



5% CASB market penetration to **85%** by 2020 (Gartner)

CLOUDSOC: THE RIGHT CASB FOR YOU

The Symantec CloudSOC platform enables companies to confidently leverage cloud applications and services while staying safe, secure and compliant. It provides visibility into shadow IT, governance over data in cloud apps, and protection against threats targeting cloud accounts.

Everyone is going to the cloud for cost and agility reasons, the problem is a lack of visibility and control. There is a need for a single pane of glass to help manage risk in public cloud – that is what a CASB does.

CASB is the most effective technology to overcome compliance and risk challenges in the adoption of public cloud. Symantec have the highest rated CASB on the market and the only one that can enhance the value of existing Symantec DLP, ProxySG, SEP and a whole host of other products.

For example, Symantec's CASB stands out from its competition by being proactive rather than reactive with its full integration with PROXY SG. Also, it works seamlessly with Symantec's DLP providing a faster and smoother customer experience whereby users don't have to leave the Symantec DLP interface.



By 2020 **95%** of cloud data losses will be due to employees (Gartner)

TARGET MARKET



Customers leveraging **Office 365, Google for work, Salesforce** and others



Customers using **Symantec DLP** today



Customers leveraging a wide array of **cloud apps**



Customers with **iCloud app monitoring projects**

THE BUSINESS NEED

What does CASB do? Classify and control data in public cloud applications and prevent risky user behaviour so that more cloud can be used.

1. Shadow IT: "Find what cloud apps my users are accessing, how risky they are and if we are being GDPR compliant."

2. Shadow Data: "Allow me to see where sensitive data is going into SaaS apps, (like Office 365, Box and OneDrive) and help me control sharing".



CASB was the **number 1 fastest growing security technology** in 2015, 2016 and 2017 (GARTNER)

WHY ENTERPRISES NEED CASB

Protect against leaks of confidential information

Cloud control and visibility

Detect unusual or fraudulent activities

Detect and eliminate malware

Detect, monitor and control unsanctioned cloud use

Aid investigation of suspicious users and incidents

Prevent cloud application lock in

WHO SHOULD YOU BE TALKING TO?

In a nutshell, you need to find the people who care about data loss. Go as high as you can because the final decision is made or approved at the executive layer or CISO.

What CISOs care about:

- ✓ The transition to cloud has introduced a number of security and compliance issues
- ✓ I want to prevent loss of confidential data in cloud apps
- ✓ I'd like to leverage the investment I've already made in Symantec DLP

Often more than one department is involved in the purchase, so nurture your relationship across departments:

- ✓ **Department VPs/Directors** - IT Security (IT Security Architect), InfoSec, Network IT/Security (Network Security Architect), DLP (DLP Manager), Risk & Compliance, Info Recovery
- ✓ **Cloud application owner**
- ✓ **The GDPR Team**

DISCOVERY QUESTIONS

- ▷ How do you gain visibility of the cloud applications being used in your organisation?
- ▷ Can you see where your data is? Is it sensitive?
- ▷ How is your data being shared?
- ▷ Are former employees still accessing cloud applications or have access?
- ▷ Can you detect and prevent malicious activity?
- ▷ Do you already use any Symantec or Blue Coat products?
If DLP; would you like to extend your DLP to govern confidential data in cloud apps?

THE TWO OBJECTIONS YOU MAY COME ACROSS

Objection: "I have CASB capability with Microsoft already"

Response: "Do you have M365 E5 or O365 E5? If not, then you don't get it included"

Objection: "It's too hard to justify the expense"

Response: "We would like to offer you a free no obligation Shadow IT or Shadow Data assessment to help you prove there is a need to your business"

How does Symantec CASB compare to the competition?

Symantec CASB are the leaders for both Gartner MQ and the Forrester Wave.

Gartner MQ Source: Gartner, Inc., Magic Quadrant for Cloud Access Security Brokers, Steve Riley, Craig Lawson, November 30, 2017

Forrester Wave Source: November 2016, The Forrester Wave™: Cloud Security Gateways, Q4 2016 *Blue Coat (acquired by Symantec) was evaluated in the Forrester Wave report.

How does Symantec's CASB compare to Microsoft and McAfee?



Microsoft has a more expensive price point compared to the Symantec CloudSOC solution and is graded as a niche player by Gartner MQ. Microsoft license O365 Cloud App Security for use with O365 within M365 and O365 E5 (NOT E3).

Disadvantages to Microsoft:

1. **Inconsistent data catch rate** which results in sensitive data being missed.
2. **No roles based access control** which is problematic for international customers.
3. **No forward proxy** which leads to no capability to identify personal cloud apps in use, encryption of data, geo-location or real-time control.



McAfee Skyhigh Security Cloud have a reputation of being expensive in the market and the latest reports show that McAfee are struggling with the sales integration of Skyhigh.

The McAfee audit module is good and comparable to Symantec CASB however their cloud app API control is lacking in comparison in the following areas:

1. **Low number of cloud apps supported**
2. **Low level of functionality can be offered**

CROSS-SELL OPPORTUNITIES

- ✓ **Data Loss Prevention** - Symantec DLP for Cloud Content
- ✓ **Web Security** - ProxySG & WSS for Shadow IT Control

- ✓ **ATP** - Malware, Crimeware, Ransomware & Sandboxing for Cloud Content
- ✓ **Encryption** - User-based selective encryption for Cloud Content

- ✓ **User Authentication** - VIP Access MGR (SSO) & Adaptive Authentication
- ✓ **Endpoint Security** - Symantec Endpoint for Shadow IT Visibility