Solutions Brief:

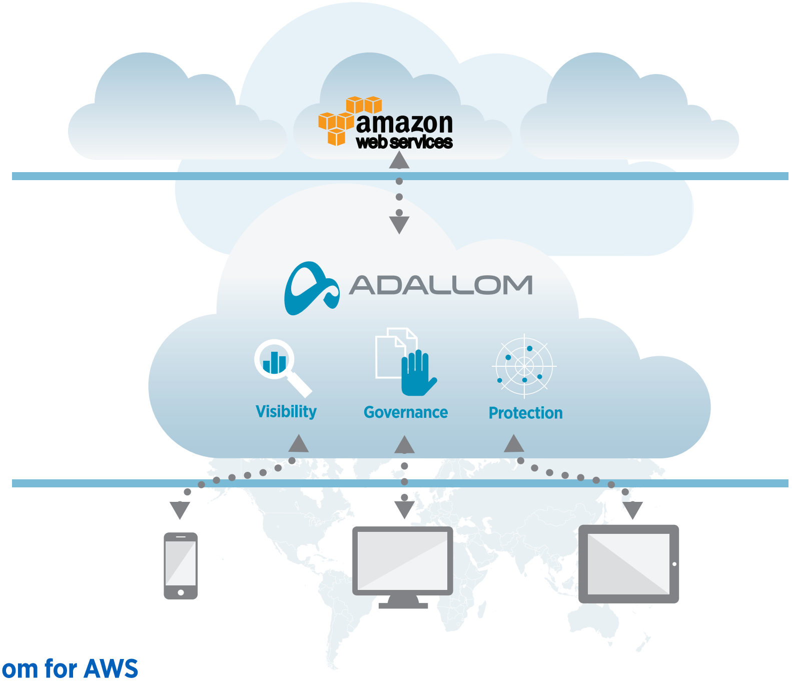
Adallom for AWS

Amazon Web Services (AWS) allows organizations to deploy application workloads in a flexible web server environment in the cloud. Multiple security solutions, ranging from virtual firewalls to virtual intrusion prevention systems are available to secure these application workloads in the cloud.

However, one of the biggest risks with AWS may be with the security of the AWS environment itself. Specifically, any unauthorized access or compromise to the environment puts entire projects and critical data at risk. In June 2014, an attacker gained access to the AWS management console for Code Spaces, a SaaS provider offering source code management tools. When his ransom demands were not met, he deleted all instances of Code Spaces, putting the company out of business.

In addition to unauthorized access, configuration changes to the AWS environment may be made by IT administrators without proper understanding of their impact. It is critical to be able to track and monitor these changes.

Adallom for AWS allows organizations to mitigate these risks. Adallom for AWS monitors all administrative API and console access to AWS, governs configuration changes and detects anomalous behaviors. The solution also enables granular controls, for example, allowing access to the console only via managed devices.



Adallom for AWS

Adallom is a cloud application security platform deployed between users and the AWS management interface. It can be deployed as a 100% SaaS deployment, featuring flexible modes ranging from API to SmartProxy^{TM,} or as an on-premise solution.

The API deployment mode integrates directly into the framework of AWS in as little as 8 minutes.

Adallom for AWS

The Adallom cloud application security platform allows IT organizations to:

- Enable secure access of the AWS administrative console for the right users, devices and from the right locations
- Address security and compliance mandates that requires attestation and reporting of AWS activities
- Govern and address risky behaviors, anomalous behaviors and security incidents

When deployed in proxy configuration, the patent-pending SmartProxyTM architecture seamlessly directs users through the Adallom cloud, providing complete control over the AWS management interface activities. Integration with identity and access management providers such as Okta and Centrify is also supported.

Adallom features for AWS include the following:

Attestation, reporting and auditing of AWS activities - Adallom provides a dashboard of users, their activities and how they're accessing the AWS management console. Comprehensive audit trails of users and their activities in the AWS environment are available, along with the ability to filter into specific users or activities for attestation or forensics reasons.

Monitoring of API calls to AWS - One of the common ways to access AWS is via language-specific API calls. Part of the security framework for protecting your data means protecting the AWS environment from badly engineered API calls or threats within the API calls that may impact your AWS environment. Adallom monitors the API requests to the AWS interface, validating that the calls are legitimate, and do not contain any threats.

Monitoring of administrators - Administrative or privileged users are a potential risk because their levels of access makes it easier for them to do more damage when they are intentionally being malicious, or if their credentials are stolen. Adallom enables organizations to monitor specific AWS administrative users, or to alert when specific activities are performed.

Customized access control policies - Adallom enables access to the AWS console to be defined based on users, devices, location. This enables appropriate governance, for example geographical restriction of access where organizations don't have office locations. Flexible policies can be created for high-risk scenarios, for example, restricting access or providing read-only access to users accessing from unmanaged devices or from vulnerable browsers and operating systems (O/S).

Configuration change monitoring – Using Adallom, organizations can define custom configuration monitoring policies to detect any deviation from security guidelines. This helps prevent high-risk configuration changes that inadvertently or intentionally bring risks to the AWS environment.

Suspicious activity detection - The Adallom SmartEngine advanced heuristics technology defines baseline usage of the AWS environment using more than 75 variables, so that deviations can be found. This allows organizations to discover potential security incidents such as high-rates of administrative activities, simultaneous access from multiple locations, activities from anonymous proxies and administrators accessing from blacklisted IPs. This feature is enabled "out-of-the-box" without requiring complex rules and configuration.

Proactive cloud 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 has successfully identified cloud security attacks, including MS13-104, a token hijack compromise in Sharepoint and Onedrive that exploited a vulnerability in Microsoft Office 365 and a Zeus variant targeting Salesforce. Adallom acts an extension of an organization's security team to help mitigate risks and threats. A regular Security and Risk Assessment Report that summarizes top cloud security risks is included as part of the Adallom cloud services.

Benefits Of Adallom for AWS

The AWS environment may be supporting some of the most critical projects and applications for an enterprise. One of the biggest security risks may be unauthorized access to this environment. It is critical to proactively monitor, and govern access to the AWS environment, and identify risky behaviors or potential security incidents. The deployment of Adallom for AWS enables organizations to secure the AWS administrative console, monitor usage and activities within the environment and protect it from threats.

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