Global Information Assurance Certification Paper

Changing the Perspective of Information Security in the Cloud: Cloud Access Security Brokers and Cloud Identity and Access Management

GIAC (GSEC) Gold Certification

Author: Jennifer Johns, jennijohns@protonmail.com
Advisor: Stephen Northcutt
Accepted: August 2nd 2016

Abstract

Businesses are leveraging cloud computing services at an exponential rate. Working in the information security industry during the cloud computing frenzy is exciting, but it is also proving to be challenging as cloud computing service providers (CSPs) have typically lacked industry standard security controls. To help explain why the rate of cloud adaptation matters, we can look at a lesson from physics on velocity versus acceleration. Velocity is how fast you are going, and acceleration is how fast velocity increases ("What is the Difference between Speed, Velocity and Acceleration?," n.d.). They affect our perceptions differently. For example, driving a car down the freeway at 70mph is no big deal, but accelerating from a dead stop to 70mph might get you short of breath. We are witnessing this battle between velocity and acceleration happen in information security in the cloud. Two game-changing security product suites, Cloud Access Security Brokers (CASBs) and Cloud Identity and Access Management (Cloud IAM) solutions are stepping up to the plate as formable contenders in the cloud security arena. Enterprises that leverage the cloud without planning for proper security controls will not be able to predict their future, but most likely can predict unauthorized access to their data. Cloud security is your responsibility. Change your perspective on information security in the cloud. Take control with Cloud Access Security Brokers and Cloud Identity and Access Management.

1 Introduction

What do you think of when you think about information security in the cloud? If you automatically let out a quiet chuckle under your breath, we might have been of the same mindset.

So far, technology solutions provided to address security in the cloud have not been so good. But times are changing. Cloud security has come a long way in recent months regarding available security solutions ("Security in the cloud," n.d.). Cloud Access Security Brokers (CASBs) and Cloud Identity and Access Management (Cloud IAM) solutions are two critical security products that can help reduce the risk of a security breach in the cloud. These solutions give information security professionals visibility and control over how, and what, is being accessed in the cloud, and who can, and is, accessing that data.

So what is a CASB? Gartner lists Cloud Access and Security Brokers as a top technology to shape information security in 2016 (Evans, 2016). Cloud access security brokers are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement including authentication, single sign-on, authorization, logging, alerting, and so on ("Cloud Access Security Brokers (CASBs) - Gartner IT Glossary," n.d.).

You are most likely familiar with Identity and access management (IAM) being the security discipline that enables the right individuals to access the right resources at the right times for the right reasons ("Identity Management - Access Management - Gartner Research," n.d.). But what is Cloud Identity and Access Management? It is a way to manage federation identity, using a federated gateway, located in the cloud. Federated identity management enables identity information to be shared among several entities and across trust domains. Identity attributes are transferred from one trusted identifying and authenticating entity to another, thus providing “single sign-on” ("Federated Identity Management - Gartner IT Glossary," n.d.). Cloud access security brokers simplify the operational management of federation identity by hosting the federation gateway in the cloud. Externalizing federation allows the enterprise to delegate issuing the various authentication token types from cloud services to itself. The work of

handling translation from one format to another is handled by the CASB federation gateway versus the enterprise's technology team (Cloud Security Alliance, 2010, p.18).

2 Visibility, Visibility, Visibility

In real estate, it's all about location, location, location. For information security in the cloud, it is all about visibility. You cannot protect and secure what you cannot see ("Visibility: The Key To Security In The Cloud," n.d.). So how do you get visibility in the cloud and ensure that you are secure? The first step is to understand that cloud security is your responsibility. Every business is responsible for their cloud security. There are no cloud service providers, or cloud security products, that will magically protect you from every data security breach. You need to know what is valuable to protect and how to protect it. Even if you know what to protect, mistakes can happen. As much as 90% of security incidents involve human error (Howarth, 2014).

Human error can become disastrous when you start to think about how this can happen with cloud services. Information security professionals are no longer able to see what is taking place within in the cloud environment like they could with on-premise systems. System misconfigurations, poor patch management practices, using default usernames and passwords, or capturing privileged credentials are all things that are caused by human error.

