Cloud Access Security Broker

CASB

- So, what is CASB?,
  - CASB, stands for Cloud Access Security Broker, a term that has been coin by Gartner
  - According to Gartner, CASBs are security policy control points
    - Placed between users in your organization and the cloud.

- Gartner believes that there is 3 ways in which you can deploy CASB:
  - The first is a proxy like on-prem gateway.
  - The second a host-based agent.
  - And the third one, an API-centric, cloud solution.

CASB

- Current market trends shows a driving dissolution of the network perimeter.

- Users are everywhere,

  - Using unmanaged devices and connecting to on-premise and cloud applications

  - making network edge solutions such as FW, IPS/IDS, Network Proxies to become less than idea.

CASB

- Gartner classifies CASB functionality into four pillars.
- Visibility
  - Who is accessing what applications?
  - What are unmanaged users doing?
- So we can say that visibility in CASB provides:
  - Shadow IT discovery and sanctioned application control
  - Consolidated view of an organization's cloud service usage and the users who access data from any device or location.

CASB

- Compliance
  - Are there any over privileged users in my systems?
  - Are my access keys non-compliant?
  - Or is my DevOps practices compliant?
- CASB can assist with data residency and compliance with regulations and standards, as well as:
  - Identify cloud usage and the risks of specific cloud services.

CASB

- Data Security
  - For data security, CASB provides the ability to enforce data-centric security policies, things like:
    - Who is sharing data in the public cloud?
    - Am I fulfilling the shared security responsibility?
    - Are there any security holes in my DevOps?
- The idea is to prevent unwanted activity based on:
  - Data classification, discovery and user activity monitoring of access to sensitive data or privilege escalation.

CASB

- Threat Protection
  - Who are risky users in my systems?
  - How fast can I stop risky user activities?
  - or How fast can I stop risky applications?
- With threat protection, we try to prevent:
  - Unwanted devices, users and versions of applications from accessing cloud services.
  - Other examples in this category are user and entity behavior analytics (UEBA),
  - or the use of threat intelligence and malware identification.

Cloud Provider CASB

- Cloud Provider monitors:
  - Activity, configurations, transactions and content for IaaS, PaaS, and SaaS services.
- App-to-App and some are BYoD-ready.
- Full security automation:
  - including capabilities to Predict, Prevent, Detect and Respond.
- With secure provisioning:
  - Offer continuous protection of applications through its entire lifecycle.