Forcepoint Data Loss Prevention (DLP)

Data protection in a zero-perimeter world

Forcepoint

Brochure

Forcepoint DLP

Security driven by the human point

Data security is a never-ending challenge. On one hand, IT organizations are required to keep up with regulations and protect intellectual property from targeted attacks and accidental exposure. 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 take the seemingly logical approach to chase data: find it, catalog it, and control it. Yet this traditional approach to data loss prevention is no longer effective because it ignores the biggest variable in data security—your people.

Instead of focusing solely on data, security should begin and end with people. The key is to gain visibility into user interactions with data and applications. Once this is achieved, you can apply a level of control based on the specific user's risk and the sensitivity or value of the data.

An organization's data protection program must consider the human point—the intersection of users, data, and networks. In addition, the enterprise must remain vigilant of data as it moves across the enterprise and highlight the people who create, touch, and move data.

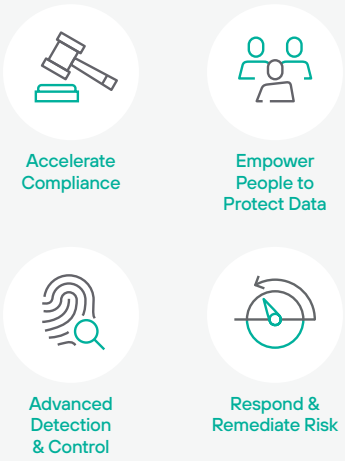
Forcepoint DLP addresses human-centric risk with visibility and control everywhere your people work and everywhere your data resides. Security teams apply user-risk scoring to focus on the events that matter most and to accelerate compliance with global data regulations.

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 intellectual property** with advanced DLP that analyzes how people use data, coaches your people to make good decisions with data, and prioritizes incidents by risk.

Visibility & control everywhere your people work and data resides

- **Cloud Applications**
- **Endpoint**
- **Network**
- **Discovery**



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 combining pre-packaged coverage of global regulations with central control across your IT environment. Forcepoint DLP efficiently secures sensitive customer information and regulated data so you can confidently prove ongoing compliance.

- → **Regulatory coverage** to quickly meet and maintain compliance with more than 370 policies applicable to the regulatory demands of 83 countries.
- → **Locate and remediate** regulated data with network, cloud, and endpoint discovery.
- → **Central control** and consistent policies across the IT environment.

Empower people to protect data

DLP with only preventive controls frustrates users who will 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 the front lines of today's cyber threats.

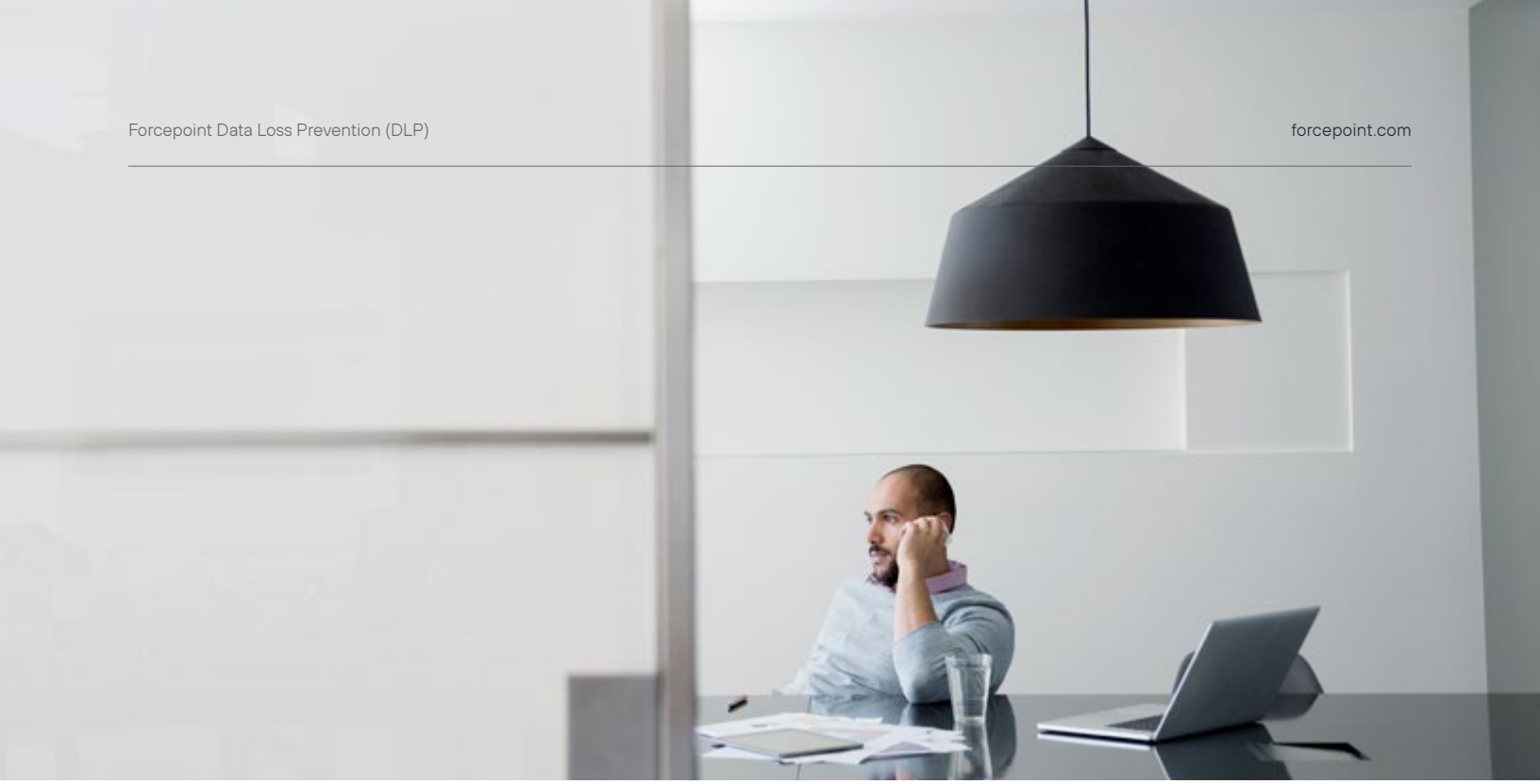
- → **Discover and control data** everywhere it lives, whether in the cloud or on the network, via email, and at the endpoint.
- → **Coach employees** to make smart decisions, using messages that guide user actions, educate employees on policy, and validate user intent when interacting with critical 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 leading third-party data classification solutions (e.g., Microsoft Azure Information Protection, Titus, Boldon James).

