Forcepoint

Your Data Is Everywhere. Do You Know Where?

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

What Is Data Sprawl?

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

Where Does Your Data Live?

On Endpoints

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

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.

In AI Tools

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

On-Premises

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

Why It Matters

When data is everywhere, risk is everywhere.

$4M

GLOBAL AVERAGE COST OF A DATA BREACH
IBM/PONEMON COST OF A DATA BREACH REPORT 2025

$19M

AVERAGE TOTAL ANNUAL COST OF INSIDER RISK SECURITY INCIDENTS
2024 COST OF INSIDER RISKS GLOBAL REPORT, PONEMON/DTEX

$5M

AVERAGE COST WHEN BREACHED DATA SPANS MULTIPLE ENVIRONMENTS
IBM/PONEMON COST OF A DATA BREACH REPORT 2025

73%

OF ORGANIZATIONS SAY UNAUTHORIZED AI USE IS CREATING INVISIBLE DATA EXFILTRATION PATHWAYS
2026 COST OF INSIDER RISKS GLOBAL REPORT, PONEMON/DTEX

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 cloud, SaaS, endpoints and AI tools
- 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, #US53135023, Jan 2024

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

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

GET A FREE DATA RISK ASSESSMENT

Forcepoint