Systems and network administrators are the most trusted and highly skilled users, however, they are also the most targeted users. Looking at Figure 1 below you can see the increase of hacking, malware, and social threat action categories over time. Notice the sharp uptick over the last few years. Phishing threats (represented by the 'Social' category), malware threats, and hacking threats, are all related to the human element. These elements have been difficult to detect effectively in the past for cloud services, but now cloud access security brokers and cloud identity and access management security solutions are providing much- needed security intelligence.

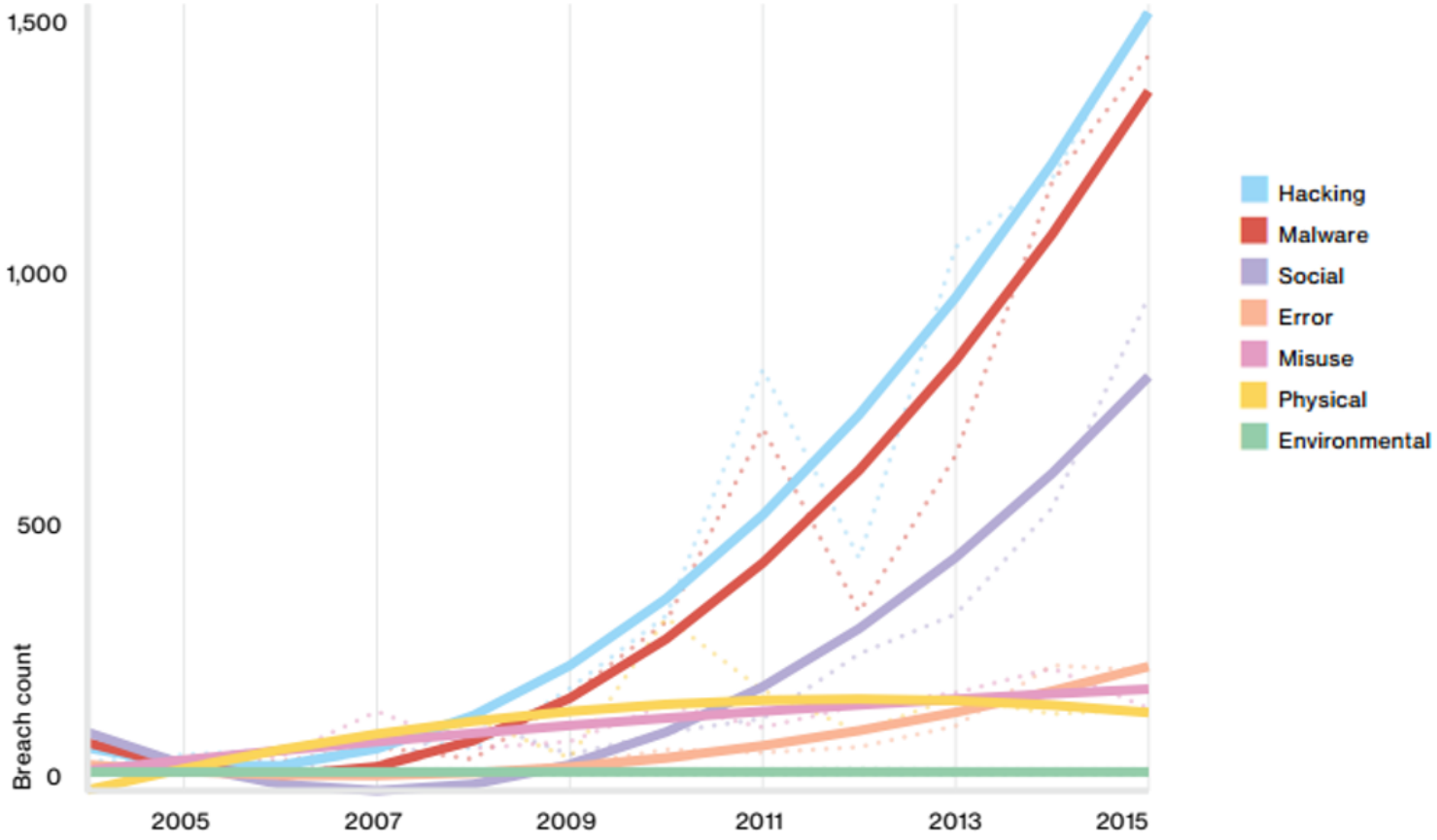


Figure 1. Number of breaches per threat action category over time

("2016 DBIR: Understand Your Cybersecurity Threats | Verizon Enterprise Solutions," n.d.)

