ADALLOM

The Case For A Cloud Access Security Broker

Executive summary

The SaaS era is here. According to Gartner, SaaS and cloud-based business application services revenue will grow from $13.5 billion in 2011 to $32.8 billion in 2016. PwC's latest Global 100 Software Leaders Report shows that the top software companies in the industry have continued a consistent and growing shift towards Software-as-a-Service (SaaS), growing their revenues by 60% to US$20 billion.

The move towards SaaS applications are helping IT teams become more efficient. It allows them to be able to offload the day-to-day operations and maintenance of applications, so they can focus on helping their business grow. However, with SaaS adoption comes new risks. SaaS applications require a new approach to data governance, risk management and security because of the ubiquitous nature of access, the collaborative nature of SaaS applications, and the myriad of ways that confidential data can be stored within applications.

This paper describes the emergence of a new IT technology category that Gartner defines as Cloud Access Security Brokers, and how Adallom's cloud access security broker is best positioned to address these requirements.

Introduction

Hundreds of years ago, what differentiated a business from another was literally keeping the lights on. Electricity was a critical utility, and the businesses that won were the ones located closest to power generating stations, making it easier to support their machines, products and services. The emergence of the electricity grid changed all that. With the ability to plug into a global electricity grid, businesses could then focus on their products and services instead of worrying about their utilities.

Fast forward hundreds of years later, the parallels are similar to cloud computing as explained in Nicholas Carr's book, "The Big Switch." IT teams used to run applications on server infrastructure that they struggled to maintain. They worried about performance, power, cooling and scale. Things were expensive, time-consuming and slow.

IT's Evolution to The Information Economy

Now, IT can deliver applications reliably and cost-effectively by purchasing almost infinite cloud computing resources from Amazon. Development and engineering teams were the first to reap the quick-to-deploy advantages of Infrastructure-as-a-Service (IaaS), with officially sanctioned IT-driven projects to follow.

The next wave of cloud is going to be Software-as-a-Service (SaaS). Instead of focusing on the creation and day to day maintenance of an on-premise system, IT can just purchase complete application systems via best-of-breed cloud providers-- Microsoft Office 365 or Google Apps for email and collaboration, Workday for human capital, Salesforce for customer relationship management and Box for content management. IT teams are now moving towards an information economy, where they can focus less on infrastructure building but more on the information and resources that can differentiate their business from others.

Part of the move is driven by mobile - a new generation of workers that now expect the ability to access data from any device, at any time. IT has to address these new needs and be able to react quickly to changing application demands. A better way to address this is to just deploy a SaaS application designed (with a formidable engineering team behind it) to deliver one application very well.

Granted, IaaS will never go away, as there will always be legacy applications that need to be deployed in an infrastructure that is an extension of the enterprise cloud. In addition, many SaaS applications are built on top of IaaS.

As enterprises become more comfortable with ceding control to IaaS providers, they will also begin to trust SaaS providers for their

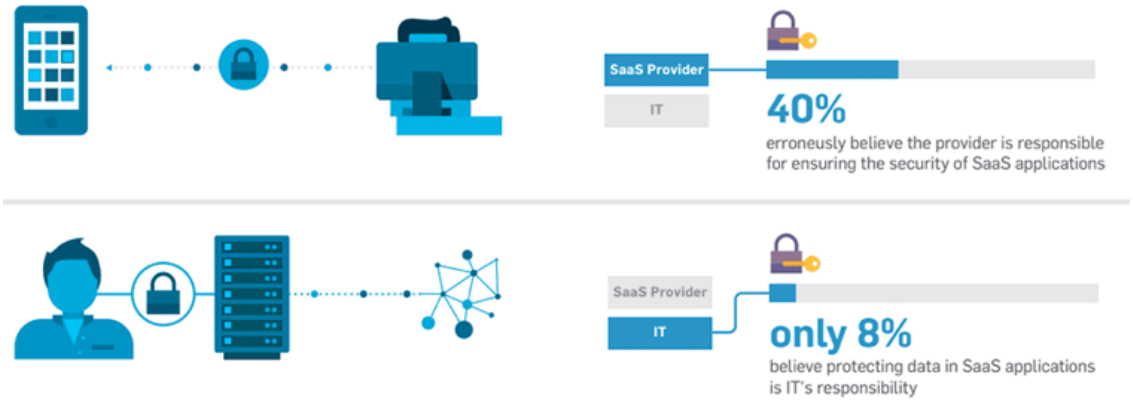
primary applications. IaaS doesn't solve a lot of the heavy day-to-day maintenance of deploying an application, SaaS does.

