Forcepoint

Datasheet

Forcepoint DLP

Industry-leading Data Loss Prevention with unified management across all channels

Data security is critical, but it doesn't have to be complicated. Today's hybrid workforce requires access to sensitive information from any device, at any location. Forcepoint Data Loss Prevention (DLP) simplifies data protection for the modern enterprise, delivering comprehensive on-premises data loss prevention without sacrificing performance or productivity.

With deep visibility into data movement across endpoints, networks and storage, Forcepoint DLP safeguards your critical assets and ensures regulatory compliance. It offers the unique ability to extend policies from the Forcepoint Security Manager (FSM) to additional channels, enabling seamless data protection across cloud SaaS apps and web while ensuring consistent and unified policy enforcement. Benefit from advanced forensics, seamless integration, scalability and a solution that evolves with your business needs.

Streamline data compliance

- → **Regulate coverage** to easily meet and maintain compliance with more than 1,800 pre-defined templates, policies and classifiers, including over 70 covering country-specific IDs, credentials, keys, and tokens, applicable to the regulatory demands of 90+ countries and over 160 regions.
- → **Locate and remediate** regulated data with network, cloud, and endpoint discovery.
- → **Central control** and consistent policies across all channels including cloud, endpoint, network, web and email.

Provide comprehensive data protection

- → **Discover and control data** everywhere it lives, whether in the cloud or on the network, via email or at the endpoint.
- → **Coach employees** to make smart decisions, using messages that guide user actions, educate employees on policy and validate user intent when interacting with critical data.
- → **Securely collaborate** with trusted partners using policy-based auto-encryption that protects data as it moves outside your organization.
- → **Automate data labeling and classification** through integration with Forcepoint Data Classification as well as Microsoft Purview Information Protection.

Utilize advanced features and controls

- **Optical Character Recognition (OCR)** embedded within the policy engine identifies data in images while at rest or in motion across on-premises and cloud deployments, simplifying infrastructure and ensuring consistent hybrid enforcement.
- **Robust identification** for Personally Identifiable Information (PII) offers data validation checks, real name detection, proximity analysis and context identifiers.
- **Custom encryption identification** exposes data hidden from discovery and applicable controls.
- **Cumulative analysis** for drip DLP detection (i.e., data that leaks out slowly over time).
- **Advanced file scanning** detects partial data exfiltration by examining randomized sections of large files, preventing exfiltrators from hiding sensitive information.
- **Integration with Forcepoint Data Classification,** leveraging highly trained AI/LLM models to provide highly precise classification for data in use and data at rest with Forcepoint Data Security Posture Management (DSPM).
- **Advanced generative AI** allows users to train the system and construct a self-learning AI model, automatically finding, categorizing and classifying all your data to save time and dramatically increase accuracy.
- **Fingerprinting** of structured (e.g., databases) and unstructured (e.g., documents) data allows data owners to define data types and identify full and partial matches across business documents, design plans and databases, and then apply the right control or policy that matches the data.
- With **Risk-Adaptive Protection,** Forcepoint DLP becomes even more effective as it leverages behavior analytics to understand user risk, which is then used to implement automated policy enforcement based on the risk level of the user.

Find and mitigate data protection risk

- **Focus response teams** on the greatest risk with prioritized incidents that highlight the people responsible for risk, the critical data at risk and common patterns of behavior across users.
- **Use the AI-powered Smart Search help tool** integrated directly into the solution to quickly find specific support information without leaving the management console.
- **Increase employee awareness** for handling sensitive data and IP with employee coaching on Windows and macOS, in addition to enabling employees with integration of classification solutions like Forcepoint Data Classification and Microsoft Purview Information Protection.
- **Enforce advanced DLP data identification capabilities,** such as fingerprinting, on remote work endpoints and in enterprise cloud applications.
- **Enable data owners and business managers** with email-based distributed incident workflow to review and respond to DLP incidents.
- **Safeguard user privacy** with anonymization options and access controls.
- **Add the context of data** into broader user analytics through deep integrations with Forcepoint Risk-Adaptive Protection.
- **Identity integrations** support cloud-native Entra ID for both administrative access and end-user policy enforcement, increasing security consistency and simplifying management.

Achieve visibility over your data everywhere

- → **Empower admins** to identify and protect data across cloud applications, network data stores, databases and managed and unmanaged endpoints.
- → **Identify and automatically prevent sharing** of sensitive data to external users or unauthorized internal users.
- → **Protect data in real time** for uploads into and downloads from critical cloud applications including Office 365, Teams, SharePoint, OneDrive, Salesforce, Box, Dropbox, Google Apps, AWS, ServiceNow, Zoom, Slack and many more.
- → **Unify policy enforcement** using a single console to define and apply data in motion and data discovery policies across all channels – cloud, network, endpoints, web and email.
- → **Maintain data ownership** with an on-prem DLP solution and hybrid options to extend advanced features like fingerprinting, machine learning and policy enforcement to cloud apps and web channels. Ideal for highly regulated industries, it ensures data sovereignty by securely keeping incidents and forensics data within your data center, supporting compliance requirements.
- → **View and manage incidents using third-party tools** through exposed REST APIs. Automate incident management workflows and support business processes relying on DLP incidents through automation and service tools such as ServiceNow, Nagios and Tableau as well as SIEM/SOAR solutions such as Splunk and XSOAR.