Visibility through security intelligence is successful when the business users support the adaptation of the security products, so balancing security with a non-disruptive user experience is critical. To explore the specifics of how we can achieve this, let's use a common business scenario of migrating corporate services to Office 365 in the cloud.

Jennifer Johns, jennijohns@protonmail.com

THE SCENARIO:

- You just migrated to Office 365 from a traditional on-premise active directory environment. The on-premise environment offered corporate services such as Exchange, SharePoint, Lync, and internally managed file shares. You required a VPN connection to access corporate resources remotely.
- You now leverage Exchange Online, SharePoint Online, Skype for Business, and OneDrive for Business in the cloud. Active Directory federation services (ADFS) with DirSync are used to populate on-premise Active Directory accounts to Azure Active Directory so your users can use their domain accounts to log in to Office 365 services. You allow users to directly access these corporate services in the cloud without using a VPN connection. You still require a VPN for all other business services.

In our scenario above of migrating to Office 365, we end up with a brand new user account in the cloud for each employee. To solve authentication after migrating, you have two options. Federate the authentication from Office 365 back to your on-premises Active Directory by using Active Directory Federation Services (ADFS). Or, sync the password hash from Active Directory into Office 365 using a tool called DirSync or more recently Azure AD Sync (AADSync, recently packaged as part of another tool called Azure AD Connect) ("Removing Identity Barriers for Office 365 | Okta," 2016).

ADFS is a very powerful federation platform, and a typical deployment requires at least two dedicated ADFS servers in your IT environment. At a minimum when deploying an ADFS solution, most companies end up with four new on-premises servers. In instances where there are multiple domains and forests, that number can climb dramatically. Instead of deploying ADFS, you can use the directory synchronization solution, DirSync / AADSync. This tool requires you deploy a new dedicated server that connects to your Active Directory, copies the password hash, secures it again by hashing the hash, and then stores it in Office 365. Office 365 then handles authentication requests directly, without federation. Often this approach is called "Same Sign-On." With AADConnect storing your Active Directory password hashes in Office 365, you don't need to deploy any ADFS servers and infrastructure. Sounds ideal? Well, it's a compromise. ADFS, while complicated to deploy, brings the authentication immediately to your Active Directory environment. The alternate option with AADConnect introduces a delay when copying the password to Office 365. Maintain multiple Active Directory environments? No problem, just

configure more ADFS farms. AADConnect, on the other hand, is a single server. You need to ensure reliable network connectivity between all your Active Directory domain controllers, and the single AADConnect. Not ideal. So the choices here are not very promising. Do you invest in building out and maintaining a highly scalable federated identity service with ADFS, or do you lose the benefits of true single sign-on and deploy a single server to copy your password hash into Office 365 ("Removing Identity Barriers for Office 365 | Okta," 2016)?

Each of the Office 365 services (Exchange Online, SharePoint Online, etc.) has a dedicated area for reviewing activities and logs. The type of information available in the logs is limited to what that particular Office 365 service captures and allows you to consume. In addition to the Office 365 admin portal for security settings and logs you have the ADFS and DirSync servers to review for security settings and user/admin activity logs.

When corporate services are on-premise, you have unlimited ability to audit, view, log, and capture data. Even when users are remote, if they have to use a VPN to access corporate services you have fantastic logging options. These visibility options dissipate when the business accesses cloud services directly.

2.1 Visualizing cloud traffic: Cloud Access Security Brokers

Proxies have been around in the information security industry for many years. It's one of those technologies you either love or hate. Traditionally, proxies have been leveraged as a way to improve security for corporate users accessing the Internet. When you proxy all Internet traffic, you can create a disruptive user experience. Cloud access security brokers proxy only the cloud services you configure, thus balancing security with a non-disruptive user experience.

