto
- PA Series Firewall
- PA Series Firewall LEEF
- Sophos
- Sophos SG
- Sophos Cyberoam Web Filter and Firewall log
- Sophos XG
- Squid
- Squid (Common)
- Squid (Native)
- Stormshield Network Security
- Stormshield Network Security
- Websense
- Web Security solutions - Internet Activity log (CEF)
- Web Security solutions - Investigative detail report (CSV)
- Zscaler
- Zscaler - Default CSV
- Zscaler - QRadar LEEF
- Zscaler - CEF
- Generic
- Generic CEF log
- Generic LEEF log
- Generic W3C log
- Other
- Custom log format
- Other (manual only)

Appendix C: Default rules available In Microsoft Cloud App Security as of 25 May 2020

- File shared with unauthorized domain
  Alert when a file is shared with an unauthorized domain (such as your competitor).

- Mass download by a single user
  Alert when a single user performs more than 50 downloads within 1 minute.

- Multiple failed user log on attempts to an app
  Alert when a single user attempts to log on to a single app, and fails more than 10 times within 5 minutes.

- New popular app
  Alert when new apps are discovered that are used by more than 500 users.

- New high volume app
  Alert when new apps are discovered that have total daily traffic of more than 500 MB.

- New high upload volume app
  Alert when new apps are discovered whose total daily upload traffic is more than 500 MB.

- New risky app
  Alert when new apps are discovered with risk score lower than 6 and that are used by more than 50 users with a total daily use of more than 50 MB.

- Collaboration app compliance check
  Alert when new collaboration apps are discovered that are not compliant with SOC2 and SSAE 16, and are used by more than 50 users with a total daily use of more than 50 MB.

- Cloud storage app compliance check
  Alert when new cloud storage apps are discovered that are not compliant with SOC2, SSAE 16, ISAE 3402 and PCI DSS, and are used by more than 50 users with total daily use of more than 50 MB.

- CRM app compliance check
  Alert when new CRM apps are discovered that are not compliant with SOC2, SSAE 16, ISAE 3402, ISO 27001 and HIPAA, and are used by more than 50 users with a total daily use of more than 50 MB.

- Anomalous behavior in discovered users
  Alert when anomalous behavior is detected in discovered users and apps, such as: large amounts of uploaded data compared to other users, large user transactions compared to the user's history.

- Logon from a risky IP address
  Alert when a user logs on to your sanctioned apps from a risky IP address. By default, the Risky IP address category contains addresses that have IP address tags of Anonymous proxy, TOR or Botnet. You can add more IP addresses to this category in the IP address ranges settings page.

- Administrative activity from a non-corporate IP address
  Alert when an admin user performs an administrative activity from an IP address that is not included in the corporate IP address range category. You must first configure your corporate IP addresses by going to the Settings page, and selecting IP address ranges.

- Potential ransomware activity
  Alert when a user uploads files to the cloud that might be infected with ransomware.

- Externally shared source code
  Alert when a file containing source code is shared outside your organization.

- File containing PII detected in the cloud (built-in DLP engine)
  Alert when a file containing personally identifiable information (PII) is detected by our built-in data loss prevention (DLP) engine in a sanctioned cloud app.

- File containing PHI detected in the cloud (built-in DLP engine)
  Alert when a file containing protected health information (PHI) is detected by our built-in data loss prevention (DLP) engine in a sanctioned cloud app.

- File containing PCI detected in the cloud (built-in DLP engine)
  Alert when a file containing payment card information (PCI) is detected by our built-in data loss prevention (DLP) engine in a sanctioned cloud app.

- New cloud storage app
  Alert when new cloud storage apps are discovered that are used by more than 50 users with total daily use of more than 50 MB.

- New collaboration app
  Alert when new collaboration apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB.

- New online meeting app
  Alert when new online meeting apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB.

- New CRM app
  Alert when new discovered CRM apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB.

- New Human-Resource Management app
  Alert when newly discovered Human-Resource Management apps are used by more than 50 users with a total daily use of more than 50 MB.

- New sales app
  Alert when new sales apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB.

- New code hosting app
  Alert when new code hosting apps are discovered that are used by more than 50 users with total daily use of more than 50 MB.

- New vendor management system apps

Alert when new vendor management system apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB.

- Anomalous behavior of discovered IP addresses
  Alerts when anomalous behavior is detected in discovered IP addresses and apps, such as: large amounts of uploaded data compared to other IP addresses, large app transactions compared to the IP address's history.

- Block upload based on real-time content inspection
  Cloud App Security will evaluate the content of files being uploaded and will block any violations in real-time.

- Block download based on real-time content inspection
  Cloud App Security will evaluate the content of files being downloaded and will block any violations in real-time.

- Block cut/copy and paste based on real-time content inspection
  Cloud App Security will evaluate the content of items that are cut/copied from and/or pasted to a browser and will block any violations in real-time.

- Access level change (Teams)
  This policy is triggered when a team's access level is changed from private to public.

- File shared with personal email addresses
  Alert when a file is shared with a user's personal email address.

- Shared digital certificates (file extensions)
  Alert when a file containing digital certificates is publicly shared.

- Log on from an outdated browser
  Alert when a user logs on from an outdated browser, and notify the user.

- Stale externally shared files
  Alert when an externally shared file that haven't been modified for at least 6 months is detected.

- Monitor all activities
  Cloud App Security will monitor all available activities.

- Activities from suspicious user agents
  Alert when there is an activity from a suspicious user agent that might indicate using an attacking tool.

- External user added (Teams)
  This policy is triggered when an external user is added to a team.

- Mass deletion (Teams)
  This policy is triggered when a user deletes a large number of teams.