Forcepoint DLP App Data Security API

Secure Your Data Everywhere

Forcepoint

Brochure

Secure Your Data Everywhere

Data security has become increasingly complex as organizational perimeters dissolve, and data resides and moves across multiple locations. In the past year alone, over 75% of organizations have reported experiencing data breaches, costing millions of dollars. Protecting sensitive data has never been more challenging.

Forcepoint is recognized as a leader in data security platforms. We enable organizations to keep data secure anywhere their people work and everywhere their data resides. Our solutions cover multiple channels, including endpoints, cloud, network, web traffic, private applications and email. This ensures that your sensitive and regulated data remains secure, regardless of its location.

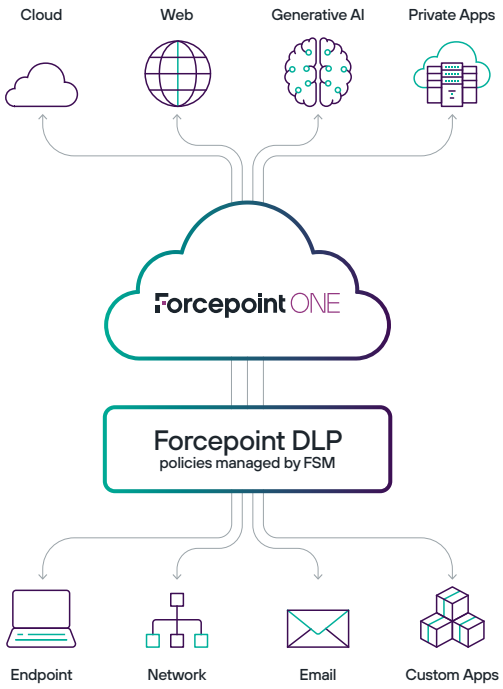

Figure 1: Extending Enterprise DLP from the endpoint to the cloud, web, and custom applications.

Extend Data Security to Custom Applications with App Data Security API

Forcepoint DLP App Data Security API makes it easy for organizations to safeguard information in their internal custom applications. It allows data within these applications to be protected based on how it is being used, ensuring comprehensive security within the application.

The App Data Security API simplifies custom development. It is a REST API that is easy to understand and simple to use without extensive training or knowledge of complex protocols. It is also language-agnostic, enabling development and consumption in any programming language or platform that supports HTTP.

Use cases:

- **Enforcing DLP policies within internal custom applications**
- **Enforcing DLP policies within internal repositories**

Actions available for custom applications:

- **Permit**
- **Block**
- **Request**
- **Confirm allow**
- **Confirm block**
- **Encrypt**
- **Drop**
- **User encrypt**
- **Safe copy**
- **Quarantine**
- **Quarantine with note**
- **Unshare external**
- **Unshare all**

Key Use Cases of App Data Security API

- → **Internal Custom Applications:** Organizations with internally developed applications can utilize the App Data Security API to analyze file and data traffic. By sending traffic to Forcepoint DLP for analysis and applying DLP policies, organizations can enforce data security within their custom applications. The API is then able to return a DLP action selected from the rich set of options that Forcepoint DLP provides. Some of the possible actions are to allow, block, ask for confirmation with a personalized pop-up, encrypt, unshare and quarantine. This opens new possibilities for applying DLP policies without requiring endpoint visibility, ensuring safe usage and preventing exfiltration of sensitive data.
- → **Third-Party Application Repositories:** With the App Data Security API, organizations can strengthen the security of third-party application repositories such as Confluence and Kiteworks. Internal developers can create plug-ins utilizing App Data Security API that examine file and data transfers within these repositories and apply DLP policies to enhance data protection.

Availability

App Data Security API enables organizations to analyze and protect both data in motion and data at rest efficiently and concisely. It is available as an add-on to Forcepoint DLP Network and DLP Suite. To learn more, visit forcepoint.com/dlp, request a demo or contact your Forcepoint sales representative or sales partner.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Brochure-Forcepoint DLP App Data Security API-US] 19July2023