FORTRA

Data Security Posture Management (DSPM) Buyer's Guide

Table of Contents

Executive Summary

The New Reality of Data Security

Today's organizations face complex security challenges: Cloud sprawl, shadow data, and patchwork solutions all make protecting critical assets far more difficult than it should be.

You can only protect what you can see, which is why visibility is the cornerstone of effective data protection.

Without complete transparency into where data resides and how it's secured, security teams must guess where to focus resources. This process creates inefficiencies and gaps in protection.

Executive Summary

Gain Control with DSPM

Data Security Posture Management (DSPM) helps organizations find, classify, and protect sensitive data, wherever it lives:

- Structured or unstructured
- On-premises, cloud, or hybrid
- Vulnerabilities, misconfigurations, and risky access

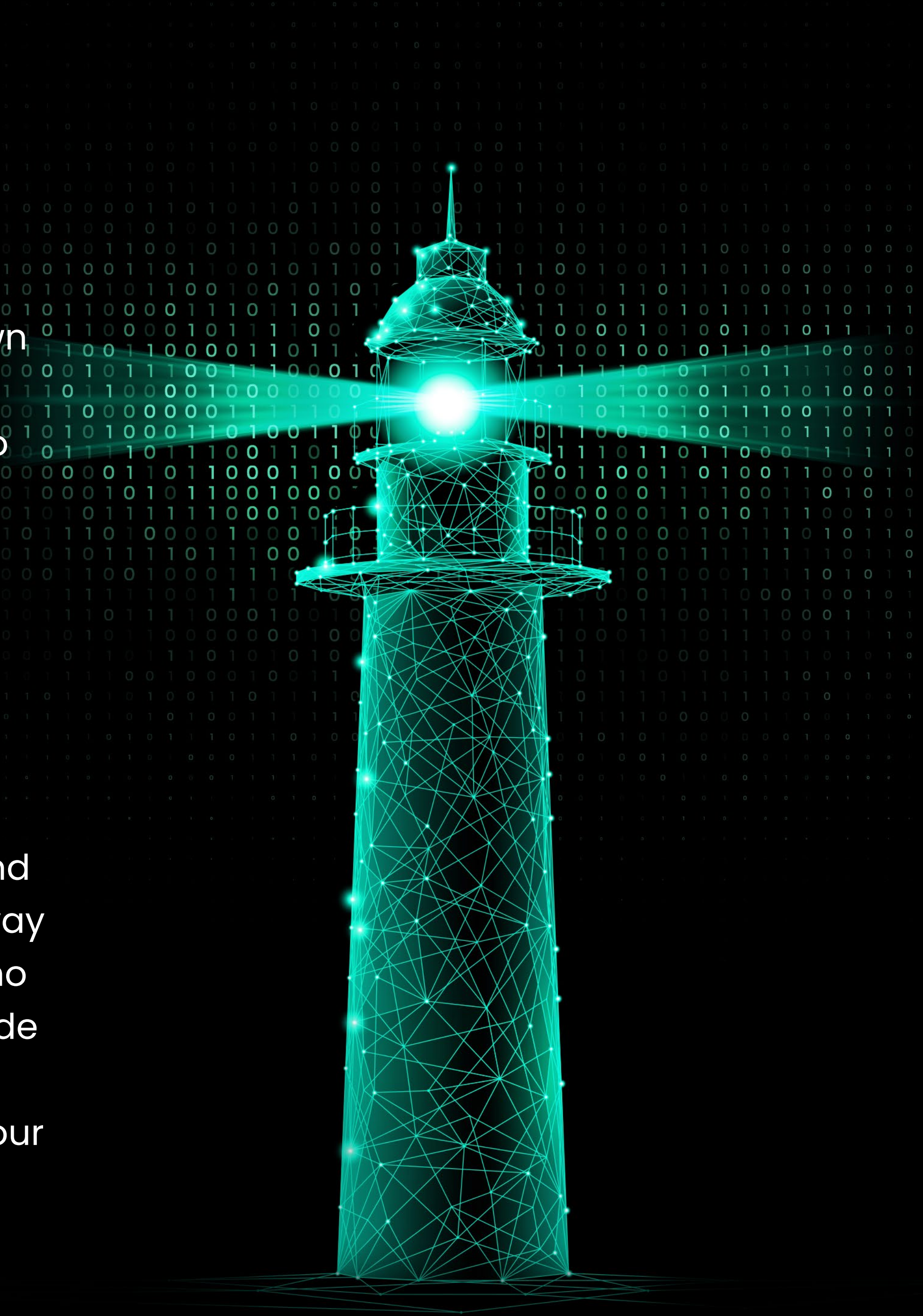
DSPM provides a critical visibility layer across all assets, unifying tools into one central dashboard. That means no more security blind spots for attackers to exploit. Only full visibility, full classification, and full control.

