FORCEPOINT Data Loss Prevention (DLP)

DATA PROTECTION IN A ZERO-PERIMETER WORLD

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

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, catalogue 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.

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 & data resides

- Cloud Applications (powered by Forcepoint CASB)
- Endpoint
- Network
- Discovery

Accelerate Compliance

Empower People to Protect Data

Advanced Detection & Control

Respond & Remediate Risk

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.

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.
- **Apply data classification and tagging** by integrating with leading third-party data classification solutions (e.g., Microsoft Azure Information Protection, Bolden James, Titus).

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, Forrester and others recognize as a leader within the industry. Forcepoint's DLP offerings are available in 2 versions: DLP for Compliance and DLP for IP Protection.

Forcepoint DLP for Compliance provides critical capability addressing compliance with features such as:

- **Optical Character Recognition (OCR)** identifies data imbedded in images while at rest or in motion (available with Forcepoint DLP – Network).
- **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 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 and unstructured 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.

RESPOND AND REMEDIATE RISK

Traditional approaches to DLP overload users with false positives while missing data at risk. Forcepoint DLP applies advanced analytics to correlate seemingly unrelated DLP events into prioritized incidents. Incident Risk Ranking (IRR) provided with Forcepoint DLP fuses disparate DLP indicators into a framework of Bayesian belief networks to assess the likelihood of data risk scenarios, such as data theft and broken business processes.

- **Focus response teams on greatest risk** with prioritized incidents that highlight the people responsible for risk, the critical data at risk and common patterns of behavior across users.
- **Investigate and respond** with workflows that link disparate events, show context of data at risk and provide analysts with the information they need to take action.
- **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 UEBA.

VISIBILITY EVERYWHERE YOUR PEOPLE WORK, CONTROL EVERYWHERE YOUR DATA RESIDES

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. 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 critical cloud applications, including Office 365, Salesforce, Google Apps, Box and more.
Forcepoint DLP – Discovery	Forcepoint DLP – Discovery identifies and secures sensitive data across your network, as well as data stored in cloud services like Office 365 and Box Enterprise. Advanced fingerprinting technology identifies regulated data and intellectual property at rest and protects that data by applying appropriate encryption and controls.
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 malicious and accidental data loss from outside attacks or from the growing insider threats. OCR (Optical Character Recognition) 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 B: DLP SOLUTION COMPONENTS DETAIL

	FORCEPOINT DLP – ENDPOINT	FORCEPOINT DLP – CLOUD APPLICATIONS	FORCEPOINT DLP – DISCOVER	FORCEPOINT DLP – NETWORK
How is it Deployed?	Endpoint Agent	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 all is the Data discovered / protected at rest?	Windows endpoints MacOS endpoints Linux endpoints	Exchange Online Sharepoint Online Box	On-premises file servers and network storage Sharepoint Server Exchange Server	
Where is Data in Motion protected?	Email Web: HTTP(S) Printers Removable media Mobile devices File servers / NAS	Uploads & sharing for Google Apps Uploads & sharing for Office 365/OneDrive Salesforce.com and Box		Email /Mobile email/ ActiveSync proxy Web: HTTP(S) ICAP
Where is Data in Use protected?	IM, VOIP file sharing, applications (cloud storage clients), OS clipboard	During collaboration activities using cloud applications		
Incident Risk Ranking*	Included	Included		Included
Optical Character Recognition			Included	Included
Data Classification Integrations	Microsoft Azure Information Protection, Bolden James, Titus			
What data can I Fingerprint?*	Structured (databases), Unstructured (documents), Binary (non-textual files)			

*features available in IP Protection version. See Appendix C for further detail.

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

CONTACT

www.forcepoint.com/contact

©2017 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

[BROCHURE_FORCEPOINT_DATA_LOSS_PREVENTION_EN] 400026.112917