CASBs deliver four types of functionality:

- **Visibility:** CASBs provide application control, as well as a consolidated view of an organization's cloud service usage and the users who access data from any device or location.
- **Data Security:** CASBs provide the ability to enforce data-centric security policies to prevent unwanted activity based on data classification, discovery and user activity monitoring of access to sensitive data or privilege escalation. Policies are applied through

controls, such as audit, alert, block, quarantine, delete and encrypt/tokenize, at the field and file level in cloud services.

- **Threat Protection:** CASBs prevent unwanted devices, users, and applications from accessing cloud services. Other examples in this category are user and entity behavior analytics (UEBA), the use of threat intelligence and malware identification.
- **Compliance:** CASBs assist with data residency and compliance with regulations and standards, as well as identify cloud usage and the risks of specific cloud services.

("Cloud Access Security Brokers - The New Frontier of Active Cyber Defenses | ActiveCyber," 2016)

2.1.1 20/20 Vision: Differentiation of Cloud Access Security Brokers

Cloud access security brokers are not created equal. A key differentiation among providers is what level of control they provide to select which traffic should go through the proxy. For example, being able to specify that you want both Office 365 services (Exchange Online, SharePoint Online, Skype for Business, etc.) and your cloud-based accounts payable solution traffic sent to your cloud access security broker but nothing else. The ability to control and fine-tune visibility of your cloud-based services, and no other internet traffic, is powerful.

In our scenario, you can now see all the traffic to Office 365. Now, what? Now you can apply information security policies to enforce business requirements. Let's say you want the users with corporate managed laptops to be able to have full access to the data within Office 365, including downloading files from email and sharing content from within SharePoint. But, corporate users accessing these services from a personal PC should only have read access with no ability to download files. Cloud access security broker policies can do that. You can create detailed policies that apply only to a single user or exempt specific users from policies. Different policies for each service within Office 365? No problem. You can create a policy to allow personal devices to access Skype for Business and still block personal devices from accessing your corporate intranet on SharePoint online. Android mobile device access to One Note Online can be allowed while blocking Apple mobile devices.

Sounds pretty good right? Wait, there is more to consider. Another visibility differentiation factor of cloud access security brokers is how they integrate into your corporate environment. An example of how to direct corporate traffic to a CASB is shown in Figure 2 below.

Implement reverse proxy as the primary enforcement method, and distribute the CASB endpoint agent as needed by applications that cannot otherwise be directed to the CASB gateway.

Reverse proxy : Configure cloud applications to accept service requests for the relevant account(s) only from the CASB gateway. Configure the application to authenticate users by an external single sign-on Identity Provider and configure the IdP to redirect via the CASB. Upon authentication, the IdP redirects the connection (with SAML identity assertion) via the CASB.

CASB Security Service : The recommended method of forward proxy enforcement for desktop endpoints is installing the CASB Security Service on organizational endpoints. Connections from all these endpoints' browsers and applications to asset destinations will then be automatically directed to go through the CASB gateway. The CASB Security Service has an extremely low resource impact, and provides a seamless user experience. The service is maintained with a watchdog service