Executive Summary

In this Guide

This DSPM buyer's guide provides a clear breakdown to what modern DSPM solutions should deliver, key capabilities to evaluate, and how these tools fit into a broader data protection strategy. The guide also highlights how an integrated approach — such as combining DSPM with established data protection controls like data loss prevention (DLP) — can help organizations move beyond visibility to more effective, scalable protection.

As data continues to spread across cloud, SaaS, and on-prem environments, teams need an effective way to understand where sensitive information lives, who can access it, and how it may be exposed. This guide will help you cut through the complexity, evaluate DSPM vendors with confidence, and future-proof your data security strategy.



What is DSPM and Why It Matters

Data Security Posture Management is a modern cybersecurity solution that automatically finds and classifies data across complex landscapes, so organizations have the visibility and control they need to keep it secure.

Before DSPM, teams had to bolt together disparate tools and do the work of unifying telemetry, analyzing results, and classifying outcomes themselves. Then, they would have to integrate with even more tools to protect that data. Thanks to DSPM, security teams have a unified solution that delivers:

Visibility

Find sensitive data wherever it lives — in the shadows or otherwise.

Control

Assess how data is vulnerable to attack. Classify it based on business impact, sensitivity, and compliance.

Confidence

Scale easily and achieve top-tier data protection affordably.

What is DSPM and Why It Matters

DSPM Business Benefits

The ability to see, manage, and control all sensitive assets easily leads directly to downstream business benefits:

- **Cloud migration:** Protect what matters when uploading data. Ensure on-prem compliance policies remain intact or are effectively replaced when migrating to the cloud.

- **Accurate AI models:** Ensure only authorized users can access or alter information in data lakes that feed your AI models and, ultimately, your business decisions. Keep it classified, secure, and easily accessible for high-level analytic retrieval.

- **Compliance:** Meet regulatory obligations, such as GDPR or CCPA, with confidence. By knowing exactly what data you hold and where it resides, your organization can respond confidently to audit requests, demonstrate appropriate safeguards, and fulfill data subject rights — such as access and deletion — without manual effort or uncertainty.

- **Mergers and acquisitions:** Let nothing fall through the cracks when integrating sensitive data. Identify and secure vital assets early on, adding an extra layer of protection against exposure when merging systems.

Top Challenges DSPM Solves

DSPM emerged as a response to siloed tools, complex security architectures, manual data inventory and classification, and patchwork workflows — problems that created overlapping responsibilities, security gaps, and operational inefficiencies. These challenges slow down internal security teams by forcing them to spend time chasing data locations and validating risks instead of focusing on higher-value work.

Without Data Security Posture Management, organizations often struggle with security and business challenges:

