WHITE PAPER

Cloud App Security with Symantec® DLP Cloud

Securlets and Gatelets: API and Inline Inspection

KEY BENEFITS

Gain Granular Visibility across SaaS and IaaS Apps
Gain visibility into user activity across a broad range of sanctioned and unsanctioned cloud apps and services, such as Office 365, Google Workspace, Box, GitHub, AWS, GCP, and Azure.

Protect Your Sensitive Data in the Cloud
Prevent data loss in the cloud with CloudSOC CASB by identifying sensitive data, monitoring data at rest and in motion, and enforcing policy controls to prevent a data breach.

Ensure Compliance
Automate the classification of PII, PCI, PHI, and other regulated data flowing in and out of cloud apps, and enforce controls that align with corporate policies.

Understand and Prevent User Risk
Security Incidents happen. Get the what, when, who, and how information that you need to respond quickly to a security event in the cloud. Correlate key information (violations, users, accounts, and assets) to assign risk scores to users and incidents using CloudSOC CASB's UEBA and machine learning capabilities, allowing you to adaptively detect high risk user activity with policy controls to alert, quarantine, or block.

Secure the Cloud against Malware
Defend against malware and ensure employees are not introducing or propagating them through cloud services.

The Challenge of Securing Sanctioned and Unsanctioned Apps

As your organization moves to adopt popular cloud apps and services such as Office 365, Google Workspace, and Salesforce, IT needs a way to apply security risk and governance controls around information that will reside in these cloud applications.

Organizations are often blind to what cloud apps and services their users are accessing (known as Shadow IT). More importantly, they are also blind to what users are doing inside cloud apps. For example, organizations might not know what sensitive content is being uploaded and shared internally and outside the organization.

In addition, organizations need to inspect cloud content for both malware and sensitive data. This content may be static (at rest) or being moved between applications (in motion). There are two main approaches to inspect content within apps and between apps: either API based or inline inspection. The API approach monitors the files at rest in apps, while the inline approach monitors files in motion.

Gartner advises firms to explore CASB systems that provide a range of architectural choices to accommodate all cloud access situations. The adaptability provided by a multi-mode CASB enables enterprises to increase their cloud security as their requirements change. DLP Cloud offers this multi-mode approach, reducing concerns about data security and compliance through the adoption of API inspection (using Securlets) and inline inspection (using Gatelets).

Securlets: API Inspection

A Securlet is what is referred to as an API-based security application in CloudSOC® CASB and monitors the data at rest within cloud apps. It provides visibility and controls for specific sanctioned SaaS and IaaS apps, such as Office 365, Google Workspace, Box, Salesforce, AWS, Azure, and GCP. It examines the data that is being accessed and retroactively takes action through policies (quarantine, delete, change permission, coach, block high risk services, and so on). With API-based inspection, you have the ability to enforce fine-grained controls. This means that you can remove access from certain users or quarantine a file for further inspection from your privacy team.

Securlets provide high levels of visibility, reporting, and control of corporate information, matched with user behavioral analytics that can quantify the immediate and future risk to the business and take automated actions to

manage this risk. Securlets can be deployed on their own or in combination with CASB Gateway (Gatelets) to add real-time controls and broader coverage. A Securlet is important for some of the following reasons:

- Automates classification and governance of compliance related data, such as PII, PCI, and PHI
- Enforces content-aware and context-aware remediation policies to protect sensitive data
- Streamlines incident response by tapping granular log data with powerful analysis tools
- Tracks objects and activities within the sanctioned cloud application
- Limits oversharing of any or all information based upon the CASB protect policy (for example, unsharing all publicly shared objects)
- Governs oversharing of sensitive information based upon DLP policy
- Is easy to deploy and only needs API authorization
- Enforces the same level of security controls on an unmanaged device, without needing an agent, as could be achieved by a managed device.

Gatelets: Inline Inspection

Gatelets are application-aware inline cloud proxies. They monitor and protect the data in motion, in real time, between the use of SaaS and IaaS apps and the users accessing the application. The inline deployment method is beneficial in environments that demand real-time visibility and control and are critical to prevent data exfiltration of sanctioned apps and unsanctioned apps.

Organizations who adopt cloud applications need Gatelets and inline functionality to prevent users from using unauthorized applications and restrict access to trusted apps and the tenants of trusted apps. Gatelets ensure that malware is not uploaded to or downloaded from cloud applications and can ensure their users are only logging into or sharing sensitive information with a trusted tenant of multi-tenanted cloud applications. They can also monitor and control if users are sharing sensitive information with external accounts or unknown tenants. For example, you can block employees from pushing code to their personal or public repositories.

CloudSOC CASB offers Gatelets with different levels of support. Gatelets that offer full support have more granular support for application activities and can support a wide variety of monitoring and policy enforcement capabilities based upon cloud app events. These policy enforcement capabilities include the following actions:

- Force login, force logoff, or block access to the non-company tenants of a cloud application
- Upload, download, share, unshare, delete, track, or block data exfiltration
- Track or block malware threats inline

Support also exists for custom Gatelets with a set of activities and objects that perform content inspection for threats and DLP.

Use Cases

Ensure Visibility in the Cloud

Uncover Shadow IT usage in your organization. Analyze logs from your proxy, firewall, and endpoints to identify the cloud services in use in your organization and assign a Business Readiness Rating to thousands of apps and services. Risk scoring is provided for over 37,000 apps using hundreds of security mechanisms, compliance certifications, and other metrics.

Govern and Control the Use of Cloud Apps at Rest and in Motion

Use Securlets and Gatelets to monitor and control the data at rest and in motion in both sanctioned and unsanctioned apps, as well as extend existing on-premise DLP policies and workflows to cloud apps and services.

Identify and Remediate Risky Data Exposures in Cloud Apps

Identify and track confidential data uploaded to and created in sanctioned cloud apps such as Box, Google Workspace, Salesforce, or Office 365 to identify any sensitive or compliance-related content that may be shared inappropriately.

Continuously Monitor for Risk

CloudSOC CASB continuously monitors risks from cloud app usage, data loss, malware, device security posture, compromised accounts, and other sources. Risk scores are applied to users and if they go beyond an acceptable threshold, adaptive access controls harness this data to protect information. For example, you can reduce someone's access privileges, reduce privileges for sharing data, block malicious content, and keep malicious or compromised users off of cloud applications.

Prevent Compliance Violations

Identify and classify critical compliance-related data such as PHI, PCI, and PII, and then continuously monitor how that data is being uploaded, downloaded, or shared in cloud apps. Policies can be used to control how this data is handled. Any attempted compliance violations can be tracked for further follow-up actions.

Monitor and Control Activities on Public Cloud (AWS, Azure, and GCP)

Prevent unauthorized activity in IaaS public cloud (AWS, Azure, and GCP). Restrict users from misconfiguring corporate AWS and Azure instances and protect AWS, Azure, and GCP accounts from hackers and malicious insiders who try to use your infrastructure for their own purposes. Identify rogue or non-compliant and malicious activities, virtual machines, and servers. Continuously assess the compliance postures of your cloud environments with PCI, HIPAA, CIS, and other compliance standards. You can also ensure compliance throughout your DevOps lifecycle with continuous monitoring and auditing of your cloud deployments, as well as get proof of compliance with documented evidence of resources that have passed security checks.

Protect Your Cloud Apps against Malware

Protect against threats spreading into your cloud apps, use capabilities such as adaptive access controls, static and dynamic malware analysis, and threat intelligence to block malware.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

dlp-cloud-wp100 March 30, 2023