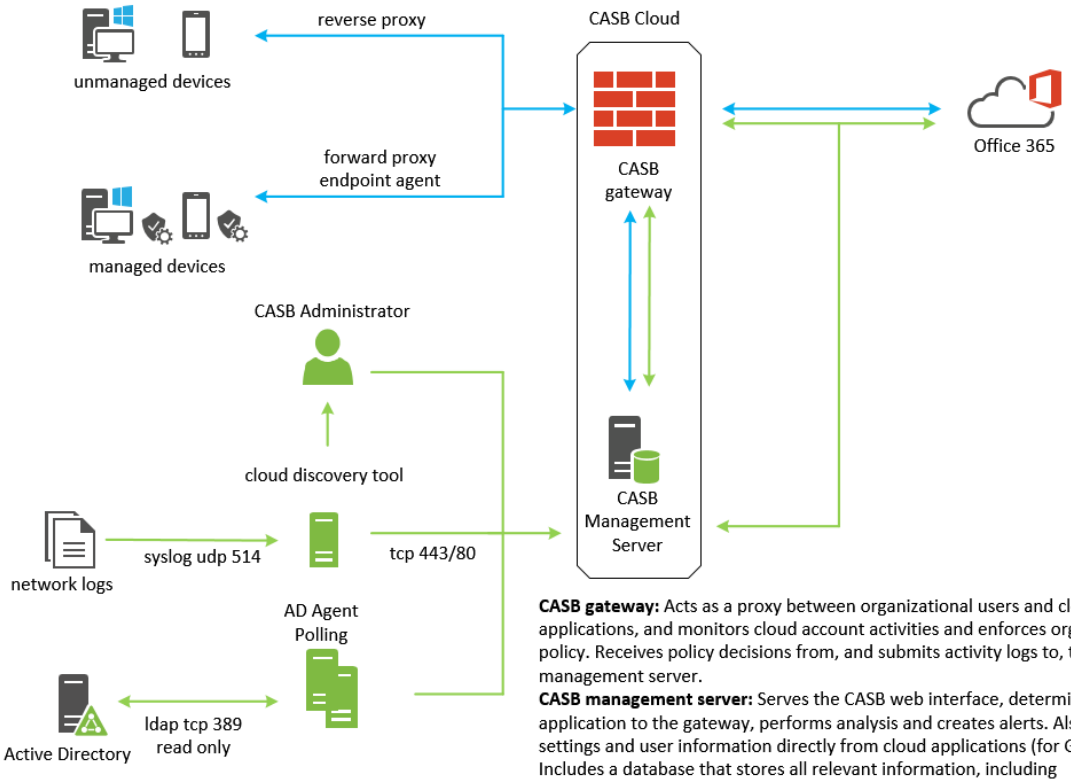


Figure 2. CASB architecture example

In the example architecture above, there are two main integration methods, a forward proxy and a reverse proxy. A forward proxy integration works by having an agent installed on endpoint devices. This agent routes traffic to the cloud access security broker and provides cloud application discovery on the endpoint device. The main benefit of this integration method is that all cloud service traffic is redirected to the cloud access security broker. Client application traffic, such as Outlook, as well as web-based traffic to cloud services, such as Exchange Online, are both routed to the CASB. The main limitation with forward proxy integrations is software installations on endpoint devices. Software installation might be suitable for corporate managed devices but what about personal devices?

Jennifer Johns, jennijohns@protonmail.com

A reverse proxy integration leverages DNS to redirect corporate cloud service traffic to the cloud access security broker. A reverse proxy can be either hosted on premise or hosted by the cloud access security broker itself. Hosting the reverse proxy on the cloud access security broker itself is recommended to remove any on-premise requirement for service availability. If the reverse proxy were to become unavailable, no users would be able to access the cloud service. Reverse proxy integration is seamless to the end user but does not support endpoint client applications such as Outlook.

The key to a successful CASB security implementation is leveraging both integration methods. Leverage forward proxy integration on corporate managed devices. Use reverse proxy integration to cover personal devices. Create custom security policies to enforce business requirements for the in-between cases, such as client applications on personal devices. With a cloud access security broker you can allow personal devices web based access to corporate cloud services and block client applications like Outlook completely. If the user is accessing the service outside corporate headquarters, you can block web based downloads from Exchange Online or SharePoint Online but still allow read access. You can exempt a user from policy in an emergency, or block a disgruntled user that was released from employment.

So this is great right? Implement a cloud access security broker and gain visibility into corporate leveraged cloud services. But wait, there is more to consider. Let's continue with our scenario and focus on a key visibility component, authentication. In our use case scenario, active directory federation services (ADFS) with DirSync are used to populate the on premise active directory accounts to Azure Active Directory so users can use their domain accounts to log in to Office 365 services. To leverage the functionality of ADFS with Office 365 for other cloud services, and centralize its operational management, you have one choice. Say hello to cloud identity and access management.