SaaS frees up IT resources to do the things that matter – tapping into the information that provides a competitive advantage. In a recent Gartner CIO event in San Francisco, Leigh McMullen, Managing VP of the CIO research team, described a sports apparel and footwear company that analyzed popular songs that runners listened to as they jogged up San Francisco hills. One song, in particular, was particularly popular and effective in motivating the runners, so they used this same song in commercials when launching a high-end running shoe. These are the types of engagement that IT can enable if they did not have to worry about installing or running a piece of software.

Understanding the Shared Responsibility Model

One of the key aspects to understand with the deployment of sanctioned cloud applications like Salesforce, Box, Office 365 or Google Apps is that while IT organizations have "outsourced" the day-to-day operations and maintenance of an application to the cloud, they do not forgo their accountability and liability for the data within the application

A recent survey performed by Forrester[1] shows how divided people in the industry are on this topic:



The shared responsibility model defines the responsibilities of the different parties involved. The analogy of the shared responsibility model between an enterprise and a SaaS provider contract is very similar to the responsibilities users undertake when choosing to park vehicles in a public parking garage. The parking garage will invest in security for their facilities, but are indemnified when it comes to valuables in the car being stolen.

Similarly, SaaS providers are responsible for securing the complete application stack, from the infrastructure through the application. However, the enterprise customer is responsible for the access to and usage of the data within the cloud application. In other words, the enterprise needs to proactively take responsibility for their usage and data within a cloud application.

The SaaS provider cannot take full responsibility in the event of a data breach because it only sees activities within its own application, and cannot understand the difference between normal usage and compromised usage. More importantly, only the enterprise can define a security policy when it comes to which users are allowed access to the application, which files have sensitive corporate data that cannot be shared publicly, and what types of usage need to be monitored.

Requirements for Securing SaaS Applications

If we are to meet the challenges of the information economy, then organizations need to embrace SaaS applications, but without compromising their security posture. Every piece of data that resides in the cloud becomes a valuable corporate and competitive asset that needs to be protected. Therefore, enterprises must proactively deploy security solutions that deliver visibility, governance and control to cloud applications as they do for on-premise applications.

However, when it comes to SaaS applications versus on-premise, there are three characteristics that define the need for a different approach to data governance, risk management and security in the cloud:

• **Anywhere anytime any device access** – Users with an account and password can access SaaS applications from anywhere on any device at any time. This includes access via managed and unmanaged devices. This is very different from on-premise applications where access is only allowed via corporate VPN networks and managed devices, and additional barriers of security exist between the user and the data center hosting the application.

• **User-defined usage** - For the first time, users, not IT, are defining how information (in files or folders) are used and shared in services like Box, Office 365, or Google Apps. Users can invite collaborators and share these files with anyone using just one link. Many of these users have very little security background to understand when their actions bring risks to the organization

• **Unique data sharing capabilities** – There are a myriad of ways that data is being shared and stored, unique to every SaaS application. For example, within Salesforce alone, sensitive corporate data may reside in Chatter files, Salesforce knowledge base articles, documents, and attachments. Existing solutions like firewalls and intrusion prevention systems don't have visibility into the data within a SaaS application, and do not understand the nuances of every SaaS application transaction.

SaaS security solutions must be able to identify data within a cloud application and understand the human transactions related to it. For example, what data exists, who is interacting with it, what application transactions are performed, how data is being accessed and shared, what types of data must meet compliance requirements—these are the very attributes that impact an organization's risk profile in the cloud.

Cloud Access Security Brokers Overview

In 2012, Gartner initiated analysis of a new technology area called cloud access security brokers (CASB) to address SaaS security. Gartner believes that by 2018[2], 25% of corporate data traffic will flow directly from mobile devices to the cloud.

The four pillars of CASB[3] include visibility, data security, compliance and threat prevention.

