

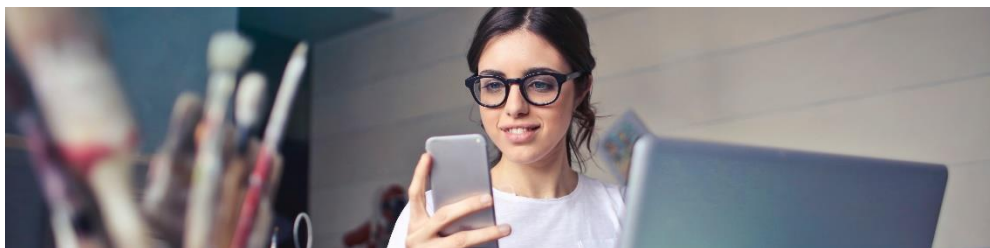


MCAS | Microsoft Cloud App Security

Extend security to cloud applications outside your firm.

Find firm data in G-Suite, Box, Dropbox, and more

MCAS gives you visibility into the cloud applications accessing your firm's data. Using sophisticated analytics to combat cyberthreats, it gives you control over where your firm's data travels.



- Discovery beyond the firm network
- Ease of deployment
- Machine-based discovery
- Seamless integration with Conditional Access, Intune, Azure AD, and Secure Gateway



Shadow IT Discovery

Identify and manage cloud apps used by your firm—in and beyond your network.



Information Protection

Track and protect sensitive information when it travels outside your firm with automated processes and real-time controls.



Threat Protection

Detect unusual behavior across cloud apps to identify ransomware, compromised users, and rogue apps. Analyze high-risk usage and apply immediate remediation.



Compliance Assessment

Assess the compliance of your firm's applications against regulatory requirements such as GDPR, legal controls, and governmental security standards.

Better together: Microsoft Cloud App Security and Azure Information Protection

MCAS extends AIP's scanning, automated labelling, and protective capabilities to cloud applications outside of Office 365. Remove collaborators to prevent excessive privilege and data leakage, place files into quarantine for additional review, and create policies to proactively apply labels to sensitive files or in risky scenarios.

Email hello@kraftkennedy.com to get started with MCAS.