RSA Conference 2019

BETTER.

Peer2Peer

Cloud Access Security Broker Best Practices

P2P3-R14: Cloud Access Security Broker Best Practices

Joshua Atencio, Senior Information Security Engineer, Aetna

Cloud Access Security Broker Best Practices

Cloud Access Security Brokers (CASB) have become a topic of discussion with the shift to the cloud in today's world. I often hear questions about the value of a CASB. How do I utilize it? What are some best practices? At RSA Conference 2019 I had the pleasure of hosting P2P on best practices regarding how to implement and utilize a CASB to its full benefit.

As I talked to attendees as they came into the room, I identified two reasons why they chose this P2P. The first group came to learn how others are using a CASB and develop new use cases and discuss existing use cases. The second group came to learn about the benefits of a CASB whether they were in the proof of concept phase, recently purchased a CASB, or figuring out if they even need a CASB. So, this made for an interesting but great P2P because most of the attendees fell into the second group and came to learn from others.

We broke this P2P down into two areas of focus: securing Sanctioned Services and Unsanctioned Services with a CASB. Sanctioned services are services the enterprise has paid for and is an approved cloud service. Unsanctioned services are more shadow IT specific these are cloud services your users could be using without your organization's knowledge.

The first topic was "How do you manage down your Unsanctioned Services. Like Shadow IT or something that your company doesn't have an enterprise license for where you inherit security controls?" After discussion the main three points were:

- Understanding the risk profile of your company and tuning the risk attributes within your CASB on how it assesses cloud services. This is a core foundational piece.
- Take action on the data your CASB provides. Block access to high risk services that were identified by your CASB via a web proxy, forward proxy, firewall. Find where your high usage of cloud services is to better use money and resources to secure the ones with high usage.
- Track your progress through KPIs (e.g., average cloud services risk score, spike in usage of cloud services, number of high-risk services blocked).

The second topic was "How do you best secure sanctioned cloud services such as O365, AWS, Salesforce, Box, etc.? "

- API connections to cloud services was the most widely used. Attendees say it was the easiest and most flexible way to implement the CASB security stack (e.g., DLP, Config Audit, User Activity Monitoring) in the cloud services without having to deploy another network appliance in their network.
- There were also some attendees that use an inline deployment. Specifically, reverse proxy which gives users the ability to have device management type of controls. As such, only managed devices can access these cloud services or unmanaged devices can only view cloud services but can't download any content.

Overall this was a great P2P discussion. Many different use cases and best practices to get started were shared. There was a little bit of everything for everyone whether they were just starting their CASB journey or far down the road in the journey. I also enjoyed seeing people exchange information after the session and build relations that will help them along the journey.