2.2 The Eye Witness: Cloud Identity and Access Management

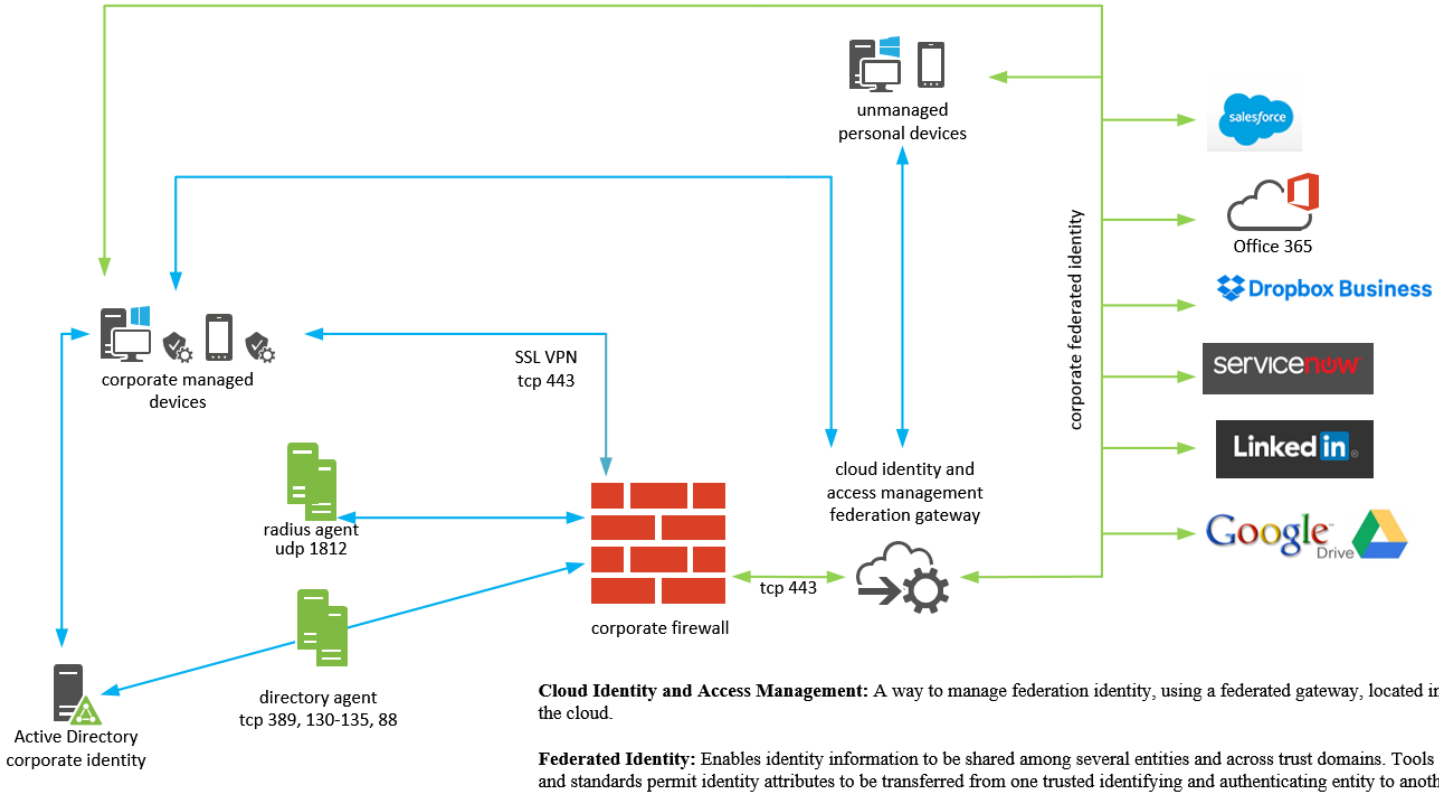
When someone comes to the front door of your house, they knock, you answer, and only if you know who they are do you let them in your home. A cloud identity and access management solution is a security guard at the front door, an eye-witness, validating the users trying to get in actually are who they say they are. Direct cloud access to corporate resources requires strong

identity and access management for user validation. It seems obvious that visibility of users accessing cloud services is critical to information security in the cloud, but how is this different than the visibility that a cloud access security broker provides? Good question. Let's discuss.

