Forcepoint Data Loss Prevention

Data protection in a zero-perimeter world

Forcepoint

Brochure

Forcepoint Data Loss Protection (DLP)

Data security everywhere your people work and data resides

Data security is a major problem for organizations of all types and sizes today. On one hand, IT organizations are required to keep up with regulations and protect personal identifiable information (PII), protected health information (PHI), and other types of regulated information from targeted malicious attacks as well as accidental data loss. On the other, they must adapt to macro IT movements, such as the adoption of cloud applications, hybrid cloud environments, and BYOD trends, all of which increase the ways data can leave your organization.

This expanding attack surface poses the most significant challenge to protecting critical data. Data security teams must consider the explosion of data movement from "inside" the organization to all the places and channels that data now resides and moves. Visibility must be gained across all data in the cloud as well as on-prem. Data security teams must also have visibility and control across all channels (endpoint, web traffic, network, email, cloud applications, and private applications) with a single point of management.

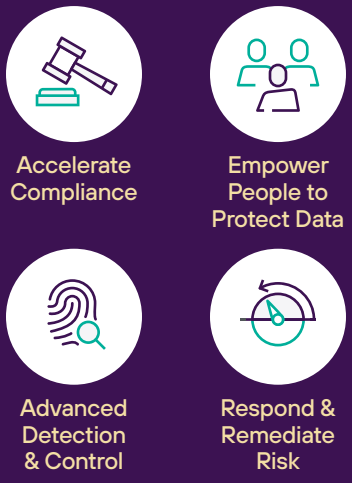
Forcepoint DLP is the industry's most trusted solution, giving you the tools to easily manage global policies across every major channel, whether its endpoint, network, cloud, web, private applications, or email. We can simplify your work with the most pre-defined templates, policies and classifiers of any DLP provider in the industry. This can dramatically streamline your incident management so you can focus on what's most important, eliminating risk so that your people can be increasingly productive. Forcepoint DLP addresses risk by bringing you visibility and control everywhere your people work and anywhere your data resides.

Data Protection must:

- **Secure regulated data** with a single point of control for all the applications your people use to create, store, and move data.
- **Protect sensitive data** with advanced DLP that analyzes how people use data, coaches your people to make good decisions with data, and prioritizes incidents by risk.

Important channels protected

- **Custom Applications**
- **Cloud Applications**
- **Private Applications**
- **Endpoint**
- **Network**
- **Discovery**
- **Web**
- **Email**



Accelerate compliance

The modern IT environment presents a daunting challenge for enterprises aiming to comply with dozens of global data security regulations, especially as they move toward cloud applications and mobile workforces. Many security solutions offer some form of integrated DLP, such as the type found within cloud applications.

Yet security teams face unwanted complexity and added costs when deploying and managing separate and inconsistent policies across endpoints, cloud applications, and networks. Forcepoint DLP accelerates your compliance efforts by providing over 1600 predefined classifiers, policies, and templates. This accelerates initial DLP deployment and simplifies ongoing DLP management. Forcepoint DLP efficiently secures sensitive customer information and regulated data so you can confidently prove ongoing compliance.

- → **Regulate coverage** to easily meet and maintain compliance with more than 1600 pre-defined templates, policies, and classifiers applicable to the regulatory demands of 83 countries and over 150 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.

Empower people to protect data

DLP with only preventive controls frustrate users who will attempt to circumvent them with the sole intention of completing a task. Going around security results in unnecessary risk and inadvertent data exposure.

Forcepoint DLP recognizes your people as at the front lines of today's cyber threats.

- → **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 & classification** by integrating with Forcepoint Data Classification as well as Microsoft Purview Information Protection.

Advanced detection and controls that follow the data

Malicious and accidental data breaches are complex incidents, not single events. Forcepoint DLP is recognized by Forrester, Gartner, Radicati Group and Frost & Sullivan as an industry leader for DLP solutions. One of the key features is Forcepoint DLPs ability to identify data at rest, in motion, and in use. Key data identification includes:

- → **Optical Character Recognition (OCR)** identifies data embedded in images while at rest or in motion.
- → **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).
- → **Integration with Forcepoint Data Classification,** leveraging highly trained AI/ML models to provide highly precise classification for data in use.