1. **Increased cost of a data breach:** Security gaps from overlapping tools and incomplete data visibility allow attackers to operate undetected. Without a clear view of where sensitive data resides, breaches take longer to identify and contain, increasing financial impact. Research shows the longer a breach goes unnoticed, the costlier it becomes — including downtime, which can reach up to $9,000 per minute depending on the industry and business size.
2. **Insider threats:** Visibility blind spots provide opportunities for savvy inside threat actors to move around. It also increases the chances of unintentional users making accidental mistakes (saving files to the wrong places, accessing sensitive documents beyond their scope).
3. **Compliance fines:** When teams are busy trying to synthesize data from disparate tools, they operate in emergency mode. There's barely enough time to hunt down active threats, much less stay ahead of compliance mandates. This creates a perfect storm of visibility gaps, inadequate reporting, heightened breach risk, and the inevitable compliance fines that follow.
4. **Trouble scaling SecOps:** Thanks to tool sprawl, much of a team's energy is spent aggregating and analyzing telemetry, rather than hunting threats. This method is hardly sustainable, much less scalable.
5. **Insecure AI usage:** Not knowing where your data resides — let alone what it contains — creates information black holes. As AI and LLM systems rely on complete data to produce accurate results, these data gaps lead to faulty analysis and incorrect conclusions that can lead to misguided business and security decisions.
6. **Limited ROI on security investments:** Tool sprawl is widely acknowledged to be counterproductive; with nearly 60% of organizations owning 41 security solutions or more, 85% of them have plans to consolidate or have already started. DSPM allows teams to maximize existing tools by consolidating and optimizing use, rescuing their ROI and driving efficiency.

Without Data Security Posture Management, organizations often struggle with security and business challenges:

7. **Discovering and classifying data at scale:** Security teams face numerous alerts, duplicate signals, and false positives. Without DSPM, much of this data must be sorted manually, leaving visibility gaps and limiting the ability to proactively identify sensitive assets. With petabytes of data sent every day, automated, unified discovery and classification is the only sustainable approach.

8. **Blocking business growth:** As businesses' growth is hampered by siloed security solutions and the drained resources of maintaining them, security leaders will be held accountable for not fulfilling their number one emerging role: defending the bottom line.

As organizations move beyond single-vendor ecosystems, DSPM integrates seamlessly with existing security investments. It acts as a critical visibility layer that fills gaps, eliminates shelfware, and reduces complexity. This allows teams to consolidate tools and achieve desired outcomes.

DSPM

Top Challenges DSPM Solves

Issues Addressed by Most DSPM Vendors

Organizations often rely on multiple tools, including IAM, DLP, code security tools, and cloud-native controls, each offering only a partial view of where sensitive data resides and how it is protected.

DSPM acts as the connective layer across these systems, discovering the data those tools are designed to protect, classifying it, and providing unified visibility so existing controls can be applied consistently and intelligently. Rather than replacing existing tools, DSPM strengthens them by ensuring every security investment operates from the same accurate understanding of your data.

Here's how DSPM integrates with and enhances your existing security stack:

1. **Eliminates security blind spots:** DSPM uncovers sensitive and shadow data across all environments, giving your existing tools the visibility they need to enforce the right controls with precision.
2. **Simplifies compliance complexity:** By continuously discovering and classifying data, DSPM provides compliance, DLP, and identity teams with a single, authoritative data inventory. This supports consistent least-privilege access, precise policy enforcement, and rapid audit responses.
3. **Unifies visibility across platforms and users:** DSPM enhances SIEM, XDR, and other monitoring tools by revealing how data flows between users and systems. With this cross-platform context, previously siloed tools can correlate events and respond more intelligently.
4. **Supports the secure development life cycle (SDLC):** DSPM identifies sensitive data stored in code repositories or used in development environments. By integrating with SDLC and DevSecOps tools, DSPM enforces the right controls earlier in the pipeline, reducing the risk of accidental data exposure before release.
5. **Makes zero trust network architecture (ZNA) operational:** Zero trust relies on accurate, up-to-date knowledge of the data protected by access rules. DSPM integrates with IAM and ZNA frameworks by continuously classifying data so access controls can be applied consistently and at scale.
6. **Discovers and classifies data at scale:** DSPM feeds discovered assets and classifications into existing tools — cloud security platforms, DLP, collaboration controls, and ticketing systems — providing the context they need to prioritize and protect sensitive information across:
   - Code repositories and GenAI
   - Cloud storage
   - Collaboration platforms
   - CRM and business systems

This unified view enables faster investigations, fewer false positives, and more targeted enforcement of data protection policies.

