Forcepoint

Your Data Is Everywhere. Do You Know Where?

Data sprawl is the silent multiplier of AI risk. Here's what it means, why it matters and how to take back control.



Data Sprawl Amplifies AI Risk

Data sprawl happens when **sensitive information spreads across more places than your security team can see or control**: AI tools, data storage, SaaS apps, endpoints and everywhere in-between.

It's a natural byproduct of how modern organizations work. Every file copied, every prompt submitted to an AI tool, every document synced to a personal device adds to a data landscape that grows faster than traditional security was built to govern.

The Tangled Web Data Sprawl Weaves

On Endpoints

Files saved locally, on USB drives or personal devices — often outside IT's line of sight.

In AI Tools

Prompts, uploads and generated outputs that may contain regulated or proprietary information and bypass standard monitoring entirely.

In the Cloud

Cloud infrastructure where development teams build, test and deploy — environments like Azure, AWS and Google Cloud Platform where data lakes, databases and storage buckets can go unmonitored for months.

In SaaS Apps

Business-critical tools where sensitive data is stored, processed and sometimes over-exposed — think Salesforce, Workday, Slack and Dropbox.

On-Premises

Legacy servers, file shares and databases that often hold regulated data and intellectual property.

Why It Matters

Employee AI use and agentic AI accelerates the risk of data sprawl and limit confident adoption of these new technologies.

40% OF ALL AI INTERACTIONS INVOLVE SENSITIVE DATA[1]

45% OF EMPLOYEES USE UNAPPROVED AI TOOLS (SHADOW AI)[2]

73% SAY SHADOW AI CREATES INVISIBLE DATA EXFILTRATION PATHWAYS[3]

223 AVERAGE NUMBER OF AI-LINKED DATA POLICY VIOLATIONS PER MONTH[4]

[1] 2026 AI Adoption & Risk Report, Cyberhaven Labs | [2] 2026 DBIR, Verizon
[3] 2026 Cost of Insider Risks Global Report, Ponemon | [4] 2026 Cloud and Threat Report, Netskope

The Problem with Fragmented Data Security

- Most organizations can't tell you where all their sensitive data is, much less who has access to it.
- The typical enterprise security stack is a collection of disconnected point products, each with its own policies and its own blind spots. When data sprawls, those gaps multiply — leaving sensitive data in over-permissioned file shares, regulated information flowing through unapproved AI tools and ROT files accumulating risk you don't know you're carrying.

How to Reduce and Control Data Sprawl

Controlling sprawl starts with one continuous approach: discover what you have, classify what matters and protect it everywhere.

FORCEPOINT DATA SECURITY CLOUD

DSPM + DDR

Discover and Remediate
Forcepoint DSPM scans cloud, SaaS and on-premises environments to find and classify sensitive data. Add-on Forcepoint DDR extends that visibility with continuous, real-time monitoring — surfacing risks as they emerge, not after the fact.

DLP

Prevent Data Loss
Forcepoint DLP enforces consistent policies across endpoints, email, web and cloud channels. One policy framework. Up to 90% fewer policies to manage.

Web Security + CASB

Extend Protection
Forcepoint Web Security controls web traffic and AI tool usage. Forcepoint CASB governs data across sanctioned cloud apps. Both run on the same platform, policies and console.

The Outcome

ORGANIZATIONS USING FORCEPOINT DATA SECURITY CLOUD GAIN:

- Unified visibility across AI, SaaS and endpoints
- Automated discovery and AI-powered classification
- Real-time detection and response to emerging data risks
- Up to 31% reduction in operational costs*
- Confidence to enable AI without exposing sensitive data

*IDC White Paper, sponsored by Forcepoint, #US51035023, Jan 2024

Know your data. Adapt to risk. Protect what matters.

See how Forcepoint Data Security Cloud helps you tame data sprawl.

EXPLORE DATA SECURITY CLOUD

Forcepoint

© 2026 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.
[FP-Data Sprawl Infographic-EN] 30Jul2026