Advanced detection and controls that follow the data

Malicious and accidental data breaches are complex incidents, not single events. Forcepoint DLP is a proven solution that analyst firms including Gartner, Radicati, and others recognize as a leader within the industry. Forcepoint's DLP offerings are available in two versions: DLP for Compliance and DLP for Intellectual Property (IP) Protection.

Forcepoint DLP for Compliance and IP Protection provides critical capabilities addressing compliance with features such as:

- → **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 Microsoft Azure Information Protection** analyzes encrypted files and applies appropriate DLP controls to the data.



Forcepoint DLP for IP Protection includes the capabilities above, plus applies the most advanced detection and control of potential data loss with features such as:

- → **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 (like databases) and unstructured (like 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 Dynamic Data Protection (DDP), Forcepoint DLP becomes even more effective as it leverages behavior analytics to understand user risk, which is then used to implement risk-adaptive policies. This allows security teams to implement dynamic policies which are individualized as compared to static global ones.

Identify, manage and remediate data protection risk

Traditional approaches to DLP overload 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, Forcepoint DLP reduces false positives which helps security operations. 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 Boldon James and Microsoft Azure 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 Insider Threat and Forcepoint Behavioral Analytics.

Visibility everywhere your people work, control everywhere your data resides

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 DLP for Cloud Applications extends analytics and DLP policies to critical cloud applications so your data is protected, wherever it resides.

- → **Focus response teams to identify and protect** data across cloud applications, network data stores, databases, and managed 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, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack, and many more.
- → **Unify policy enforcement** via single console to define and apply data in motion and data discovery policies across all channels—cloud, network, and endpoints.
- → **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.

Forcepoint DLP includes advanced analytics and regulatory policy templates from a single point of control with every deployment. Enterprises choose the deployment options for their IT environment.

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 DLP – Cloud Applications	Powered by Forcepoint CASB, DLP – Cloud Applications extends 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.
Forcepoint DLP – Discovery	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 and web channels. 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 identify DLP to stop the theft of data one record at a time and other high-risk user behaviors.

Appendix A: DLP solution component overview

	FORCEPOINT DLP – ENDPOINT	FORCEPOINT DLP – CLOUD APPLICATIONS	FORCEPOINT DLP – DISCOVER	FORCEPOINT DLP – NETWORK
How is it deployed?	Forcepoint One Endpoint	Forcepoint Cloud	IT Managed Discovery Server	Network Appliance or Public Cloud
What is the primary function?	Collection of information on the user's endpoint	Discovery of data and enforcement of policies in the cloud or with cloud-delivered applications	Discovery, scanning, and remediation of data at rest within data centers	Visibility and control for data in motion via the web and email
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, ActiveSync proxy, Web: HTTP(S) ICAP
Where is data in use protected?	Zoom, Webex, Google Hangouts, IM, VOIP file sharing, applications (cloud storage clients), OS clipboard	During collaboration activities using cloud applications		
Dynamic Data Protection*	Add-on			Add-on
Optical character recognition			Included	Included
Data classification & labeling integrations	Microsoft Azure Information Protection, Boldon James, Titus			
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 Across data centers and public cloud			
Robust policy library	Discovery & enforcement from broad compliance policy library			

Humans Are the New Perimeter.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[DLP-BROCHURE-US-EN] 3Nov2020