WHITE PAPER

Symantec® CloudSOC® CASB

Cloud Managed Data Loss Prevention (DLP)

TABLE OF CONTENTS

Overview

Symantec® CloudSOC® CASB now provides you with the ability to create and manage DLP policies for CASB data at rest using Securlets, CASB data in motion using Gatelets, Cloud Secure Web Gateway (SWG), and email. DLP incidents are captured in the console and incident responders can manage them. Customers that have DLP Cloud or Cloud Detection Service for Cloud SWG and Email can now apply DLP policies to find sensitive content in web and email traffic. Administrators have the ability to reuse existing DLP profiles through the CloudSOC console.

Where Do I Find This Feature?

You can find this feature in the following locations:

- **Protect module** – DLP policies are managed in the Protect module. When the appropriate policy type is selected, you can add DLP profiles to the policies to detect the content you plan to protect. You have the ability to choose from over 70 profile templates (out-of-the-box profiles) or create a profile from scratch. When defining a profile from scratch, you can choose from over 300 data identifiers, keywords, regular expressions (RegEx), and exact data matching. Text-based scanning and image scanning (OCR) functionality is also supplied.
- **Investigate module** – DLP incidents are listed in the Investigate module under the DLP Incidents tab. Each incident has a unique ID number associated with it. The incident snapshot provides details about what triggered the incident, including the policy violated and the matched content.

Why Manage DLP in the Cloud?

Bringing these components together enables you to efficiently manage your deployment. Bringing DLP to the cloud and embedding policy and incident management in a common console makes it easier to understand who is doing what with your sensitive information. This knowledge allows you to implement tighter controls when and where needed, and also allows for better cross-team cooperation.

YOU CAN EASILY DEPLOY DLP POLICIES TO PROTECT THAT SENSITIVE INFORMATION STRAIGHT FROM THE CLOUDSOC CONSOLE, WITH NO RELIANCE ON ORACLE OR MAJOR UPGRADES.

Cloud Managed DLP provides inspection, but it does not require additional server resources, infrastructure, or personnel.

Cloud-native DLP provides the following capabilities:

- The solution is easier to deploy.
- System upgrades are simpler because they require fewer resources.
- New features and content are delivered to customers faster.
- Total cost of ownership is reduced.

Customer Benefits

Cloud Native DLP

The service is in the cloud. There is no infrastructure to manage for the console, incident storage, or detection servers for each channel or protocol that you want to monitor. Being cloud native allows for easier access to the console without the need to VPN into the corporate network. The service is designed for high availability and for disaster recovery.

Protect Your Sensitive Data in the Cloud, Web, and Email

Cloud Managed DLP covers cloud applications, web traffic through our Cloud SWG and Email, whether it is on-prem email routed to the cloud detection service or from cloud email providers (Microsoft Office 365 and Gmail).

Gain Granular Visibility

Gain visibility of all the DLP incidents that show up in the CloudSOC console regardless of the channel or protocol being monitored. You can filter the incidents down to individual channels, by policy, by user, and within a specific date or date range. Use these filters to get the granular visibility you need.

Direct Cloud to Cloud Traffic

With a cloud native solution it is cloud to cloud. You avoid the need to backhaul traffic, removing latency issues.

Easier Deployment

The service is provisioned for you. After you log into the Cloud Management Portal and configure CloudSOC CASB and the Detection Services, you are deployed. We scale the volume of traffic from your environment. Once provisioned, you just need to create your policies. After those policies are created, they are automatically pushed out to the detection services and incidents will start to flow to the console for management.

Flexible Policies

Policy creation is easy to do in CloudSOC. CloudSOC CASB uses DLP profiles in the policies. With these profiles you can create them once and then use them in as many policies as you like. If you need to edit the profiles, the policies that leverage those profiles are automatically updated when you save the profile.

Automatic Upgrades

Because it is a SaaS capability, we do the upgrades for you. When new features are completed, they are pushed out to production on a regular basis. No planning is required by you and there is no need to perform those tedious upgrades. You can easily deploy DLP policies to protect that sensitive information straight from the CloudSOC console, with no reliance on Oracle or major upgrades.

To ensure that you get the most value from your CloudSOC deployment, make sure to check the CloudSOC CASB product page often.

For more information about Could Managed DLP, see the CloudSOC Release Notes.

Use Cases

Secure Data Across Cloud, Web, and Email

You can secure data across the following services:

- **Cloud applications** – Cloud managed DLP allows you to monitor your users' interactions with your cloud applications. DLP policies can be applied to scan data at rest (DAR) through CloudSOC securlets. When a file is uploaded or changed, DLP automatically scans those files for sensitive content. The appropriate response action is applied and the incident is recorded in the cloud console. DLP policies can be applied to data in motion (DIM) to or from your cloud applications through CloudSOC gatelets. As files are uploaded or downloaded, DLP scans those files for sensitive content, applies the appropriate response action to protect that data, and records the incident.
- **Web traffic** – Cloud managed DLP allows you to monitor web traffic through our Cloud SWG. As sensitive content is flowing through your instance of our Cloud SWG, DLP policies are applied. When a violation occurs, the appropriate response action is applied and the incident is recorded in the cloud console.
- **Email** – Cloud managed DLP allows you to monitor email traffic as it is leaving your environment. The traffic can be from an on-prem email routed to our cloud detection service, or a cloud email originating from Exchange Online, Microsoft Office 365, or Gmail routed to our cloud detection service. DLP policies are applied to the email, and the message itself is scanned in addition to any attachment in the message. When a violation occurs, the appropriate response action is applied and the incident is recorded in the cloud console.

Ensure Visibility in the Cloud

The cloud console has predefined widgets in the dashboard section in CloudSOC. These widgets give you visibility into your incidents. You will see widgets for DAR and DIM severity, a DAR and DIM policy summary for your cloud applications, a network incident summary, a network policy summary, and a network policy table for Internet Content Adaptation Protocol (ICAP) and email. This data allows you to view at high level how your DLP program is doing and where you need to investigate further. You also have the ability to create your own widgets for more custom dashboards for your DLP program. Additionally, each incident has correlation information where you can see information about other incidents. For example, you can correlate information about the sender, recipient, cloud application, file name, URL, and policy name.

Remediate Incidents in the Cloud

Customers can remediate incidents in bulk or individually from one location, the DLP Incident List page. This page reduces the time spent on incident management. They can granularly filter the list to identify the incidents they are interested in and take the appropriate action. The UI gives customers the ability to quickly review the incident details with a flyout window, or they can go to the incident details page and review it more thoroughly.

BROADCOM connecting everything®

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

cloudSOC-DLP-WP102 May 11, 2023