DSPM tackles core security challenges by discovering and classifying data at scale. However, without integrated protection, organizations remain exposed — making it essential to choose a DSPM vendor that both identifies and safeguards sensitive data.

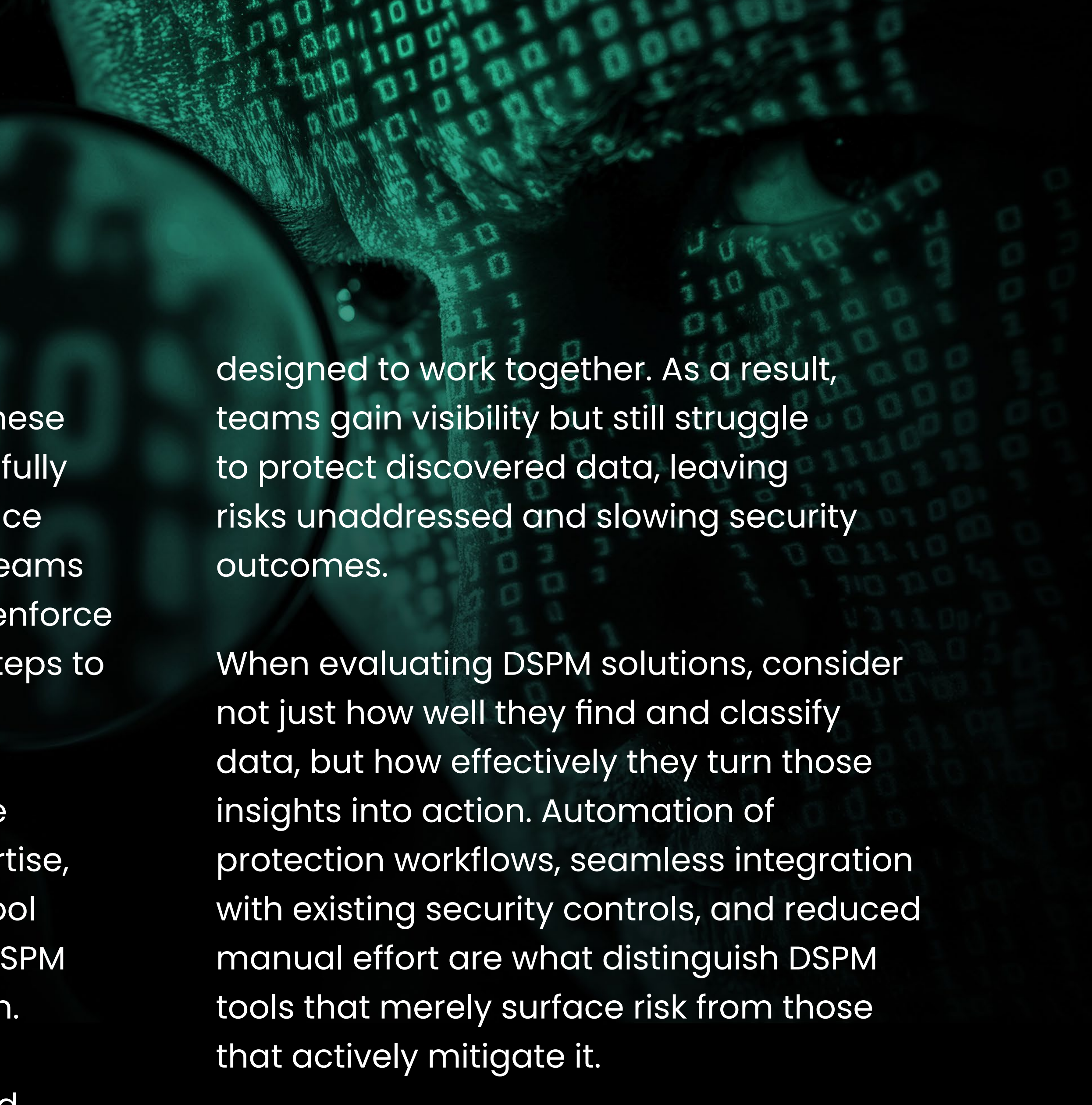
Top Challenges DSPM Solves

Classic vs. Modern DSPM

Classic DSPM solutions recognize the value of finding and classifying data to feed downstream data protection tools. Modern DSPM solutions go the extra step of integrating data security directly. They also offer flexible deployment options, secure both structured and unstructured data, and more.

This table breaks down the key differences.

CLASSIC DSPM	MODERN DSPM
Data Discovery and Classification Only	**Data Discovery, Classification, and Protection:** Integrates with SIEM, SOAR, EDR, and DLP tools to reduce data exposure.
Emphasis on Secure Cloud Storage	**Secures from Endpoint to Cloud:** Protects data, regardless of where it resides, including cloud devices, collaboration tools, and shadow repositories.
Label-based Classification	**Classification Beyond Labels:** Captures real context and classifies data by what's sensitive, regulated, and business critical.
Possible Integration with Downstream Tools	**Guaranteed DLP Integration:** A built-in "classification-to-policy" loop ensures controls are enforced accurately, reducing risk far beyond what standalone discovery tools can achieve.
One-time Scans	**Continuous Monitoring:** Proactively monitors your data to detect new misconfigurations, data changes, vulnerabilities, and risky paths.
Bolted-on Security Tools	**Unified Security Portfolio:** Can be integrated with a larger, unified security stack, including: • DLP • CASB • ZTNA
Risk Detection	**Risk Prioritization:** Leverages context to identify the most critical risks, creating intelligence-driven results.
Point-in-Time Data Scan	**Dynamic, Real-time Inventory:** Flexible protection adapts as your environment grows, securing new data stores the moment they appear. DSPM mean-time-to-exploit is just five days.



What to Look for in a DSPM Solution

Many DSPM vendors focus only on discovery and classification. While these capabilities are essential, they don't fully solve the operational challenges. Once sensitive data is identified, internal teams must manually manage workflows, enforce controls, and execute remediation steps to secure it.

For many organizations, this is where real gaps appear. Limited staff expertise, competing priorities, and complex tool stacks make it difficult to translate DSPM findings into consistent, timely action. Manual remediation doesn't scale, introduces the risk of errors or missed steps, and often relies on tools not designed to work together. As a result, teams gain visibility but still struggle to protect discovered data, leaving risks unaddressed and slowing security outcomes.

When evaluating DSPM solutions, consider not just how well they find and classify data, but how effectively they turn those insights into action. Automation of protection workflows, seamless integration with existing security controls, and reduced manual effort are what distinguish DSPM tools that merely surface risk from those that actively mitigate it.

Choose a DSPM solution that delivers these essential features:

FEATURE	DESCRIPTION
Complete Data Discovery	Automates continuous discovery of sensitive data across all environments, including shadow apps, misconfigured cloud platforms, and silos.
Classification	Uses advanced automation and AI to categorize sensitive data based on business impact, sensitivity, and compliance requirements.
Risk Prioritization	Evaluates risk using multiple factors, such as likelihood of exploitation, data sensitivity, business impact, and exposure context.
Continuous Monitoring	Provides real-time visibility into new data assets and emerging risks, detecting misconfigurations, vulnerabilities, and improper access controls.
Sensitive Data Protection	Integrates with data protection controls, securing sensitive data quickly and consistently without adding operational burden.

The Buyer's Checklist: Questions to Ask Vendors

To maximize the value of your DSPM investment, get the answers to these key questions from potential vendors.

1. How does the solution scale with data growth and multi-cloud expansion?

DSPM should provide unified visibility across all environments. Ensure the DSPM vendor provides coverage across these environments:

- SaaS
- IaaS
- PaaS
- On-premises
- Cloud
- Hybrid
- Backups

2. How quickly does your solution deliver meaningful insights?

A DSPM solution's key goal is to reduce cycle time for internal security operations centers (SOCs) attempting to identify exposed assets on their own. Choose a tool that uses AI to accelerate the process, learns your unique environment, and delivers customized, accurate insights. Ask how quickly the platform begins to discover sensitive data and produce an initial risk assessment once deployed.

3. Does your solution integrate with our existing data protection tools?

Gaining rapid insights into your environment is one thing; acting on them is another. For this to occur, you need intuitive integration. For maximum effectiveness, ensure the DSPM product supports seamless integrations with DLP, CSPM, IAM/PAM, SIEM, and other security platforms.

5. How transparent is risk reporting?

Look for a tool that offers unified risk reporting in real-time with contextual enhancements, so you not only see risks but understand them across your attack surface. Ensure it provides explainable scoring, prioritized findings, and why something is flagged.

4. What ongoing support does the solution provide?

Look for a vendor that provides dedicated support to shorten the learning curve and achieve ROI faster. Prioritize solutions designed for low-touch operation, automation, and minimal configuration or policy maintenance.

6. How does the solution scale with data growth and multi-cloud expansion?

DSPM must scale with growing data volumes and evolving architectures. To replace fragmented point solutions, it should constantly discover, classify, and protect both structured and unstructured data across any telemetry at scale.

The Fortra DSPM Difference

Fortra DSPM doesn't just find and classify your data — it automatically orchestrates protection across your entire digital ecosystem. By learning your organization's unique DNA, it leverages those insights to anticipate threats.

While many vendors deliver DSPM and DLP as separate, loosely connected tools, Fortra takes a unified approach. Our cyber platform brings data discovery, classification, and protection together in one ecosystem, helping teams close visibility gaps and enforce consistent controls as data evolves.

With DSPM, Data Loss Prevention becomes more effective. DSPM provides the upstream visibility DLP has traditionally lacked — a complete inventory of sensitive data, and classification by sensitivity, business impact, and context. This allows our DLP tools to apply the right policies to the right data, rather than relying on reactive or manually built rules:

- **Network DLP:** Controlling the flow of sensitive data across your network is easier and more accurate when asset sensitivity levels are clearly defined.
- **Endpoint DLP:** DSPM maps who has access to what data and which systems should interact with it, enabling EDR tools to more easily spot when something is awry.

Datasets finely tuned by Fortra DSPM feed downstream tools such as Fortra DLP, enabling them to orchestrate workflows, set policies, and enforce controls more efficiently.

The Fortra DSPM Difference

Why Fortra DSPM Stands Out

Fortra's integrated portfolio streamlines risk management, reduces operational friction, and ensures critical information is safeguarded across endpoints, cloud, and hybrid environments.

Here's how.

- **Unified platform:** Fortra DSPM integrates seamlessly with Fortra Data Classification and Fortra DLP, minimizing friction and redundancies while optimizing workflows.
- **Depth and accuracy:** Gain granular visibility across both structured and unstructured data, transcending the limits of other vendors while building scalable defenses as your data grows.
- **Trusted expertise:** Fortra has over 40 years of experience in data protection and compliance, with a long-standing focus on preventing data exposure and loss in complex environments.
- **Scalable for the enterprise:** Our flexible deployment adapts to any environment, large or small.
- **Wide-search capabilities:** Locate sensitive data across cloud, SaaS, and on-premises environments.

The Fortra DSPM Difference

Fortra DSPM: Built for the Future

Fortra leads the way in DSPM innovation, and that future is powered by intelligent, predictive AI.

Unlike solutions that require manual set up, Fortra automatically learns your data landscape. It distinguishes between the spreadsheet that runs your quarterly planning and the one someone forgot in a shared drive.

No rulebooks. No endless configuration. Just an immediate understanding of what you have, where it lives, and why it matters.

The result?

- Your team stops playing data hide-and-seek and starts making decisions with complete information.
- Compliance becomes a byproduct of clarity, not a scramble to catch up.
- Instead of chasing shadows, your people focus on building the business forward.

Fortra DSPM: Because knowing what you have is the first step in protecting what matters.

Is your cloud data at risk?
We can help you find out.

Sign up for our free Data Risk Assessment and find out where your data might be hiding.

GET STARTED AT FORTRA.COM/DRA

FORTRA

ABOUT FORTRA

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.