You can think of cloud identity and access management solutions as the "who", and cloud access security brokers as the "what, when, and where." Cloud identity and access management services centralize the operation of who is allowed to access all of your corporate cloud services. Active Directory login credentials are no longer stored at each cloud service provider, they are federated with the cloud identity and access management provider, and then all cloud services the business integrates with leverage that single copy of your directory to allow users seamless access using their corporate domain credentials. You can control access to each cloud service based on active directory group membership. You can enforce strong authentication by leveraging multi-factor authentication. Multi-factor authentication across all cloud services, as well as VPN, will be standardized.

2.2.1 20/20 Vision: Differentiation of Cloud Identity and Access Management Solutions

As we previously discussed, not all cloud services are alike including cloud identity and access management. CIAM is a core cloud infrastructure component and should always be available, secure, and adaptable to new technologies and services as they emerge. Figure 3 below is an example of a cloud identity and access management architecture.



Cloud Identity and Access Management: A way to manage federation identity, using a federated gateway, located in the cloud.

Federated Identity: Enables identity information to be shared among several entities and across trust domains. Tools and standards permit identity attributes to be transferred from one trusted identifying and authenticating entity to another for authentication, authorization and other purposes, thus providing "single sign-on" ("Federated Identity Management - Gartner IT Glossary," n.d.).

Federation Gateway: Is an architectural option where the enterprise externalizes its federation implementation. Using this method, organizations can delegate issuing various authentication token types to the federation gateway, so the gateway handles the core work of translating tokens from one format to another (Cloud Security Alliance, 2010, p.18).

Figure 3. CIAM architecture example

In the above example architecture of a cloud identity and access management (CIAM) solution, the directory agent communicates internally to the Active Directory forest using LDAP over TCP 389, AD over TCP 135-139, and Kerberos over TCP 88. Outbound, the directory agent, communicates through the corporate firewall via an HTTP request over port 443 to the CIAM federation gateway service. This allows the directory agent and the CIAM federation gateway service to mutually authenticate and establish a transport layer security (TLS) channel without requiring an inbound "hole" in the corporate firewall. TLS channels are encrypted using asynchronous keys, a process that protects data in transit from unauthorized interception and disclosure. The AD agent enables delegated authentication and user provisioning from AD to the CIAM and vice versa ("Okta Security: Technical White Paper | Okta," 2015).

The radius agent is used to provide multi-factor authentication to end user client VPN sessions. It communicates internally to the corporate firewall using radius over UDP 1812. The

radius agent communicates outbound through the corporate firewall via an HTTP request over port 443 to the CIAM federation gateway service. Just like the directory agent, this allows the radius agent and the CIAM federation gateway service to mutually authenticate and establish a transport layer security (TLS) channel without requiring an inbound “hole” in the corporate firewall. The radius agent enables delegated authentication from AD to the CIAM and vice versa.

Cloud Access Security Brokers handle client applications differently than web applications, so do Cloud Identity and access management solutions. Using a federated identity to log into a client application, like Outlook for Office 365, requires a feature called Desktop Single Sign-On. With a web application, you can use one of two methods, leverage the federation identity to log in manually with the username and password from the Windows domain or leverage Integrated Web Authentication (IWA) protocol to automatically log users into an internal web application, for example, the company intranet site on SharePoint Online.

Desktop single sign-on extends local users Windows domain login procedures to grant access to the Cloud Identity and Access Management solution and their cloud applications. In a Windows environment, the directory agent uses Microsoft's Integrated Windows Authentication to authenticate users seamlessly who have already authenticated via their Windows domain login ("Okta Directory Integration - An Architecture Overview | Okta," 2013).

When an internal web application is configured to delegate authentication, the cloud identity and access management solution leverages IWA to capture the user’s AD/LDAP password at login and automatically set that password for that user in any application that also delegates to AD or LDAP. This allows users to simply click a link to access these applications, and then be logged in automatically ("Okta Directory Integration - An Architecture Overview | Okta," 2013).