• **Visibility** – The requirement here is the ability to gain visibility into users, data, access, locations in a SaaS application, in addition to integration with security information and event management (SIEM) solutions to extend visibility to existing monitoring solutions.

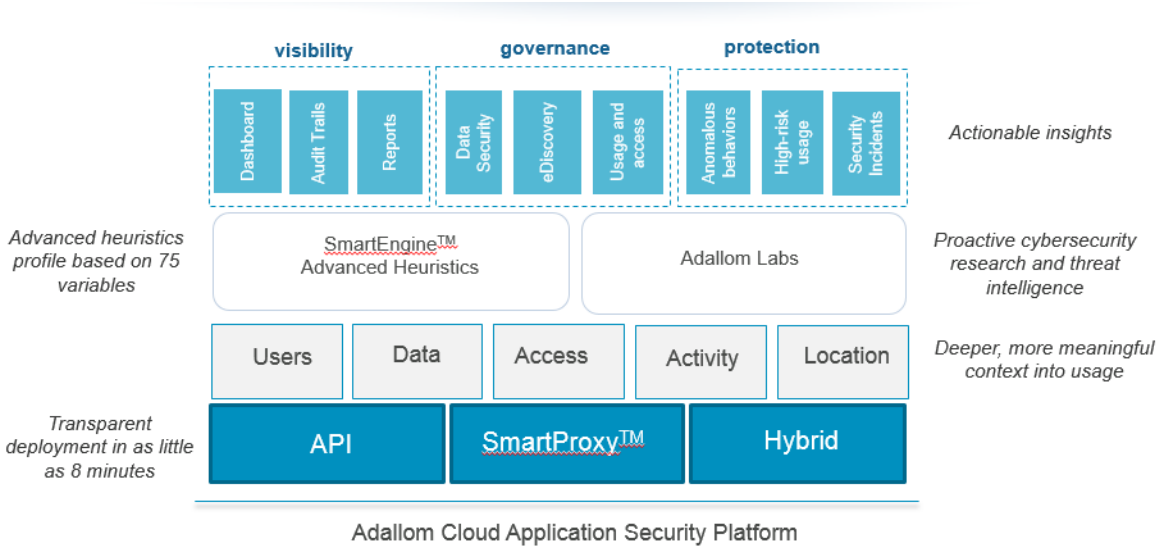
• **Data security** – The encryption of sensitive data must be supported via a configurable policy. As part of data security, files and content must not be "orphaned" when users are de-provisioned. This pillar also includes the ability to address data loss prevention (DLP) and e-discovery capabilities in the cloud.

• **Compliance** – Organizations must address the compliance requirements of who, what, when, why and where, including auditing of user behavior. In addition, CASBs must be able to deliver out-of-the box compliance reports.

• **Threat prevention** – This pillar includes the ability to identify access from suspicious hosts, devices, locations and more, zombie users, users bypassing identity access management solutions, users using outdated operating systems, and access from compromised accounts. This pillar also includes the ability to define a policy to identify and prevent malicious and anomalous activities.

Introducing Adallom Cloud Security Platform

Adallom is a cloud access security broker designed to seamlessly secure data in the cloud. The Adallom cloud application security platform allows enterprises to govern application usage, secure corporate data and detect suspicious activities in any application.



Key differentiators include the following:

Flexible and Extensible Platform Architecture

One of the important considerations with cloud access security brokers is the platform architecture. The appropriate platform architecture can deliver a seamless user experience, ubiquitous access for any user (on any device, managed or unmanaged) and secure data in any type of application.

This is the strength of the Adallom platform. The Adallom cloud access security platform supports API mode, SmartProxy and hybrid deployment modes. These configuration modes provide flexibility for users and IT with the ability to secure data-at-rest and data-in-motion for managed and unmanaged devices.

In addition, hybrid deployment modes can be deployed for specific use cases. For example, organization can combine API mode for normal access with SmartProxy mode for unmanaged devices.

The Adallom platform architecture is also extensible, allowing organizations to extend their existing security investment in Identity Access and Management (IAM), DLP and SIEM solutions to the cloud. Integration with Identity Access and Management (IAM) providers and directory infrastructures like Active Directory provides visibility into user authentication and identity information, and enables governance based on user identity.

