ADALLOM

Solutions Brief:

Adallom for Microsoft Office 365

Office

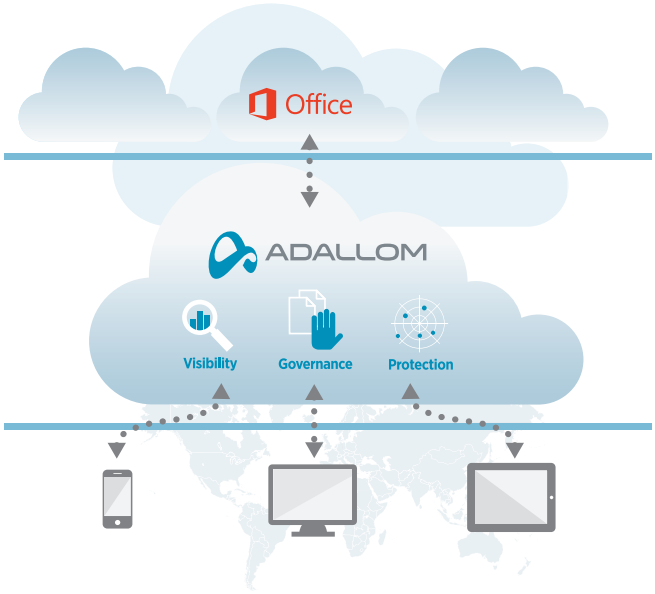
Microsoft Office 365 is a subscription-based suite of business productivity applications including email, social networking and collaboration, content management and cloud storage. This suite of applications in the cloud allows organizations to be productive, efficient and support "anywhere any device" access, without the headache of updating and maintaining an application server infrastructure. However, while Microsoft invests in security, under the shared responsibility model, organizations must take a proactive approach to securing their data in the cloud. Adallom for Microsoft Office 365 mitigates the risks associated with Office 365 adoption by securing data, governing appropriate usage and protecting users in real-time.

Microsoft invests enormously in making their cloud offering "enterprise-grade" and embeds information rights management, eDiscovery and Data Leakage Protection (DLP) features in the Office 365 suite of products. However, the ability to address compliance checkbox requirements isn't enough. Under the shared responsibility model, organizations are responsible for access to and usage of their Office 365 data, and must take a proactive approach to securing their application.

Adallom delivers visibility, governance and protection for the top SaaS applications used by businesses worldwide. In particular, Adallom complements Office 365 features with file and sharing management, and protection against anomalies and threats. In addition, while DLP and eDiscovery are supported on Office 365, Adallom allows organizations to extend their policies from existing on-premise solutions, and enable them consistently across all supported SaaS applications.

Introducing Adallom For Microsoft Office 365

Adallom is a cloud application security platform deployed to protect cloud applications approved for business use, such as Microsoft Office 365. It can be deployed as a 100% SaaS deployment, featuring flexible modes ranging from API to SmartProxy™, or as a private cloud.



Adallom for Microsoft Office 365 secures your sensitive corporate data, governs appropriate usage and detects high-risk behaviors and threats

Our unique cloud application security platform allows IT organizations to :

- Mitigate risks by reducing the attack surface and identifying high-risk usage, anomalous behaviors and security incidents
- Govern appropriate access to and usage of the Microsoft Office 365 suite of applications
- Manage file sharing, and enable sharing-aware cloud drive DLP across Office 365 and all other SaaS applications

The API deployment mode integrates directly into the framework of enterprise cloud applications in as little as 8 minutes. When deployed in proxy configuration, the patent-pending SmartProxy™ architecture seamlessly directs users through the Adallom cloud, providing complete control over the application without breaking application functions.

Specifically for Microsoft Office 365 deployments, you can select the ideal deployment mode for your organization or hybrid deployment modes are available for optimal governance and security:

Deployment modes	Adallom feature highlights per deployment mode
API	Visibility into file sharing Audit trail for file creation and modification Sharing-aware DLP File-sharing reporting User management reporting
SAML Proxy	Granular visibility into logins Access control for device, location and user Custom activity alerting Security and threat protection
SmartProxy	Granular visibility into activities for both Web and Outlook In-line policy enforcement

Features include the following:

Visibility and Audit Trails

Adallom provides a clear and actionable audit trail of all user activities in Office 365 including a dashboard featuring geographical and device access, files, and internal and external collaborators. Complete attestation of all Office 365 activities are available, for compliance reasons or for forensics analysis.

