Cloud Access Security Broker Keeping Confidential Information Confidential

In the past few years, the use of personal cloud storage has been on the rise, from GoogleDrive to Dropbox and even Microsoft Onedrive. These cloud storage options allow users to share data across computer systems, and while this can be seen as a boon in productivity for employees, these cloud storage services can become an IT security nightmare nearly overnight. Users and more importantly, employees have these services installed on their personal cell phones, personal computers, and even their work computers.

Malicious or Accidental Exfiltration of Company Data?

Every company has different policies on how data is to be handled, these policies are only as good at the tools and prevention measures that monitor and block malicious, or ignorant use by employees. While a company may have measures in place to monitor malicious use or exfiltration of files and information, are they monitoring every possible aspect? USB devices may be disabled but does the company have a way to monitor cloud storage or even data stored in the cloud? Who has access to the cloudstorage, that a company's confidential data may be saved to? How would a company even know if their data was being saved to cloud storage by malicious or even well-meaning employees?

Even well-meaning employees can create compliance violations, a nurse or medical transcriptionist saving patient data within the cloud on a personal storage account, could lead to hefty fines as well as possible loss of contracts or abilities to bid on future projects for the company. The average HIPAA fine currently being 1.5 million (a), so these types of slip-ups can and have cost companies greatly.

BYOD is a lurking issue for cloud storage

More companies are switching to BYOD, or Bring Your Own Device, and allowing users to have access to the company's networks and data with their personal devices (b). These devices often mobile devices, usually come preloaded with cloud access, be it Google Drive with Android devices, or icloud with Apple devices. While the rise in productivity seems to benefit companies, the potential loss of confidential or proprietary data is greater with this policy.

How to guard against this?

The answer to these problems is a simple one, CASB or Cloud Access Security Broker. "Cloud access security brokers" (CASBs) 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. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on (c)."

Essentially, a guardian of your companies data that alerts and forbids sensitive company, personal, or proprietary information from being loaded onto unsanctioned cloud services.

These systems achieve this goal in different ways, from scanning the information that is passed through the network, to checking the hashes of the files and information passing through the CASB. In the case of Netskope, a popular CASB solution, as well as several others, even the use of steganography is not enough to get past the system and exfiltrate data.

Cloud DLP

All data stored within the cloud is not scary; however, it is still vulnerable to the same issues with security. Companies that have adopted the practice would be relieved to know that many of the big players in the CASB market offer a form of cloud DLP.

Cloud DLP specifically protects the companies that have moved to cloud storage by ensuring sensitive data is not stored on the cloud without first being encrypted, and is only sent to the authorized cloud services. These Cloud DLP options will either alter or altogether remove the classified or sensitive information before it comes in contact with the cloud.

Some of the key benefits of this cloud DLP include:

- Integration with cloud storage to scan servers, and then identify and encrypt data
- Continuous audit of uploaded information
- Instantly alert the proper administration when data has been put at risk.

Think of Cloud DLP as having a virtual security guard that checks the receipts of users taking files out into the world of the internet, and ensuring nothing gets taken that has not been approved.

> *“…these cloud storage services can become an IT security nightmare nearly overnight.”*

The Big Players in CASB

According to the Gartner Magic Quadrant, there are four big players currently in the CASB market:

- Netskope offering multiple built-in and tenant-specific threat intelligence feeds.
- McAfee with their recently acquired Skyhigh Networks offering the ability to create Data Loss -Prevention Policies without the need for coding, allowing a recording extension to observe the behavior as the app is invoked.
- Bitglass offering the ability to include enterprise digital rights management within their Data Loss Prevention policies.
- Symantec offering a large range of predefined DLP selectors based on compliance, and other common factors.

Resources

(a) Sivilli, F. (2018, September 17). Average HIPAA Violation Fine now $1.5 Million. Retrieved from https://compliancy-group.com/average-hipaa-fine-is-now-1-5-million/

(b) BYOD Statistics Provide Snapshot of Future. (n.d.). Retrieved from https://www.insight.com/en_US/learn/content/2017/01182017-byod-statistics-provide-snapshot-of-future.html

(c) Cloud Access Security Brokers – CASB – Gartner tech definitions. (2018, February 08). Retrieved from https://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs/