



DATASHEET (FORTRA)

Fortra DSPM

Map and Secure Your Entire Data Landscape

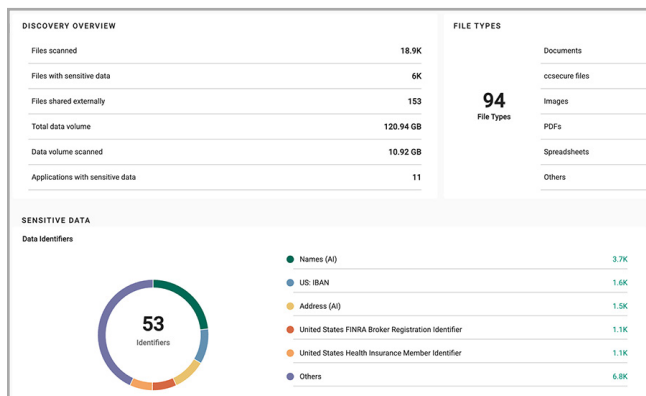
Sensitive data is everywhere: across cloud applications, SaaS platforms, endpoints, and shadow IT environments. As organizations create, store, and share more data than ever before, security teams face a growing challenge: understanding where their sensitive information lives, who has access to it, and how to protect it before attackers exploit it.

Fortra DSPM helps organizations discover, classify, and protect sensitive data across their entire environment based on sensitivity, risk, and context. By combining deep visibility with risk-based prioritization and integrated protection, Fortra enables organizations to reduce exposure, improve compliance, and strengthen overall data security posture.

PRODUCT HIGHLIGHTS

- Data visibility across hybrid environments
- Risk-based enforcement & remediation
- Proactive risk mitigation
- Faster incident response

Discover Sensitive Data Across Your Environment



Gain a centralized view of sensitive data across your environment, including discovered file types, external sharing activity, compliance exposure, and high-risk data identifiers.

Shine a Light on Shadow Data

Organizations can't secure the sensitive information they can't see.

Fortra DSPM continuously discovers sensitive data across your entire data environment, including cloud services, SaaS applications, on-network file shares, databases, and more helping organizations uncover shadow IT, undiscovered and/or unclassified data, and the unmanaged risk they create.

With real-time discovery capabilities, security teams gain visibility into:

- Where sensitive data resides
- How data moves across the environment
- Who has access to what data
- Which data assets present the greatest risk

The deeper visibility that Fortra DSPM delivers creates the foundation for smarter, more informed security decisions and faster incident response. Leveraging our enterprise-grade AI classifiers, our solution was found to be **over 95% accurate** in testing, maximizing data discovery precision and consistency while minimizing false positives.

Key Benefits

- Improved visibility across SaaS data stores, public cloud, on-network file shares and databases, and hybrid environments
- Better understanding of data movement and usage
- Faster identification of the highest-risk exposures
- Reduced blind spots caused by shadow data and shadow IT

Enrich Data with Context

Identify Critical Risks and Reduce Noise

Unlike many DSPM tools that simply identify files or repositories on a surface level, Fortra DSPM automatically classifies sensitive, regulated, and business-critical data while specifically considering its context, risk profile, and importance to the organization.

This allows security teams to:

- Prioritize the most critical, high-fidelity risks first
- Reduce alert fatigue
- Focus remediation efforts effectively
- Support and ease regulatory and compliance initiatives

By understanding both the sensitivity and context of data, organizations and their users can make more informed decisions about protection and access. Moreover, this critical context allows downstream security tools like DLP to enforce policies and implement controls more effectively and accurately.

Key Benefits

- Automated classification of sensitive and regulated data
- Risk-based prioritization to reduce operational overload
- Improved compliance readiness
- More efficient remediation workflows

Hybrid DSPM for Modern Organizations

DATA DISTRIBUTION			
SaaS Applications			
AWS_Cloudupnetworks.s3	4.1K	Box_Cloudupnetworks_V1	926
GoogleWorkspace.gdrive	868	Azure_Cloudupnetworks.azureblob	453
Salesforce	14	Salesforce	2
M365_Cloudupnetworks.sharepoint	900	M365_Cloudupnetworks.onedrive	874
GitHub_CloudUpNetworks	105	Slack	95
File Servers			
FSx_ONTAP_MortgageApp	3.8K	FSx_Win_corporatedata	3.1K

See where sensitive data lives across SaaS applications, cloud storage, and file servers to uncover shadow data and prioritize protection efforts.

Enforce Data Protection from Endpoint to Cloud

While DSPM vendors now usually offer solutions delivering both cloud and on-network visibility, organizations may find that they are more tailored to one or the other as opposed to delivering comprehensive visibility into hybrid environments.

Fortra delivers an integrated security approach that extends protection to customer-hosted infrastructure, cloud environments, and SaaS applications — helping organizations with hybrid environments reduce friction while maintaining consistent policy enforcement.

By continuously assessing data security posture, Fortra DSPM helps organizations identify:

- Misconfigurations
- Excessive access rights
- Shadow data
- High-risk exposures

Moreover, Fortra DSPM enables accurate, consistent policy enforcement through both inherent capabilities and integrations with solutions like DLP. Using the context applied to data after discovery, our solution can then apply the proper remediation and policy enforcement actions, including blocking, masking, redaction, and more. This proactive approach enables teams to remediate risks before they become breaches.

Key Benefits

- Proactive risk mitigation
- Faster remediation of data exposures
- Reduced time and cost of incident response
- Consistent protection across the data ecosystem

Why Organizations Choose Fortra DSPM

Improved Visibility Across Data Environments

Map sensitive data — including shadow data — across on-premises, cloud, and SaaS environments to gain complete visibility into data storage, movement, and usage.

Risk-Based Prioritization

Focus on the data that matters most by prioritizing risks based on sensitivity, exposure, and business impact.

Proactive Risk Mitigation

Identify misconfigurations, risky data actions, and unnecessary access, and apply proper policy enforcement or remediation measures to prevent breaches and attacks.

Faster Incident Response

Accelerate investigations and remediation with streamlined workflows and integrated security capabilities.

Secure Your Data with Confidence

Fortra's unified, hybrid approach to DSPM empowers organizations to discover hidden risks, classify sensitive data and enrich it with critical context, and enforce protection across modern environments, allowing organizations to create, use, and share sensitive data with confidence.

FORTRA[®]

Fortra.com