File and Sharing Management

Adallom provides unique file sharing trends, helping organizations understand which users are sharing the most files, what types of files are being shared, and with which domains. Organizations can create policies to manage employees who are sharing too many files publicly, or monitor and prevent files from being shared with specific organizations or competitors. Specific custom policies can also be created, for example, monitoring files that are being shared by the CEO or specific individuals in the organizations.

Cloud Drive DLP

Using Adallom, organizations may centralize DLP policies across all SaaS applications, or extend existing DLP solutions to Office 365. Both traditional and sharing-aware DLP is supported. With traditional DLP, personal healthcare information (PHI), personal credit card information (PCI), personal identifiable information (PII) or intellectual property is identified with DLP mechanisms, and via metadata analysis of file names and extensions. Sharing-aware DLP enables DLP policy creation based on the content and sharing context of files – internal, external, public.

Access Visibility and Threat Detection

Adallom enables organizations to monitor access and usage of Office 365. Visibility is available via a simple activity log or integrated reports that are available out-of-the-box. Custom alerts and reports can also be created to monitor specific use cases of interest, across all SaaS applications. For example, in proxy mode, organizations can monitor access and usage by users such as IT administrators, or monitor the types of files the legal staff is accessing. Appropriate governance polices can be created, for example geographical restriction of Office 365 access from Ukraine.

Combined with Adallom SmartEngine™ advanced heuristics technology, anomalies in the usage of Office 365 can be detected. The Adallom SmartEngine learns how each user interacts with each SaaS application using more than 75 variables, and through behavioral analysis,

assesses the risks in each transaction. This feature is enabled "out-of-the-box" without requiring complex rules and configuration. More than thirty out-of-the-box alerts are available, including alerts on high-rates of download activities, simultaneous logins from multiple locations, or users accessing from blacklisted IPs.

Proactive SaaS Security Research and Forensics

Adallom cloud services include proactive research on threats and alerts by Adallom Labs, staffed by a team of cybersecurity researchers. Adallom Labs identified MS13-104, a token hijack compromise in Sharepoint and OneDrive that exploited a vulnerability in Microsoft Office 365 and collaborated with Microsoft on it. Adallom Labs is the only SaaS security vendor invited to the Microsoft Active Protections Program (MAPP). In addition, a regular SaaS Security Assessment Report that summarizes top Office 365 security risks and mitigations is available as part of the Adallom cloud services.

Feature Comparison With Office 365

	Office 365 features:	Adallom complements with the following:
Visibility and Audit Trails	• Mailbox access audit trail • Impersonated admin audit trail • Basic reports (mailbox connections, message delivery)	• Comprehensive audit trails and attestation for user, data, access, activities • File visibility and sharing trends to monitor sensitive files • User visibility and monitoring for internal and external collaborators • Privileged user and activity monitoring, for example, CEO and CFO of an organization or IT administrators • Visibility dashboard and reports
Governance and Compliance	• DLP for Exchange • DLP for SharePoint • DLP for OneDrive • Encryption for emails • eDiscovery for Exchange • eDiscovery for SharePoint	• File sharing management • Cloud Drive DLP - traditional and sharing-aware DLP • Governance on user activities within Office 365 • Governance on access - which users, locations and devices are allowed access • Compliance reports
Threat Protection	Cloud provider infrastructure security	• Detection of risky usage - zombie users or users oversharing files publicly • Detection of anomalous behaviors - high-rate of activity within Office 365 that may be indicative of data exfiltration, or suspicious login patterns. • Detection of security incidents - login from blacklisted IPs, or users sharing files with compromised personal accounts • Customized alerts for specific industry needs. For example detecting usage from proxies in specific countries

Benefits Of Adallom for Microsoft Office 365

The deployment of Adallom for Microsoft Office 365 enables organizations to optimize productivity and collaboration while addressing compliance mandates, and ensuring corporate data is secure from internal and external threats. Organizations also benefit from Adallom's cybersecurity research on alerts, anomalies and threats that impact their application.

ADALLOM

HQ
2390 El Camino Real, Suite 240
Palo Alto, CA 94306
+1 (650) 268-8322

R&D
Habarzel 21 Street, Building B
Tel Aviv, 6971001
Israel

www.adallom.com