ADALLOM

Datasheet

Adallom extends IT visibility, governance, and protection to cloud applications

Organizations have adopted SaaS applications like Salesforce, Box, Google Apps and Office 365 not only to reduce costs, but to unlock competitive advantages such as better collaboration and improved time-to-market.

Along with all the benefits offered by SaaS, its adoption has also introduced a new set of risk, compliance and security concerns. Important corporate assets now reside in a cloud infrastructure that is outside of enterprise control, accessed by users on a variety of mobile devices, occasionally over unsecured networks.

These valuable assets – intellectual property, customer data and financial information – need to adhere to corporate compliance mandates. In addition, the usage of this data must also be governed and protected from malicious, accidental and compromised insiders.

Unfortunately, legacy security solutions are not designed to protect data in SaaS applications. Traditional network security solutions such as firewalls and IPS don't have visibility into the transactions that are unique to every application, including how data is being used and stored. Further, cloud applications are designed to be accessed outside of the traditional corporate VPN network which means they are outside the purview of existing IT controls.

Cloud provider security should be complemented by new cloud security controls, as all SaaS vendor terms of service dictate the customer is accountable for protecting access to and usage of the service.

Adallom is a **new approach to cloud security** – one that is transparent to users, supports anywhere any device access, and delivers visibility, governance and protection for corporate data.

Visibility

Gain complete context into users, data, devices, activities, access.

Governance

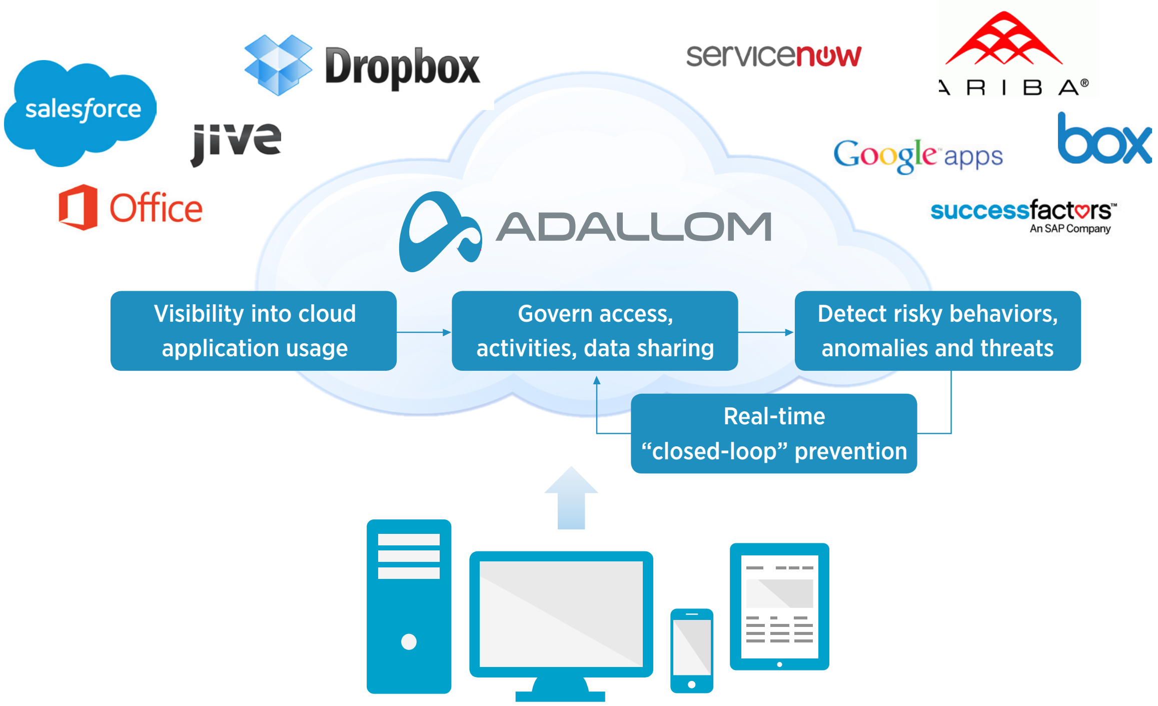
Implement policies for access, activities and data sharing.

Protection

Address risky activities, suspicious behaviors and threats.