Another key differentiation factor among cloud identity and access management solutions is "de-provisioning". With CIAM you can centralize user deactivation. De-provisioning works by deactivating a user in Active Directory. Once a user is deactivated in AD, the CIAM deactivates access to cloud applications. You can configure administrator alerts to email out reminders to deactivate user access that is required to process manually as well.

3 Conclusion

Despite their many advantages, cloud-based applications can bring a loss of visibility and control. Unauthorized access through employee credential misuse and improper access controls, hijacking of employee accounts, and malicious insiders are all risks that are outside the scope of the cloud service provider. Businesses must provide their own security practices when using cloud services.

Cloud Access Security Brokers and Cloud Identity and Access Management solutions are two critical security products that can help reduce the risk of a security breach in the cloud. These solutions give information security professionals visibility and control over how, and what, is being accessed in the cloud, and who can, and is, accessing that data.

Cloud security is your responsibility. Change your perspective on information security in the cloud. Take control with Cloud Access Security Brokers and Cloud Identity and Access Management.

"Ultimate excellence lies not in winning every battle, but in defeating the enemy without ever fighting."

Sun-Tzu
(Sunzi & Minford, 2003, p. back cover)

Jennife

References

Sunzi, & Minford, J. (2003). *The art of war*. New York, NY: Penguin.

Cloud Access Security Brokers (CASBs) - Gartner IT Glossary. (n.d.). Retrieved from http://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs/

Cloud Security Alliance. (2010). *Domain 12: Guidance for Identity & Access Management V2.1*. Retrieved from https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf

Identity Management - Access Management - Gartner Research. (n.d.). Retrieved from http://www.gartner.com/it-glossary/identity-and-access-management-iam/

Federated Identity Management - Gartner IT Glossary. (n.d.). Retrieved from http://www.gartner.com/it-glossary/federated-identity-management/

Cloud Access Security Brokers - The New Frontier of Active Cyber Defenses | ActiveCyber. (2016, February 1). Retrieved from http://www.activecyber.net/cloud-access-security-brokers-the-new-frontier-of-active-cyber-defenses/

Kumerow, L. (2015, April 24). Why CASBs are essential for enterprise cloud security. Retrieved from https://blog.code42.com/cloud-access-security-brokers-enhance-data-loss-prevention/

Avoid the Hidden Costs of AD FS with Okta | Okta. (2015, October 23). Retrieved from https://www.okta.com/resources/whitepaper-avoid-hidden-costs-of-adfs/

Removing Identity Barriers for Office 365 | Okta. (2016, February 6). Retrieved from https://www.okta.com/resources/whitepaper-remove-identity-barriers-O365/

Williams, A. (2015, September 18). Visibility: The Key To Security In The Cloud. Retrieved from http://www.darkreading.com/risk/visibility-the-key-to-security-in-the-cloud/a/d-id/1322240

Evans, S. (2016, June 15). Gartner Predicts Top Ten InfoSec Technologies - Infosecurity Magazine. Retrieved from http://www.infosecurity-magazine.com/news/gartner-predicts-top-ten-infosec/

Howarth, F. (2014, September 2). The Role of Human Error in Successful Security Attacks. Retrieved from https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/

2016 DBIR: Understand Your Cybersecurity Threats | Verizon Enterprise Solutions. (n.d.). Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Okta Security: Technical White Paper | Okta. (2015, October 27). Retrieved from https://www.okta.com/resources/whitepaper-okta-security-technical-white-paper/

Okta Directory Integration - An Architecture Overview | Okta. (2013, June 25). Retrieved from https://www.okta.com/resources/whitepaper-ad-architecture/

Security in the cloud. (n.d.). Retrieved from https://www.themissinglink.com.au/news/security-in-the-cloud

What is the Difference between Speed, Velocity and Acceleration? (n.d.). Retrieved from http://www.edinformatics.com/math_science/acceleration.htm/

Identity Management - Access Management - Gartner Research. (n.d.). Retrieved from http://www.gartner.com/it-glossary/identity-and-access-management-iam/

Jennifer Johns, jennijohns@protonmail.com

Visibility: The Key To Security In The Cloud. (n.d.). Retrieved from http://www.darkreading.com/risk/visibility-the-key-to-security-in-the-cloud/a/d-id/1322240