

Solutions Brief:

Adallom for Custom Apps

Organizations deploying cloud applications have embraced the Adallom cloud access security platform for visibility, governance and protection of their cloud data. At the same time, many organizations have also created custom, home-grown applications that require governance and security controls. Adallom for Custom Apps allows organizations to extend Adallom features to their internal, custom applications.

Adallom delivers visibility, governance and protection for data in any cloud application, from enterprise SaaS to internal, custom applications. Adallom for Custom Apps allows organizations to extend features such as visibility, file-sharing management, user management, comprehensive access control policies and threat protection to internal, custom applications. These features can be extended to any application, whether it is running in a private data center, private cloud or in a public cloud infrastructure such as Amazon Web Services, Azure or Rackspace.

Introducing Adallom For Custom Apps

Adallom is a cloud access security platform designed to protect data in any cloud application. With Adallom for Custom Apps, traffic from the internal, home-grown application is sent to Adallom for application templating. Once this is completed, all of the capabilities of the Adallom cloud access security platform can be supported for the internal, custom application. Adallom for Custom Apps can be deployed out-of-band or as an inline proxy.

Key features include the following:

Visibility and Audit Trails

Adallom provides a clear and actionable audit trail of all user activities in the custom application including a dashboard featuring geographical and device access, files, and internal and external collaborators. Complete attestation of all activities is 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 with their personal email accounts, or monitor and prevent files from being shared with specific organizations or competitors. Once violations occur, users can be automatically notified, or a variety of actions initiated -- removing public access, removing shared links, changing user access. Specific custom policies can also be created, for example, monitoring files that are being shared by the CEO.

Cloud DLP

Using Adallom for Custom Apps, organizations may inspect for specific content within their internal application, such as healthcare information (PHI), personal credit card information (PCI), personal identifiable information (PII) or intellectual property. Content is identified with DLP mechanisms, and via metadata analysis of file names and extensions. Sharing-aware DLP enables DLP policies based on the content and sharing context of files – internal, external, public. When violations occur, users can be notified, and file permissions changed in addition to traditional block or quarantine actions.

Adallom for Custom Apps secures your sensitive corporate data, governs appropriate usage and detects high-risk behaviors and threats

Our unique cloud access security platform allows IT organizations to deliver the following for internal, custom application:

- Gain visibility into users, data and access for internal, custom applications
- Govern file sharing, access control, and enable DLP or encryption policies
- Mitigate risks by identifying high-risk usage, anomalous behaviors and security incidents

Access Visibility and User Monitoring

Adallom enables organizations to monitor access and usage of their custom application. 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. For example, 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 policies can be created, for example geographical restriction of Adallom access from Ukraine.

Anomaly and Threat Detection

Anomalies in the usage of the custom application can be detected using the Adallom SmartEngine™ advanced heuristics technology. 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 and comprehensive reports are available, including high-rates of download activities to users accessing the custom application from blacklisted IPs.

Forensics

Adallom for Custom Apps provides complete audit logs for IT security teams to perform forensics. Organizations can also enable forensics to be performed by the Adallom Labs team of cybersecurity researchers. Adallom Labs has identified and protected businesses in the past, ranging from a Zeus malware variant targeting Salesforce, to a token hijacking compromise exploiting a vulnerability in Microsoft Office 365. The team has also collaborated with multiple application vendors on threat research.

Adallom for Custom Apps

	Features
Visibility and Audit Trails	<ul style="list-style-type: none"> • Comprehensive audit trails and attestation for user, data, access and activities • File visibility and sharing trends to monitor sensitive files • User visibility and monitoring for internal and external collaborators • User and activity monitoring, for example, CEO and CFO of an organization or IT administrators • Visibility dashboard and reports
Governance and Compliance	<ul style="list-style-type: none"> • Cloud DLP - content inspection for confidential corporate data and compliance-related data • File and sharing management • Governance around activities • Governance around access - user, device, locations • Compliance reports
Threat Protection	<ul style="list-style-type: none"> • Detection of risky usage - zombie users, users with administrator privileges, or users oversharing files publicly • Detection of anomalous behaviors - high-rate of activity within custom applications that may be indicative of data exfiltration • 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 Custom Apps

The deployment of Adallom for Custom Apps enables organizations to provide governance and security controls to custom applications, whether they are deployed in the organization data center, private clouds or public cloud infrastructure. Organizations benefit not only from the comprehensive visibility, governance and threat protection features within Adallom, but also the ability to manage custom and enterprise applications using the same management interface.



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