Forcepoint Data Loss Prevention

Know your data. Adapt to risk.
Protect everywhere.

Forcepoint

Brochure

Data Loss Prevention (DLP)

Safeguard Your AI Transformation with Forcepoint

Today's employees open Outlook, collaborate in SharePoint, ask Copilot a question, upload a file to ChatGPT, download a report, copy to USB, share through Teams, and access Salesforce, all before lunch. Data moves continuously across endpoints, cloud applications, email, web, and AI tools. Traditional security wasn't built for this. What's needed is a solution that's not only comprehensive, but intelligent enough to keep pace with how people actually work.

Forcepoint DLP prevents the exfiltration of sensitive data through unified policy management and centralized control. A single policy engine lets your security team define a policy once and enforce it consistently across every channel, giving you real-time control over sensitive data and user activity wherever work happens.

AI is transforming how your organization works, but it's also creating new data security blind spots. An engineer pastes proprietary source code into ChatGPT. A finance analyst uploads a forecast model to an AI assistant. A sales rep asks Copilot to summarize a deal that contains customer PII. These aren't policy violations by careless employees. They're people trying to get work done. The question is whether your security can let them innovate securely.

Forcepoint pairs advanced AI-powered classification with behavioral risk signals to deliver adaptive, intelligent protection. By continuously monitoring how people interact with data, the solution spots risk early and applies the right controls before data loss occurs, so your teams can use AI tools with confidence, not caution. Whether someone is working in Microsoft 365, uploading to a GenAI application, or accessing Salesforce from a home network, Forcepoint gives you centralized visibility and consistent control across every channel.

Unified Data Security. One Policy, Enforced Everywhere.

As regulations evolve (GDPR, HIPAA, DORA, NIS2, PCI DSS, CCPA, and emerging AI mandates), security leaders need a data protection strategy that scales without adding complexity. Forcepoint DLP makes that possible with over 1,800 predefined classifiers, templates, and policies aligned to regulatory requirements across 90+ countries and 160+ regions, with coverage for 900+ file types.

Trusted by organizations across financial services, healthcare, manufacturing, retail, government, and critical infrastructure worldwide, Forcepoint DLP delivers consistent protection from day one. Risk-Adaptive Protection responds to real-time user behavior and risk signals, keeping your security posture ahead of threats rather than chasing them.

Data Protection must:

- **Know** where your sensitive data lives, what it is, where it moves, and who is interacting with it across endpoints, SaaS, web, email, and AI interactions.
- **Adapt** protection continuously based on user behavior, business context, data sensitivity, and real-time risk signals so security responds intelligently, not rigidly.
- **Protect** sensitive data consistently across every channel (endpoint, email, web, SaaS, AI workflow, and AI agents) using a single policy engine.

Meet Alice

Alice is a sales rep preparing for a high-stakes partner meeting. She's doing her job. She's not trying to cause a security incident. **Watch what happens to sensitive data as she gets ready.**

Salesforce → Excel

Alice runs a report on her top strategic accounts in Salesforce and downloads it as an Excel file. The data, includes account names, contacts and revenue figures.

Regulated PII, IP and strategic account data exits a controlled CRM environment.

Excel → Cloud

She uploads the file to a collaboration platform to share with her team. SharePoint. Box. OneDrive. It doesn't matter.

Critical data now exists in multiple locations, accessible to anyone with permission.

Excel → Public AI

Alice uses a public AI tool to summarize trends and create talking points. She uploads the Excel file directly to the prompt.

Critical data has been uploaded to Shadow AI with a risky prompt.

AI Output → Slack

She shares the AI-generated summary with her team in Slack.

New content that includes elements of critical data spreads to a collaboration channel.

Slack → External Email

Alice emails the summary to a partner outside the organization.

Critical data is exported via the riskiest channel, with no access or audit controls.

What just happened?

PII. Intellectual property. Strategic insights. In one day, all of it has now exploded across collaboration platforms, cloud storage, AI tools and external trust boundaries. Alice didn't mean to cause a problem. She was simply trying to work smarter and faster. That's what makes insider risk so hard to manage: most of it isn't malicious. It's human.

Streamline Compliance

Regulatory requirements are multiplying, and each new mandate demands continuous proof that sensitive data is identified, controlled, and auditable. Many organizations still rely on fragmented DLP capabilities embedded in CASB or SWG tools, creating inconsistent enforcement and reporting gaps.

Forcepoint DLP cuts through that complexity. With the broadest library of pre-built regulatory content in the industry, Forcepoint accelerates deployment and simplifies ongoing compliance so your team spends less time configuring policies and more time protecting data.

