ARTICLE

Extend Your DLP to the Cloud

Symantec™

Introduction

Times have changed. Traditional DLP coverage – network, email, and endpoint – cannot fully protect organizations against the leakage of sensitive or compliance related data. With the widespread adoption of cloud apps and services, a new threat vector has emerged that necessitates the extension of DLP capabilities into the cloud. And since organizations still have an obligation to comply with relevant regulatory requirements like PCI, DSS, and HIPAA standards when data leaves the network perimeter, the need for consistent DLP policies on-prem and in the cloud is critical.

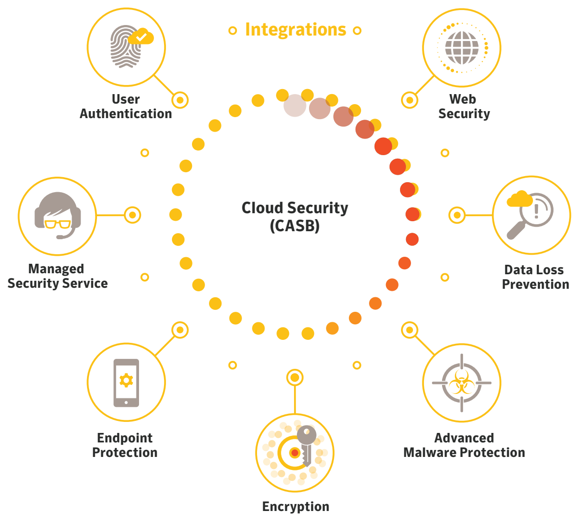
Given that cloud DLP necessitates a fundamentally different approach to data loss due to different sharing semantics, etc., addressing this challenge is not straight forward. While the first generation of Cloud Access Security Broker (CASB) solutions partially addressed this problem by providing DLP capabilities designed specifically to address cloud requirements, they also introduced additional complexity and management overhead into the network security environment as IT departments struggled to build and maintain a separate set of DLP policies and remediation workflows in the cloud. Early attempts to eliminate this overhead through integration with on-prem DLP had its own set of problems as it introduced unacceptable amounts of latency and still necessitated separate management and reporting consoles.

This article will address the limitations of traditional DLP and CASB, and discuss the need for a CASB 2.0 solution that quickly, simply, and effectively extends on-prem DLP into the cloud through seamless integration with your existing security architecture.

Limitations of Traditional DLP Solutions

Traditional DLP solutions do not provide the best security in the cloud because they face four critical limitations:

- **Lack of basic visibility into SaaS applications on mobile devices:** Traditional DLP can only monitor traffic on enterprise-controlled assets (e.g., networks/endpoints) but are blind, for instance, to a mobile user, using a native mobile application, going direct-to-net over a mobile network. The only option is to backhaul traffic, introducing additional cost and latency.
- **Failure to interpret encrypted traffic:** Traffic to and from SaaS applications is typically encrypted (e.g., transmitted over SSL/TLS). Therefore, unless a separate SSL inspection capability is purchased, traditional DLP solutions alone will not be able to interpret the underlying content.
- **Inability to interpret links to data:** Traditional DLP solutions process raw data directly. However, data is never being directly shared in SaaS file sharing apps. Instead, what is being shared is some type of link (e.g., a URL) to the content. What must be done, therefore, is to analyze the content being pointed to by the link, which is not something that traditional DLP solutions can do.
- **Use of "perimeter defense" sharing semantics:** Traditional DLP sees data leakage as the crossing of data across the enterprise perimeter. For SaaS file sharing applications, data loss is different for two reasons. First, data hosted with a SaaS provider is already outside the enterprise network and can be shared with third parties who are also outside the network. Second, data in a SaaS application is shared on a per-user basis. For example, if you want to share a file with someone else, you can typically do so by simply entering that person's email address or the username they use for the SaaS application. Traditional DLP solutions do not understand these sharing semantics, and cannot assess if data is being leaked.



The CASB 2.0 Solution

Limitation of Cloud DLP Using CASB 1.0

Cloud DLP provided by the first generation of Cloud Access Security Broker (CASB) solutions addressed the cloud limitations of on-prem DLP listed above, but typically didn't provide DLP coverage that was as comprehensive. Cloud DLP typically faced three primary limitations:

- **Use of rudimentary detection methods:** DLP vendors have been honing the sensitive data detection capabilities of their solutions for over a decade and have developed extensive, flexible methods that can be layered for more accurate and effective detection of sensitive data. Many CASB solutions still rely on rudimentary detection methods, such as regular expression pattern matching, which often prove to be false-positive prone, though the best ones also apply data science and machine learning to the problem.
- **Inconsistent policies and workflows between on-prem and cloud:** To maintain consistent security, no matter where your sensitive data resides, the same policies must be enforced at all times. The only alternative to spending extra effort replicating on-prem policies in the cloud was to integrate your CASB 1.0 solution with on-prem DLP using ICAP, which introduces unacceptable levels of latency.
- **Introduction of unwanted policy deployment and management overhead:** If you already have an on-prem DLP solution, you have spent many hours building and refining your DLP policies and workflows. If you select a CASB 1.0 solution, you will need to rebuild all of these policies from scratch in the cloud—and continue doing duplicative work every time a new policy is added. In addition, these systems will still require different management consoles for on prem and cloud DLP.

