Symantec Endpoint DLP Integration with Chrome Enterprise Setup Guide
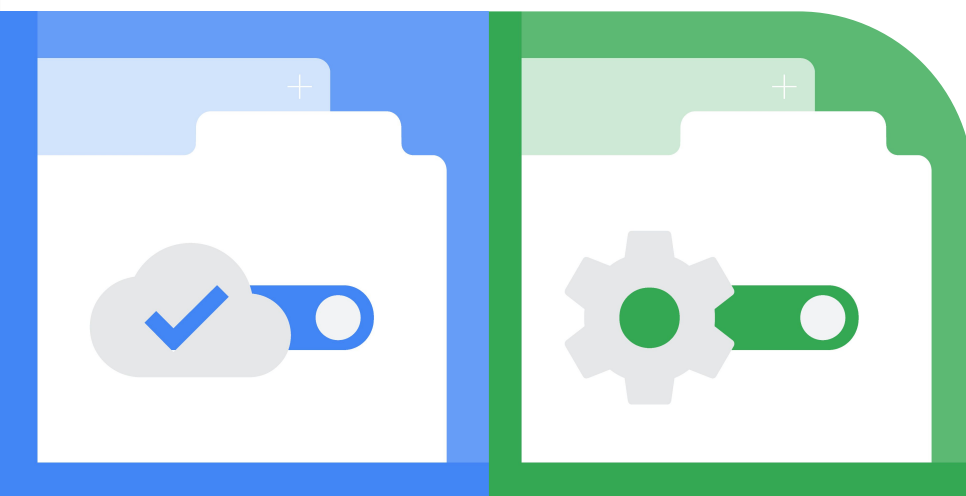
November 2023

Table of Contents

chrome enterprise

Symantec™
by Broadcom

Chrome Enterprise Connector to Symantec Endpoint DLP Overview

Many enterprises wish to extend Symantec Endpoint DLP protection to monitor Chrome browser usage for data exfiltration and apply allow/block controls based on their DLP policies.

Existing extension-based methods for allowing DLP systems to interface with Chrome need continual review and version upgrades can cause incompatibility, resulting in instability and performance issues. In addition, these solutions are less effective at solving advanced DLP use cases. The integration with Chrome solves many of these issues.

This document outlines the steps to enable and use the Chrome Enterprise Connector to Symantec Endpoint DLP.

Requirements:

- **Symantec Endpoint DLP Version 16.0.1 or later**
- **Chrome Browser M118 or later**
- **Chrome Browser Cloud Management**

Key Use Cases

- Users upload files containing sensitive data in Chrome by browsing to the file.
- User uploads a file containing sensitive data in Chrome by dragging & dropping it into the page.
- Users upload files containing sensitive data in Chrome by copying and pasting into the page.
- User pastes content into a page in Chrome from the clipboard.
- User prints a page containing sensitive data in Chrome via File->Print or keyboard shortcuts.

Benefits

- Reduced risk of compatibility issues or breaks in DLP monitoring
- Shortened testing cycles in the customer environment
- Enhanced coverage for previously unsupported use-cases
- Improved browser performance and stability for end users due to the native integration

Chrome Enterprise Connector to Symantec Endpoint DLP Overview

Below is a overview of the solution:
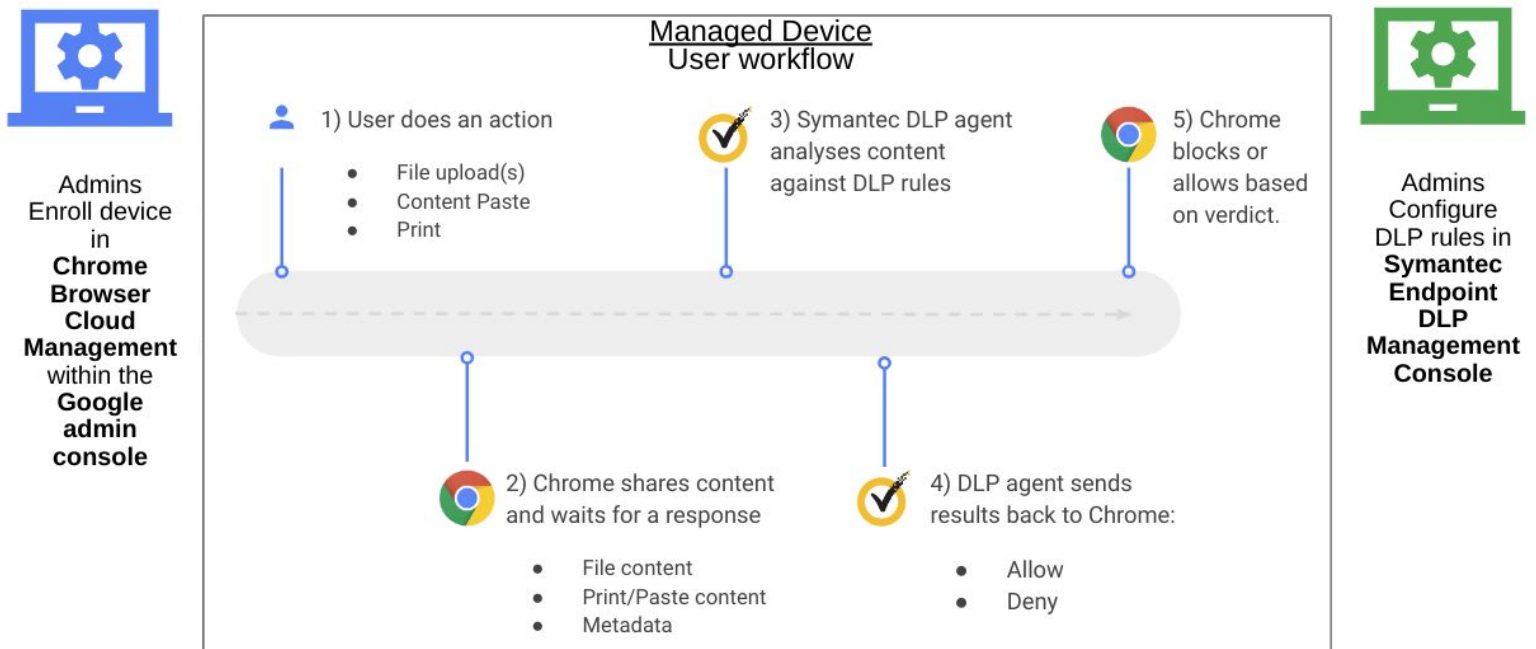
Chrome Enterprise Connector to Symantec Endpoint DLP Overview

