Dear [BOSS, DECISION-MAKER, COMMITTEE],

Please accept this recommendation that [ORGANIZATION] deploy a Cloud Access Security Broker. [INDIVIDUALS OR COMMITTEE NAME] has put a great deal of effort into this recommendation, including a thorough review of our cloud environment and cloud policy, synthesis of third-party research such as the Gartner Market Guide for Cloud Access Security Brokers, delivery of a cloud risk assessment, and evaluation of the leading CASB vendors in the industry.

As a reminder, Gartner defines CASB as “security policy enforcement points placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.” Gartner also articulates four critical capabilities that CASBs provide: **visibility**; **compliance**; **data security**; and **threat protection**.

**Cloud Consumption**

Our organization is adopting the cloud across all of our functions and lines of business. From Finance to HR to Marketing, we are using cloud services such as [THREE EXAMPLES]. According to the Netskope Cloud Report, the average enterprise has 977 cloud services in use. We have [NUMBER]. Centrally, we are deploying [OFFICE 365, BOX, ETC.]. Beyond that, our lines of business are taking advantage of new tools to stay competitive and efficient, and virtually all of these tools are in the cloud. Gartner predicts that more than $1 trillion in IT spend will shift to the cloud by 2020; we are already seeing evidence of this shift in our business.

**Lack of Visibility**

As our productivity tools move to the cloud, our security tools and processes need to accommodate that shift. Today, we have little or no visibility into what cloud services are being used, much less the ability to audit usage and detect things like data leakage or exfiltration. Having a CASB in place would give us the ability to understand at a deep, contextual level what cloud services we’re using and what our real risk is.

**No Policy Compliance**

Beyond visibility, we also can’t enforce policies such as different access levels to users on managed devices versus BYOD, govern cloud activities such as “share” and “download” for users in different directory groups or organizational units, and control activities and data in different instances of the same app (like our corporate version of OneDrive or Box versus the many personal instances that users access). Our perimeter tools cannot address these use cases, but a CASB can.

**Risk of Data Loss or Exposure**

Our lack of visibility means we cannot see whether and how much sensitive or regulated data we have in our sanctioned or unsanctioned cloud services. We need to be able to find and protect sensitive content in our sanctioned apps as well as detect sensitive content on its way to unsanctioned apps and take action like block the activity or encrypt the content on-the-fly. Up to now, many organizations have responded to this risk by blocking cloud, but by all measures this tack is ineffective as it creates an “exception sprawl” problem and forces users to find an alternative (often lower-quality) service, forcing us into a game of whack-a-mole. Instead, a CASB would help us safely enable a set of reasonable cloud services, as well as monitor and control the rest in a granular way.

**Cloud Malware and Other Threats**

According to a recent study from Netskope and the Ponemon Institute, one out of three organizations has cloud malware and doesn’t know it. Moreover, 31 percent have experienced one or more data breaches involving cloud. Hackers are going where the data are, and today that’s cloud. We’re seeing a growing number of malware and ransomware incidents involving cloud, and we believe that’s because malware can hide in plain sight in many cloud services, and organizations can’t protect themselves because they either don’t know about the cloud service or they’re not inspecting it when it comes into the network because SSL inspection impacts performance. Having a CASB in place that can detect and remediate malware in the cloud, as well as alert the rest of our security infrastructure, will go a long way in protecting us against threats.

In summary, our cloud usage and risk profile point to an urgent need to invest in a CASB. This will allow us to say “yes” to the tools our users need while enabling us to protect our data and achieve compliance.

Thank you for your consideration.

Sincerely,

XYZ