Actionable Insights and Governance

Adallom uses data from all deployment modes to deliver deep, meaningful insights on users, data, access and their activities across all cloud services. Any insight is actionable, allowing organizations to enable the right policies. Organizations can easily address compliance mandates like cloud DLP, eDiscovery and encryption. Compliance policies can be created within the Adallom management interface, or by extending existing on-premise compliance policies to the cloud.

In addition, the Adallom SmartEngine™ heuristics engine uses more than 74 different variables to learn about each unique user in order to profile normal cloud application usage. Out-of-the-box, the SmartEngine can create alerts that are customized per user and apply them when that user acts outside of their "normal" profile.

This heuristics engine, along with integrated, out-of-the-box reports allows organizations to understand risks and threats in cloud application usage, without needing to undergo complex analysis.

Any Application Supported

Adallom's unique application templating framework allows any application to be supported. This includes securing enterprise SaaS applications such as Box, Google Apps, Salesforce and Office 365, AWS and Azure environments, as well as internally developed applications.

• Enterprise SaaS applications – Adallom provides the ability to extend visibility, governance and protection across all corporate sanctioned SaaS applications used by businesses.

• IaaS environments –One of the challenges with IaaS environments like AWS and Azure is the risk to the environment itself such as compromised access, unauthorized configuration changes and threats. Adallom allows organizations to mitigate these risks by monitoring all administrative API and console access to AWS, governing configuration changes and detecting anomalous behaviors. The solution also enables granular controls, for example, allowing access to the console only via managed devices.

• Custom, home-grown applications – Most organizations utilize a combination of enterprise off-the-shelf applications and home-grown applications. Adallom allows organizations to extend governance and security controls to custom, home-grown applications, whether these are deployed in internal data centers, private clouds or public cloud infrastructure.

Adallom Labs

There are two key challenges for organizations dealing with security today. One is the ability to hire skilled people in security, and the other is prioritizing which security risks are critical and need to be dealt with immediately.

Adallom Labs is a team of cybersecurity, machine learning and forensics experts that addresses these challenges. The team collaborates with top security and cloud groups, from Salesforce to Microsoft, and analyzes data from both internal and external security intelligence feeds. More importantly, Adallom Labs adds human-driven analysis to the SmartEngine™ heuristics. When there is an alert, security experts vet the risks to the organization and create an actionable alert that can be instantly applied as policy with the click of a button. Additionally, Adallom Labs performs cloud-based attack forensics, such as malware and insider threat analysis, and adapts cloud security risk patterns on an ongoing basis to improve the overall security of all Adallom customers.

Adallom Labs acts as an extension of an organization's IT team, delivering regular Risk Assessment Reports, and recommending appropriate security policies as part of the Adallom services. Adallom is the only cloud security vendor that has protected businesses against real-world attacks, and in the process discovered a Zeus malware variant targeting Salesforce and an Office 365 token hijacking vulnerability.

Summary

The promise of productivity and efficiency benefits from the deployment of SaaS applications is real. In order to reap these benefits, it is critical to select a cloud access security broker with the following requirements:

• A platform architecture approach that is flexible and extensible to address all cloud use cases

• A solution that delivers critical features necessary to secure and govern data in the cloud, in particular incorporating heuristics technology that understands the difference between normal and compromised or malicious usage

• The ability to address governance and security for any user on any network (corporate or public) on any device (managed or unmanaged)

• Human-driven analysis to continually assess new threats and continually evolve protection capabilities.

The Adallom platform delivers the most flexible, non-intrusive deployment options for cloud application security. With the combination of our API and SmartProxy deployment modes, organizations can gain visibility into users, data, access, activities, and support a diverse set of governance and protection features. These benefits can be accomplished without any impact to users. More importantly, the combination of the Adallom SmartEngine heuristics and Adallom Labs delivers the highest signal-to-noise ratio when it comes to identifying risks and threats to your cloud applications.

References

[1] A. Cser, "SaaS Adoption Requires A New Approach To Information Security," Forrester Consulting, 2014.

[2] I. Keene, C. Wong, L. Lowerree. "Market trends: Small Cell Infrastructure, Small Cell Deployment Strategies," Gartner 2014

[3] C. Lawson, S. Deshpande, "Mind the SaaS Security Gaps" Gartner 2014

ADALLOM

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

www.adallom.com

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