- → **Regulatory coverage at scale.** Meet and maintain compliance across 90+ countries and 160+ regions with the industry's most comprehensive library of pre-built policies and classifiers, ready to go from day one.
- → **Centralized control.** Write a policy once and enforce it consistently across cloud applications, web, email, endpoints, and AI workflows.

Empower People to Protect Data

Block-only DLP policies frustrate employees and push them toward workarounds that create even greater risk. Forcepoint DLP takes a different approach: empower people to make good decisions about data while keeping the guardrails your organization needs in place.

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

- → **Discover and control data everywhere** it resides, across cloud applications, web, email, endpoints, and AI tools, with unified visibility from a single console.
- → **Coach employees** to make smart decisions, using custom 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** 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 is recognized by leading industry analysts as an enterprise DLP leader (IDC MarketScape Worldwide DLP 2025 Leader, Forrester Wave Data Security Platforms Q1 2025 Strong Performer, G2 Leader in Data Loss Prevention 2026), Forcepoint DLP identifies and protects data at rest, in motion, and in use across more than 900 file types.

Key detection capabilities include:

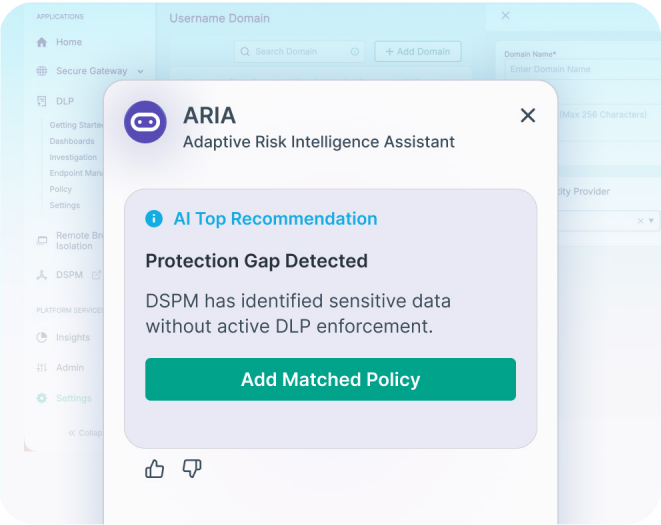
- → **Optical Character Recognition (OCR)** identifies data embedded in images while at rest or in motion.
- → **Robust identification** for Personally Identifiable Information (PII) offers data validation checks, real name detection, proximity analysis, and context identifiers.
- → **Advanced Fingerprinting** identifies structured and unstructured sensitive data with exact data matching, even when files are modified, renamed, or partially copied.
- → **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).
- → **Smarter enforcement** identifies 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.

"62% of breaches involve the human element" — Now add AI to the equation

- VERIZON, DBIR 2026

Adaptive Risk Intelligence Assistant (ARIA)

Managing data security at scale takes more than static rules. ARIA is an always-on AI assistant built into the Forcepoint Data Security Cloud with deep product knowledge and awareness of your environment. It removes the need for every administrator to be a DLP expert, helping teams deploy the right policies faster and get to value sooner.



- → **Natural language policy creation.** Describe what you need in plain language and ARIA translates your intent into enforceable DLP policies through Forcepoint's industry-leading policy engine. No specialized DLP expertise required.
- → **AI-powered investigations.** Ask ARIA about risky users, data movement patterns, or incident trends across any channel. Get answers in seconds, not hours.
- → **Intelligent recommendations.** ARIA analyzes cross-platform risk signals to recommend protection actions, identify policy gaps, and suggest enforcement adjustments, all while keeping full control in the hands of the administrator.
- → **Faster time to value.** ARIA draws on deep knowledge of Forcepoint capabilities and your specific environment to guide deployment, recommend policies, and surface the insights that matter most, so your team is effective from day one.

Identify, Manage and Remediate Data Protection Risk

Most DLP solutions overwhelm security teams with false positives while missing critical data at risk. That leads to analyst fatigue, frustrated employees, and blind spots that go undetected. Forcepoint DLP changes the equation by combining the industry's broadest pre-built policy library with AI-powered classification and behavioral analytics, cutting through noise to surface the incidents that actually matter.

- → **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.
- → **Employee coaching** comes in the form of pop-ups that can be personalized with the organization's name, a brief training statement for the reason for the pop-up, and a URL that users can click on to find more information on the organization's relevant security policy.
- → **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.
- → **Forensics and investigation**. Build a rich, auditable timeline of the events leading up to any incident. Give your security, compliance, and legal teams the evidence they need to demonstrate regulatory compliance, support internal investigations, and respond to legal proceedings with confidence.

Prevent Data Breaches in Real-time

The average cost of a data breach has reached $4.44M (IBM 2025), and it takes organizations an average of 241 days to identify and contain one (IBM 2025).

