Data sheet

HP Cloud Access Security protection platform

Visibility, governance and protection to Cloud apps

We are rapidly moving towards a cloud majority world. However, cloud adoption has also introduced a new set of risks, both internal and external. HP's Cloud Access Security (CAS) protection platform helps organizations to solve this complex issue by delivering greater visibility, governance, and protection for cloud applications.

Visibility

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

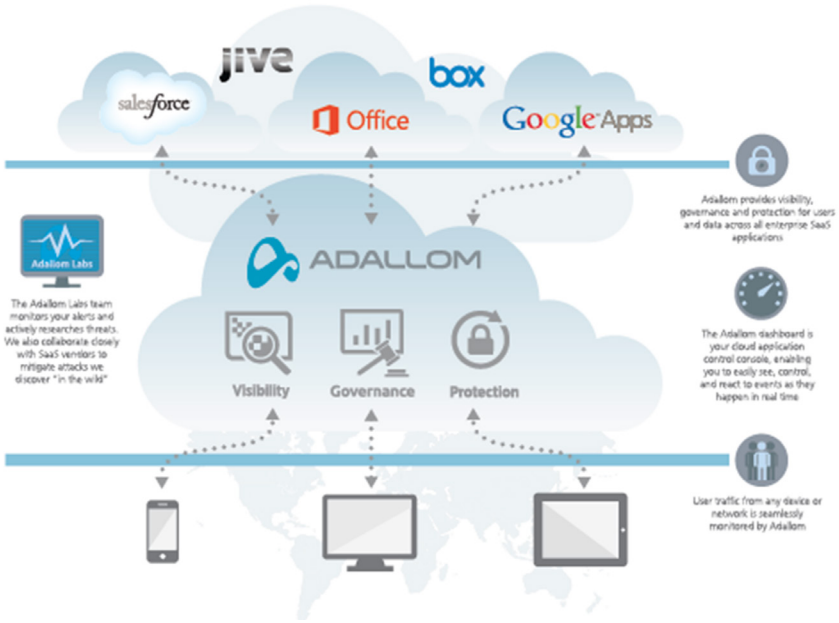
Governance

Implement policies for access, activities and data sharing

Protection

Address risky activities, suspicious behaviors and threats

Figure 1. Adallom Cloud Access Security Broker (CASB) protection



Evolving security to cloud apps

The SaaS (Software-as-a-Service) era is here. Organizations worldwide have adopted cloud applications such as Salesforce, Box, Google Apps and Microsoft® Office 365 not only to reduce costs, but also to unlock competitive advantages such as better collaboration and improved time-to-market. However, cloud applications require a new approach to data governance, risk management and cloud data security because of the ubiquitous nature of access, the collaborative workflow enabled, and the myriad ways that confidential data can be stored and shared.

The Adallom™ Cloud Access Security Broker (CASB) is the first component of HP's Cloud Access Security (CAS) protection platform strategy, designed to address this complex issue by delivering visibility, cloud governance and protection for the cloud applications used by businesses worldwide.

About Adallom

Adallom provides a CASB that seamlessly integrates with your enterprise cloud applications without impact to end-users. Adallom delivers visibility, cloud governance, and protection for any user, in any location, on any device. Adallom's comprehensive audit trail correlates each activity to a user. You can govern cloud application usage, secure corporate data, and react in real time to an account compromise or risky behaviors.

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, HP Atalla, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

How it works

The Adallom CASB protection integrates with multiple cloud applications, giving extensive visibility into an organization's SaaS activities. Adallom is designed to work with any user, any network, and any device (managed or unmanaged) without painful network configuration or endpoint agent installation. It can secure both data-at-rest and data-in-motion depending on deployment mode. It can be deployed in the following distinct modes:

API mode (out-of-band)—integrates directly with cloud application APIs for an out-of-band implementation that is quick to set up and fully transparent to users. The API mode allows collection and correlation of user identity and activity information such as login/logout, location, duration, uploads, downloads, sharing privileges and more across multiple cloud applications. Once integrated with multiple cloud applications, Adallom analyzes the information from the different data sources and creates a command and control center (the Adallom console) which allows for full visibility of an organization's SaaS activities. cloud governance and compliance (cloud DLP) policies can be created to inspect and govern sensitive content for files at rest, across all applications.