When the user performs an operation such as File Upload, Clipboard paste or Print within Chrome, Chrome communicates the user action and the content (along with some metadata) to the Symantec DLP agent. Chrome then waits for a verdict from the service. During this time, Chrome freezes the tab and displays an appropriate UI to the user. Note this dialog is only shown if the scan tasks take more than 1 second.
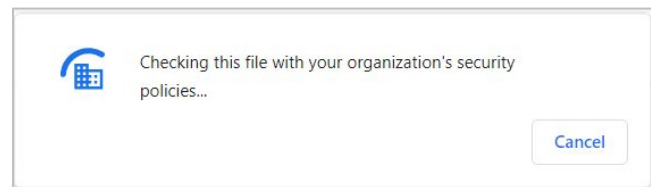
Symantec DLP Agent analyzes content against DLP Rules and generates a verdict. If the Verdict is 'Block' or 'Warn', the agent will show a popup to the end user with an appropriate message.

The agent will also communicate this verdict with Chrome. If Chrome receives an "Allow" verdict from the agent, it will proceed to let the user complete the operation. If the verdict is 'Block' it will prevent the user from completing the desired operation.
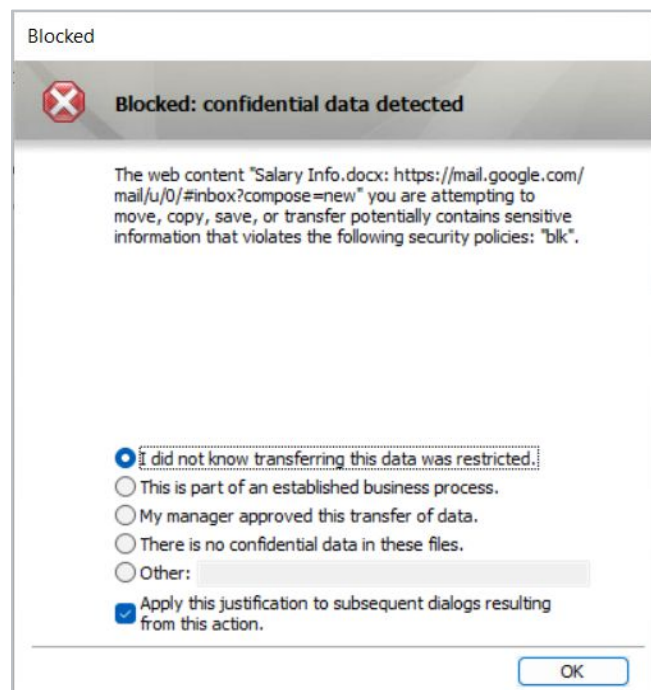
Enable Chrome Enterprise Connector to Symantec Endpoint DLP in the Google Admin console

1. Go to the [Google Admin console.](#)

2. Go to *Devices > Chrome > Settings > Users & browsers*.

3. Filter for the word **"connectors"** and select "**Category contains**" and you should see a section titled "**Chrome Enterprise connectors**".

4. Select "**Allow users**" to enable Enterprise Connectors from the dropdown menu.

5. Agree to the Connectors disclosure, if applicable.

6. Click "**Save**" on the upper right corner

7. Select "**Symantec Endpoint DLP**" as your Content Analysis vendor from the dropdown menu.

    Currently supported functions are:
    - Upload content analysis
    - Bulk text content analysis
    - Print content analysis
    - Hit "Add Configuration".

8. Click "**Save**" again on the upper right corner.

Setup Symantec Endpoint DLP Agent

You will need to deploy the Endpoint DLP Agent 16.0.1 version or above on your Windows endpoint devices.

Please refer to [this documentation](#) on how to install the DLP agent.

Platform Supported

Chrome Enterprise Connector to Symantec Endpoint DLP is currently supported on:

✓ Windows

Additional Resources

🔗 [Chrome Browser Cloud Management](#)

🔗 [Learn More at Chrome Enterprise Help Center](#)

🔗 [Learn More at Symantec by Broadcom Support Center](#)