For more information about our enterprise DLP solutions, request a demo.

Appendix A: DLP Solution Component Overview

Forcepoint DLP Endpoint	Forcepoint DLP Endpoint protects your critical data on Windows and Mac endpoints on and off the corporate network. It includes advanced protection and control for data at rest (discovery), in motion, and in use. It integrates with Microsoft Azure Information Protection to analyze encrypted data and apply appropriate DLP controls. It enables employee self-remediation of data risk based on guidance from DLP coaching dialog. The solution monitors web uploads, including HTTPS, as well as uploads to cloud services like Office 365 and Box Enterprise. Includes OCR embedded in the policy engine, providing visibility into data in images. Full integration with Outlook, Notes, and email clients.
Forcepoint CASB	Powered by Forcepoint CASB, extend the advanced analytics and single control of Forcepoint DLP to sanctioned cloud applications, including Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack, and many more. Gain continuous control of business-critical data, no matter where users are or what device they use.
Forcepoint Web Security	Forcepoint Web Security allows you to securely access any website or download any document while getting the highspeed web performance your team relies on. Integrate with RBI for secure-container rendering of risky sites, and Zero Trust CDR for complete sanitization of all downloadable documents.
Forcepoint DLP Discover	Forcepoint DLP Discovery identifies and secures sensitive data across file servers, SharePoint (on-premises and cloud), Exchange (on-premises and cloud), and detection within databases such as SQL server and Oracle. Advanced fingerprinting technology identifies regulated data and intellectual property at rest and protects that data by applying appropriate encryption and controls. Includes OCR embedded in the policy engine, providing visibility into data in images.
Forcepoint DLP Network	Forcepoint DLP Network delivers the critical enforcement point to stop the theft of data in motion through email, web channels, and FTP. The solution helps identify and prevent data exfiltration and accidental data loss from outside attacks or from insider threats. OCR embedded in the policy engine, providing visibility into data in images. Analytics provides Drip DLP to stop the theft of data one record at a time as well as other high-risk user behaviors.
Forcepoint DLP for Cloud Email	Forcepoint DLP for Cloud Email stops unwanted exfiltration of your data and IP through outbound email. You can combine with other Forcepoint DLP channel solutions such as Endpoint, Network, Cloud and Web to simplify your DLP management, writing one policy and deploying that policy across multiple channels. Unlike non-cloud solutions, Forcepoint DLP for Cloud Email enables enormous scalability potential from unforeseen bursts of email traffic. Includes OCR to provide consistent enforcement across hybrid deployments. It also allows your outbound email traffic to grow with your business without having to configure and manage additional hardware resources.
Forcepoint DLP App Data Security API	Forcepoint DLP App Data Security API makes it easy for organizations to secure data in their internal custom applications and services. It enables analysis of file and data traffic and enforces DLP actions such as allow, block, ask for confirmation with a personalized pop-up, encrypt, unshare and quarantine. 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.

Appendix B: DLP Solution Component Overview

	FORCEPOINT DLP ENDPOINT	FORCEPOINT CASB	FORCEPOINT WEB SECURITY	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
What is the primary function?	Data Discovery and Enforcement of Data protection policies on user's endpoint via application, web, print, removable media channels, to name a few.	Discovery of data and enforcement of policies in the cloud or with clouddelivered applications	Visibility and control for data in motion via outbound email	Discovery, scanning, and remediation of data at rest within data centers and other on-prem environments	Visibility and control for data in motion via the web and web email within the network	Visibility and control for data in motion via the web and web email within the network	Visibility and control of data in internal custom applications and services
Where is the data discovered/ protected at rest?	Windows endpoints MacOS endpoints	OneDrive, Sharepoint Online, Exchange Online, Google Drive, Box, DropBox, Salesforce, ServiceNow	On-premises file servers and network storage, Sharepoint server Exchange server, Databases like Microsoft SQL Server, Oracle, and IBM Db2				
Where is data in motion protected?	Email, Web: HTTP(S), Printers, Removable media, File servers / NAS	Uploads, downloads and sharing for Office 365, Google Apps, Salesforce. com, Box, Dropbox and ServiceNow via API and ALL other major apps via proxy	HTTP(S)		Email, Printers, FTP, Web: Http(S), ICAP	Email	Internal custom applications and custom services
Where is data in use protected?	Zoom, Webex, Google Hangouts, IM, VOIP file sharing , M365 Teams sharing, applications (cloud storage clients), OS clipboard	During creation, modification, and collaboration activities using cloud applications					Internal custom applications and custom services

Appendix B: DLP Solution Component Feature Comparison

	FORCEPOINT DLP ENDPOINT	FORCEPOINT CASB	FORCEPOINT WEB SECURITY	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Risk-Adaptive Protection	Add-on		Add-on; currently supported with GRE/ IPSec tunnels with Forcepoint Web Security	Add-on	Add-on	Add-on	
Optical character recognition	Included			Included	Included	Included	
Data classification and labeling integrations	Forcepoint Data Classification and Microsoft Purview Information Protection.						
What data can be fingerprinted?	Structured (databases), Unstructured (documents), Binary (non-textual files)						
Unified policy management	Policy configuration & enforcement via single console from endpoints to cloud applications						
Robust policy library	Discovery & enforcement from the largest compliance policy library in the industry						