- → **Machine learning** allows users to train the system to identify relevant, never-before-seen data. Users provide the engine with positive and negative examples to flag similar business documents, source code, and more.
- → **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.
- → **Analytics** identify changes in user behavior as it relates to data interaction such as increased use of personal email. 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. This allows security teams to implement dynamic policies which are individualized as compared to static global ones.

Identify, manage and remediate data protection risk

Most DLP solutions lack the robustness of a strong predefined classification library and sensitive visibility across all your data, overloading users with false positives while missing data at risk. In addition to making security teams less effective, this makes employees or end users frustrated as they see security solutions as a hindrance to their business productivity. Leveraging analytics, and the largest library of pre-built templates and policies in the industry Forcepoint DLP drastically reduces false positives which helps security operations to be more efficient. To increase employee security awareness, DLP supports employee coaching and integration with data classification solutions.

- → **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.
- → **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.

Visibility everywhere including both your data on-prem and data in the cloud

Today's enterprises are challenged with complicated environments, where data is everywhere and requires the protection of data in places that aren't managed or owned by the enterprise. Forcepoint ONE CASB, SWG and ZTNA extends analytics and DLP policies to critical cloud applications, web traffic and web based private applications so your data is protected, wherever it resides. REST APIs such as Forcepoint DLP App Data Security API brings visibility and DLP enforcement to internal custom developed applications.

- → **Focus response teams 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** via a single console to define and apply data in motion and data discovery policies across all channels—cloud, network, endpoints, web and email.
- → **Deploy a Forcepoint-hosted solution** that extends DLP policy features including fingerprinting and machine learning to cloud applications, while having the option of maintaining incidents and forensics data within your data center.
- → **View incidents and manage in 3rd 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.

Forcepoint DLP includes advanced analytics and regulatory policy templates from a single point of control with every deployment. cloud applications, web traffic and web based private applications so your data is protected, wherever it resides.

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. Full integration with Outlook, Notes, and email clients.
Forcepoint ONE CASB	Powered by Forcepoint ONE 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 ONE SWG	Forcepoint ONE SWG allows you to securely access any website or download any document while getting the high-speed 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 ONE ZTNA (coming 2H 2023)	Forcepoint ONE ZTNA brings simple, safe and scalable Zero Trust remote access to internal and private cloud applications without the need for a VPN across both managed and unmanaged devices.
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. Discovery also includes OCR which provides 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 recognizes data within an image. 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. 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 ONE CASB	FORCEPOINT DLP— DISCOVER	FORCEPOINT DLP— NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	FORCEPOINT DLP APP DATA SECURITY API	FORCEPOINT ONE ZTNA (COMING 2H 2023)
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	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 for data in motion via outbound email	Visibility and control of data in internal custom applications and services	Visibility and Data protection policy enforcement for data in motion (uploads & downloads) within a corporate private application
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 & sharing for Office 365, Google Apps, Salesforce. com, Box, Dropbox & ServiceNow via API and ALL other major apps via proxy		Email, Printers, FTP, Web: Http(S), ICAP	Email	HTTP(S)	Internal custom applications and custom services	Uploads & Downloads via ZTNA Connector to private apps
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 CLOUD APPLICATIONS	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP—CLOUD EMAIL	FORCEPOINT WEB TRAFFIC	FORCEPOINT DLP APP DATA SECURITY API	FORCEPOINT ONE ZTNA (COMING 2H 2023)
Risk-Adaptive Protection	Add-on		Add-on	Add-on	Add-on	Add-on; currently supported with GRE/IPSec tunnels with Forcepoint ONE SWG		
Optical character recognition			Included	Included	Included			OCR support for DLP Enhancement (2H2023)
Data classification & labeling integrations	Forcepoint Data Classification and Microsoft Purview Information Protection.							
What data can be finger-printed?*	Structured (databases), Unstructured (documents), Binary (non-textual files)							Available 2H2023
Unified policy management	Policy configuration & enforcement via single console from endpoints to cloud applications							Available 2H2023
Robust policy library	Discovery & enforcement from the largest compliance policy library in the industry							

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-DLP-Brochure] 18Aug2023