Evolving IT Security To The Cloud

Adallom™ is a cloud access security broker. The Adallom cloud application security platform delivers visibility, governance and protection for the top SaaS applications used by businesses worldwide.


salesforce
Dropbox
jive
Office
servicenow
ARIBA®
Google apps
box
successfactors
An SAP Company
ADALLOM
Visibility into cloud application usage
Govern access, activities, data sharing
Detect risky behaviors, anomalies and threats
Real-time "closed-loop" prevention

Platform Architecture

The Adallom cloud application platform was built from the ground up to support a cloud-first architecture, designed to work with **any user, any network, any device** (managed or unmanaged) without painful network configuration or endpoint agent installation. Both data-at-rest and data-in-motion can be secured. The platform can be deployed as a 100% SaaS or on-premises if desired. The Adallom platform was designed to make it seamlessly simple to secure data in the cloud:

- **Flexible deployment:** Adallom supports flexible deployment modes. The API out-of-band deployment mode integrates directly into the framework of enterprise cloud applications in as little as 8 minutes. The patent-pending SmartProxy™ mode seamlessly directs users through the Adallom cloud, providing complete in-line control over the application without breaking application functions. These deployments can be selected per application or by specific use cases. For example, API mode for normal user access, and SmartProxy for unmanaged device access.

- **Extensible platform:** Adallom delivers a complete set of visibility, governance and protection capabilities. At the same time, the architecture is extensible, and can integrate with existing security solutions such as secure web gateway (SWG), security information and event management (SIEM), data leakage protection (DLP) and information rights management (IRM), to extend these capabilities to the cloud.

- **Any cloud application:** Adallom's unique application templating framework easily secures data in any cloud application, including Salesforce, Google Apps, Box, Office 365, Jive, SAP Success Factors, AWS, ServiceNow, Ariba and DropBox. Custom, home-grown applications can also be supported.

Security As-A-Service

One of the biggest challenges with security today is the lack of resources with security expertise, and the ability to prioritize critical threats. Every Adallom deployment is backed by SmartEngine™ heuristics technology and Adallom Labs™, an elite cybersecurity team staffed by the world's foremost experts in security and machine learning technology. SmartEngine "fingerprints" and builds a baseline of normal usage within an organization, and alerts on deviations. Adallom Labs vets all alerts, recommends cloud policies and delivers regular **SaaS Security Assessment Reports**, essentially acting as an extension of an organization's security team.

Complete Cloud Security Framework

The Adallom platform supports a complete set of features to secure data in SaaS applications.

- **Visibility and Context** - The Adallom platform fuses together information from multiple cloud application "connectors", including API, SmartProxy and IAM, to provide the most complete context on cloud application usage:
    - Discover and assess the risks of over 13,000 cloud applications in use: Manage vendor selection and the procurement process, and use the results to guide users towards corporate approved cloud applications.
    - Gain complete context on cloud usage: Understand users, data, activities, and how cloud applications are being accessed. Identify file sharing patterns, including with third-party ecosystems and personal email accounts.
    - Drill down into specific users: Searchable audit trails and integrated reports are available for forensics analysis.
- **Govern With Simplified Policies** - Granular cloud security policies can be built easily with the visibility already available on cloud application usage. Every insight is actionable, allowing organizations to remediate with a single click, or implement long-term access control, data sharing and granular usage policies:
    - Address compliance with DLP and eDiscovery features: Accurately identify documents with PII, PCI, PHI and sensitive IP. Address legal hold requirements in the cloud.
    - Enable robust data security: Govern file-sharing and access to sensitive files. Encrypt sensitive documents in the cloud and ensure they are shared and viewed in a secure manner.
    - Implement granular access and activity policies: Limit cloud application access by IP, role, user, or device. Restrict specific activities based on user and device.
- **Threat Protection Designed For the Cloud** - The Adallom threat protection capabilities were designed to identify high-risk usage, anomalous behaviors and security incidents. This is accomplished via proactive research and fine-tuning of the SmartEngine heuristics by Adallom Labs. SmartEngine uses more than 74 different variables to define normal usage within an organization, and can create alerts that are more customized per user when that user acts outside of their 'normal' profile. Pre-defined reports and alerts are available out-of-the-box, ensuring that organizations can address the following:
    - Detect high-risk usage: Identify high-risk users such as zombie users and IT administrators with super privileges, or users performing risky actions like sharing too many files publicly.
    - Detect anomalous behavior: Alert on suspicious activities such as simultaneous logins from two countries or sudden download of gigabytes of data.
    - Detect security incidents: Address potential security incidents and threats such as users connecting from blacklisted IPs or multiple failed-login attempts.