Adallom SmartProxy™ mode (in-line)—seamlessly redirects all application traffic through the Adallom cloud service to provide organizations with complete visibility and real-time control over user requests, provider responses, and activities from managed or unmanaged devices. The Adallom SmartProxy technology provides real-time alerting and blocking of policy violations (DLP, managed IP ranges, etc.), in addition to real-time access control (including geographic information, device and data policy). This mode can also be used to deliver cloud governance on file or application transaction activities, and provide real-time alerts on threats or policy violations.

Hybrid mode—hybrid mode combines the benefits of both API and Adallom SmartProxy modes and can be used to address the widest variety of use cases. For example, API mode for normal access, and Adallom SmartProxy for unmanaged device access.

Once deployed, Adallom constantly collects user identity and activity information. The Adallom SmartEngine™ heuristics technology learns about each user, and creates alerts when a user acts outside of their normal profile.

Every Adallom deployment benefits from the collective intelligence of all cloud application deployments and proactive research by Adallom Labs™, a team staffed by the world's foremost experts in machine learning technology, Big Data processing, and cyber forensics skills. The Adallom SaaS security framework has been proven to be effective in protecting businesses from real-world attacks, including a Zeus malware variant targeting Salesforce.com and an Office 365 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 cloud data security penetration testing is regularly conducted by third parties, including Ernst & Young. In addition, the Adallom service is 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 reduce the likelihood of service disruption.

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.

Key features:

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 cloud application 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, Yammer), IaaS environments (AWS, Azure), and custom, homegrown applications.

Visibility and intelligence

- Application dashboard and audit trails: Gain extensive visibility and context into user and application usage. Comprehensive and granular audit trails are available for forensics analysis.
- Files and data sharing monitoring: Monitor data within cloud drives and discover data-sharing capabilities within applications. Analyze and modify sharing permissions directly from the Adallom management console.
- User monitoring: Get visibility into cloud application users without installing any agent on user devices. Remove user privileges directly from the Adallom management console.
- 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 such as Okta or Centrify.

Governance and compliance

- Cloud data loss prevention (DLP) and field level DLP policies: Comply with regulatory mandates such as PCI, HIPAA and more. Govern data in the cloud or within cloud application fields by using predefined fields or extending existing enterprise DLP policies to SaaS applications.
- Cloud data security: Deliver comprehensive cloud data security by encrypting files stored in, uploaded to, or downloaded from cloud applications to confirm that they are retrieved and viewed safely.
- Access policies: Customizeable policies are available to enforce granular access control. For example, blocking access from unmanaged devices, or enabling encryption/IRM when sensitive documents are downloaded on unmnanaged devices.
- eDiscovery policies: Execute against legal and information governance mandates. Identify and hold content required for eDiscovery across all SaaS applications.
- Cloud 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 users and behaviors: Detect high-risk users (zombie users, IT admins, and privileged users) and behaviors to reduce the attack surface.
- Detection of anomalous behaviors: Detect and alert on anomalous behaviors that may be indicative of breaches, identity theft, data theft and credential theft. This is accomplished leveraging Adallom SmartEngine™ advanced machine-learning heuristics.
- Detection of security incidents: Identify and react quickly to cloud data security incidents with actionable alerts. These include alerting on vulnerable user accounts (example: users compromised by the Adobe® Creative Cloud breach), users connecting from blacklisted IPs or multiple failed login attempts that may signify a brute force attack.

Resources

Sales contact
HPAtallaGlobalSales@hp.com

Learn more about HP Enterprise Security products, services, and solutions
hpenterprisesecurity.com

Cloud applications supported

- Salesforce
- Google Apps
- Microsoft Office 365
- SuccessFactors
- ServiceNow
- AWS
- Jive
- Box
- Dropbox
- Workday
- Yammer
- Zendesk
- Ariba
- Azure

HP Cloud Access Security protection platform offerings

Offering	Details	Deployment options
Adallom Cloud Protection Platform	Available for either SaaS or on-premise/private cloud deployment. Licensed per platform user and per application user. Requires purchase of both Adallom platform and per application user components. Available as 1-year term. Includes 24x7 support.	SaaS On-premise/private cloud

Learn more at
hp.com/go/CloudAccessSecurity

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-8065ENN, April 2015