Forcepoint DLP helps your team detect and stop breaches in real time, before sensitive data leaves the building, with unified visibility, adaptive enforcement, and AI-powered investigation.

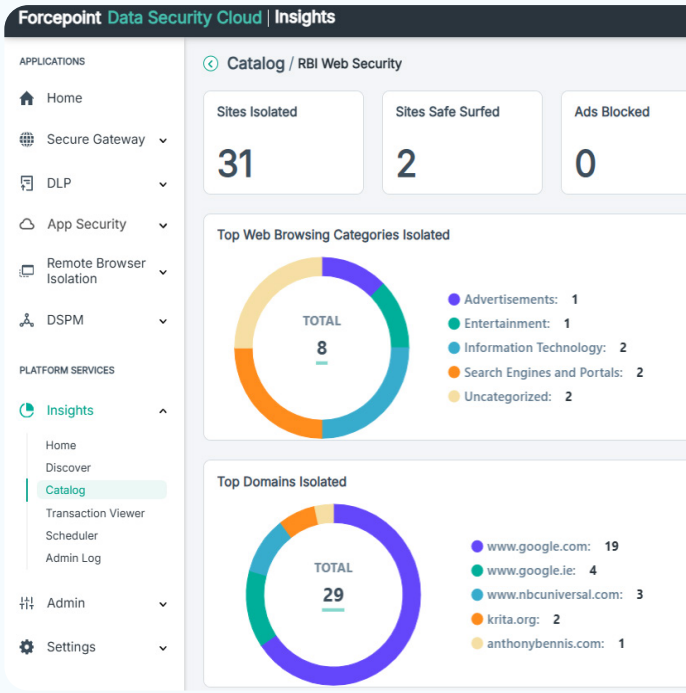
- → **Real-time monitoring and blocking:** Detect and stop data breaches as they happen, before sensitive information is exposed.
- → **Unified policy management:** Simplify security with a single console to manage policies across your environment for Data Security Everywhere.
- → **Cross-channel incident visibility:** Gain complete visibility into data movement across web, cloud, email, and endpoints for swift response to threats.
- → **Forensics:** Uncover the full story of data movement to investigate incidents, prevent breaches, strengthen policies, and ensure compliance.
- → **Risk-Adaptive Protection:** Dynamically adjust security controls based on user behavior and risk levels to ensure sensitive data stays protected without disrupting productivity. Forensics and investigation.

Executive Visibility with Forcepoint Insights

Effective data security is only half the story. Leadership teams also need to see the impact. The CISO Dashboard, powered by Forcepoint Insights on the Data Security Cloud platform, transforms operational DLP activity into executive-level insights and measurable business outcomes.

Instead of relying on raw logs and manually assembled reports, CISOs and leadership teams get a clear view of data risk, incident trends, program effectiveness, and the return on their DLP investment through intuitive dashboards, built-in analytics, and actionable smart recommendations.

- → **Demonstrate security outcomes.** Show the board what your data security program is delivering in business terms, not just alert counts.
- → **Strengthen executive reporting**. Purpose-built dashboards designed for leadership audiences, not SOC analysts. Ready to present without hours of manual preparation.
- → **Continuously improve.** Smart recommendations identify opportunities to tighten policies, close coverage gaps, and optimize your data security program over time.



Data Security Everywhere, Including Both in the Cloud and On-prem

A single employee's workday might span Outlook, SharePoint, Microsoft 365, Copilot, ChatGPT, a downloaded report, a USB drive, Teams, Salesforce, and a browser, from the office or the kitchen table. Data touches every one of those points, and each one is a potential exposure.

Forcepoint DLP supports flexible deployment across cloud, on-premises, and hybrid environments. You deploy based on your business needs, not your vendor's architecture, and maintain consistent protection everywhere.