The Adallom cloud access security broker has effectively protected businesses from real-world attacks, including a Zeus malware variant targeting Salesforce and an Office 365 token hijacking vulnerability.

Adallom Security, Availability and Trust

The Adallom cloud services are delivered on a highly secure, reliable and scalable global infrastructure that can support millions of concurrent users. The Adallom cloud service is SOC2 and SOC3 certified and security penetration testing is regularly conducted by third-parties, including EY. In addition, the Adallom service has been built to withstand network failures and disasters with a highly available architecture composed of active regional clusters around the world. In the event of a failure, customer traffic is automatically rerouted to another active node to ensure no disruption of service.

Adallom also uses the same advanced cloud application controls to protect the Adallom service that is provided to customers. Adallom services include full audit trail capabilities, identity theft protection, actionable alerts and SIEM integration.

Feature Highlights

Shadow IT and Sanctioned SaaS Applications

Discovery of Cloud Services: Discover and assess the risks of over 13,000 cloud services in use. The Adallom comprehensive risk ratings can help with both vendor selection and procurement.

Manage Corporate-Approved Applications: Adallom's unique templating framework easily secures any cloud application including enterprise SaaS (Salesforce, Google Apps, Office 365, Box, Jive, Dropbox, SAP SuccessFactors, Ariba, ServiceNow), IaaS environments (AWS, Azure), and custom, home-grown applications.

Visibility and Intelligence

Application Dashboard and Audit Trails: Gain complete visibility and context into user and application usage, with details on user, location, activities, devices and data sharing patterns. Complete, granular, audit trails are available for forensics analysis.

Files and Data Sharing Monitoring: Monitor data within cloud drives such as Box, Google Drive and OneDrive. Discover data sharing capabilities within applications including Salesforce, Ariba, and ServiceNow. Analyze data by type and sharing permissions. Deep dive into file sharing patterns, and modify sharing permissions directly from the management console.

User and Activity Monitoring: Get visibility into cloud application users, internal or external, whether connected from home, office or mobile without installing any agent on user devices. Remove user privileges directly from the management console. Monitor user activities.

Third-Party Application Discovery: Discover third-party applications running on cloud application platforms (example: Mapping Sheets or HangOuts running on GoogleApps) or applications connected to identity and access management providers like Okta or Centrify.

Governance and Compliance

Cloud DLP and Field DLP Policies: Comply with regulatory mandates such as PCI, HIPAA and more. Govern data in the cloud, for example, files that are stored in cloud drives, as attachments or within cloud application fields. Use predefined fields or extend existing enterprise DLP policies to SaaS applications.

Data Security: Deliver complete data security by encrypting files stored in cloud applications, and ensuring they are retrieved and viewed in a secure manner. Manage file lifecycle, for example, transfer ownership of orphan files when users depart the company. Ensure the right users have access to critical corporate documents, and govern inappropriate file-sharing.

Activity Policies: Govern cloud application activities including allowing specific application functions or triggering an alert for activities from anonymous proxies.

Access Policies: Customized policies are available for granular access control. This includes addressing unauthorized mobile device access or limiting access to specific applications based on devices.

eDiscovery Policies: Execute against legal and information governance mandates. Identify and hold content required for eDiscovery across all SaaS applications.

Governance and Compliance Reports: Dynamic reports can be run on DLP violations, sensitive file sharing, and data sharing violations.

Comprehensive Protection

Detection of High-Risk User and Behaviors: Detect high-risk users and behaviors to reduce the attack surface. High-risk users include zombie users, IT administrators with substantial privileges, or users that are sharing too many files publicly.

Detection of Anomalous Behaviors: Detect and alert on anomalous behaviors that may be indicative of breaches, identify theft, data theft and credential theft. Adallom SmartEngine advanced machine-learning heuristics learns how each user interacts with each SaaS application, and through behavioral analysis, accesses the risks in each transaction. For example, access from multiple locations simultaneously or suspicious login patterns.

Detection of Security Incidents: React quickly to security incidents with actionable alerts. These include alerting on users using vulnerable accounts (example: users compromised by the Adobe Creative Cloud breach), users connecting from blacklisted IPs or multiple failed log-in attempts that may signify a brute force attack.

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