The CASB 2.0 Solution

In order to protect your cloud apps and data no matter the user, location, or access device, your CASB needs to integrate natively with your DLP, endpoint management, web security, encryption, adaptive authentication and other existing security investments. Ultimately you want the same peace of mind in the cloud that you've come to trust from your existing security infrastructure – without having to rebuild an island of security just for the cloud. Known as CASB 2.0, these solutions should natively integrate, and leverage common management consoles and APIs.

Top 6 Reasons Why You Need to Integrate Your On-Premise DLP with CASB Cloud DLP

1. Intro: CASB 2.0
a. What is DLP + CASB?

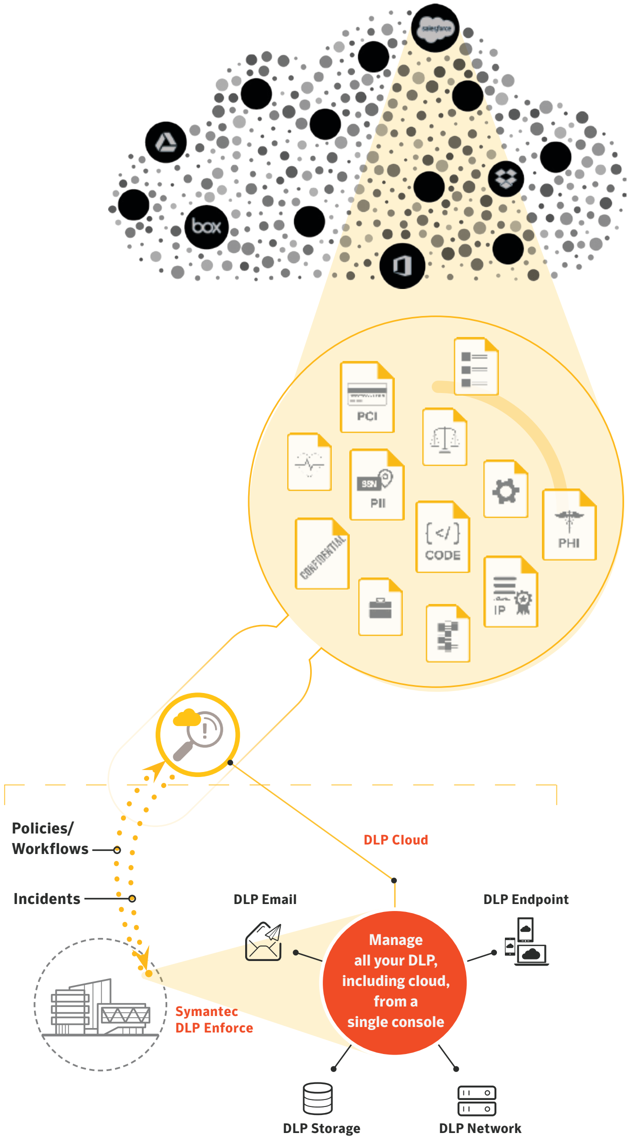
2. Gain granular CASB visibility and controls; detailed visibility of user activity in the cloud, alerts to risky behavior, and controls to prevent inappropriate sharing

3. Consolidate multiple islands of DLP: reduce complexity and gain consistent control on prem and in cloud

4. Centralized management: on-prem and cloud: Reduce administrative over head

5. Enforce consistent DLP Policies. No need to rebuild policies from scratch.

6. Leverage seamless remediation workflows



CASB 2.0 and DLP

Integrated Data Loss Prevention is a key component of CASB 2.0. When selecting a CASB 2.0 solution, you should choose one that will provide all of the benefits of on-prem DLP and the cloud DLP capabilities of CASB 1.0, without their limitations. CASB 2.0, integrated with DLP should provide:

- **Consistent DLP policies on-prem and in the cloud:** Your CASB 2.0 must be able to leverage your existing DLP policies and workflows to extend your finely tuned rules sets and business logic to cloud apps.
- **Seamless integration, without impacting performance:** a streamlined solution with a native cloud-based API integration between its DLP and CASB 2.0 solutions will provide a user experience that doesn't impact performance, and provides rick remediatopn options, unlike ICAP.
- **Granular CASB visibility and controls:** CASB 2.0 solutions must, like CASB 1.0, provide detailed visibility of user activity in the cloud, alerts to risky behavior, and controls to prevent inappropriate sharing. This information should be integrated with your DLP solutions as well.
- **Centralized management:** CASB 2.0 integrated with your DLP should enable you to manage on-prem and cloud DLP from one console where you can enforce policies and workflows everywhere.
- **Optimized performance:** When your DLP is seamlessly integrated with your CASB 2.0 solution, the combined solution enables rich policy actions and eliminates inefficiencies incurred when shuttling content between the cloud and on-prem hardware.

Conclusion

With the rise of cloud, your sensitive and compliance related data is at risk now more than ever. Nether your on-prem DLP nor your first generation CASB solution can ensure that your data remains secure whether in the cloud, in-transit or within your network perimeter. Only a CASB 2.0 solution will enable consistent DLP policies everywhere it travels, without impacting performance.

CASBs should not be an island but the control point for cloud application activity that leverages and is leveraged by the extended security capabilities. Those integrations may include:

- CASB + DLP (Extending on Prem DLP policies and workflows to the Cloud)
- CASB + SWG (Going beyond App visibility to get control)
- CASB + Authentication (Achieving intelligent, adaptive access control)
- CASB + Encryption/Tokenization (Building more effective security in the cloud for your compliance related data)
- CASB + Endpoint (Gaining Shadow IT visibility and control beyond the network perimeter)
- CASB + ATP (Protecting your data from advanced threats in cloud accounts.)

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com