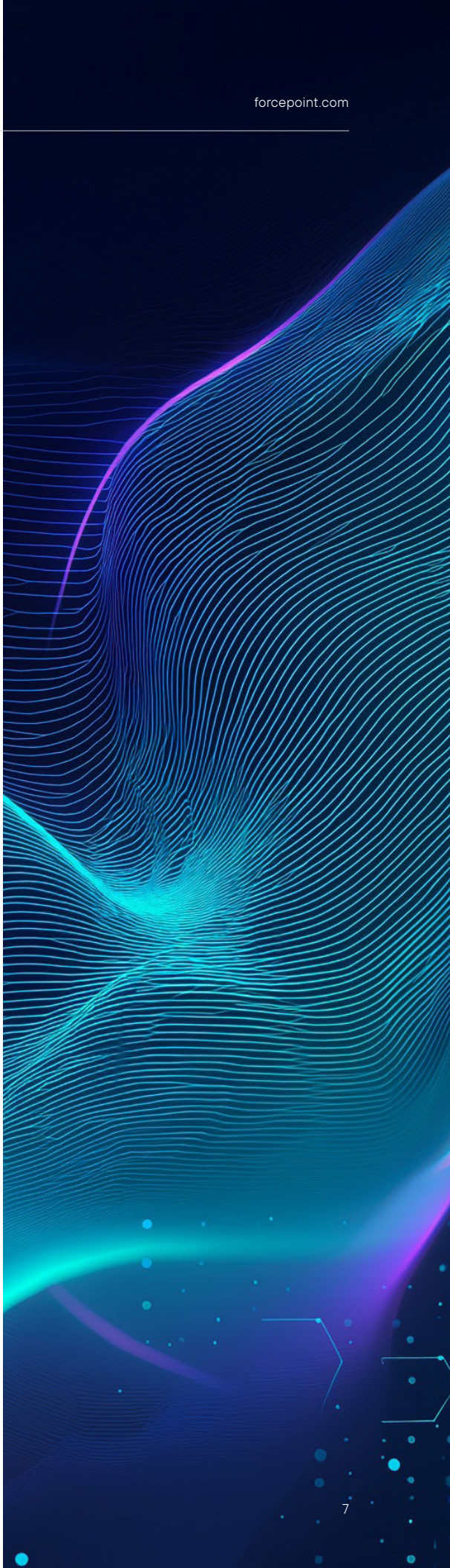
- → **Unified incident visibility.** See and respond to data security events across AI interactions, SaaS, web, email, and endpoints from a single investigation view.
- → **Identify and automatically prevent** sharing of sensitive data to external users or unauthorized internal users.
- → **Protect data** 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.
- → **One policy, enforced everywhere.** Define policies once and apply them across cloud, network, endpoints, web, email, and AI interactions from a single console.
- → **Flexible deployment.** Deploy cloud-native, on-premises, or hybrid. Keep incidents and forensic data within your data center for sovereignty and compliance requirements, or leverage the full Forcepoint Data Security Cloud for simplified operations. Modernize at your own pace with no forced migration.

For More Information About DLP.

Request a Demo

Schedule a tailored walkthrough with a Forcepoint expert.

Talk to an Expert



Forcepoint DLP Solutions

Forcepoint Data Security	Forcepoint Data Security, a cloud-native DLP solution, safeguards sensitive data, prevents breaches, and ensures global compliance. With rapid deployment and policy management, it streamlines data protection. It delivers unified management across cloud apps, web, email and endpoints. With Forcepoint Risk-Adaptive Protection, it offers real-time user risk insights. Experience reduced costs, risks, and increased productivity with Forcepoint Data Security.
Risk-Adaptive Protection	Unlike traditional policy-centric DLP solutions, our Risk-Adaptive Protection (RAP) puts people at the forefront, understanding behaviors to proactively mitigate risk. RAP prioritizes high risk users offering real-time risk calculations, 160+ behavior indicators, and frictionless deployment. Gain insights with easy to read dashboards, enhance productivity with granular policy enforcement, and proactively mitigate insider threats through dynamic automation.
Forcepoint Data Security for Email	Forcepoint Data Security for Email shields against sensitive data leaks across the critical email channel. This fully cloud-native solution fends off email breaches and data loss through email across both endpoints and mobile devices. Seamlessly integrated with popular email providers, it brings simplified management with pre-built security policies, classifiers and templates.
Forcepoint Data Security for Cloud Apps and Web	Forcepoint Data Security for Cloud Apps and Web provides the same fully cloud-native DLP solution as Forcepoint Data Security for Endpoint and Forcepoint Data Security for Email, allowing you to manage any or all of the 4 channels from a single user interface and to sync all policies from the same policy management console. Write policies once and deploy across all Forcepoint Data Security channels - saving time and resources syncing policies across multiple services.
Forcepoint Data Classification	Forcepoint Data Classification redefines data classification with AI Mesh enabled precision and automation, eliminating manual errors and enhancing DLP efficacy. We leverage AI Mesh technology and Large Language Models to deliver superior classification accuracy. Through continuous learning and improvement, it delivers confident recommendations, enhancing policy enforcement and compliance. Seamlessly integrate with your workflow, improve productivity, and reduce false positives.
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 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, 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 tosimplify your DLP management, writing one policy and deploying that policy across multiple channels. 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.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint enables Self-Aware Data Security, an AI-native approach that helps enterprises and governments know their data everywhere, adapt to evolving risks and regulations in real-time, and protect at scale with a unified, single-policy framework. 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, LinkedIn, Instagram and YouTube.

[FP-Brochure-DLP-US-EN] 10Aug2026