FORTRA

# Fortra Data Security

Interlocking solutions that protect sensitive data while keeping users productive.

# Fortra Data Security

AI-driven data growth and cloud adoption are exploding, and businesses need a way to protect their most critical information across endpoints, cloud and collaboration tools.

It's already a massive challenge, and it's getting bigger as companies embrace AI and run their operations online.

Fortra's strategy is to build the first unified data security platform that connects discovery, classification and protection, so organizations can see where sensitive data lives, understand its risk and enforce policies everywhere data moves.

We have 25,000 customers, 2,200 employees, and $750M in annual revenue, with a clear path to $1B on our way to becoming the leader in data security.

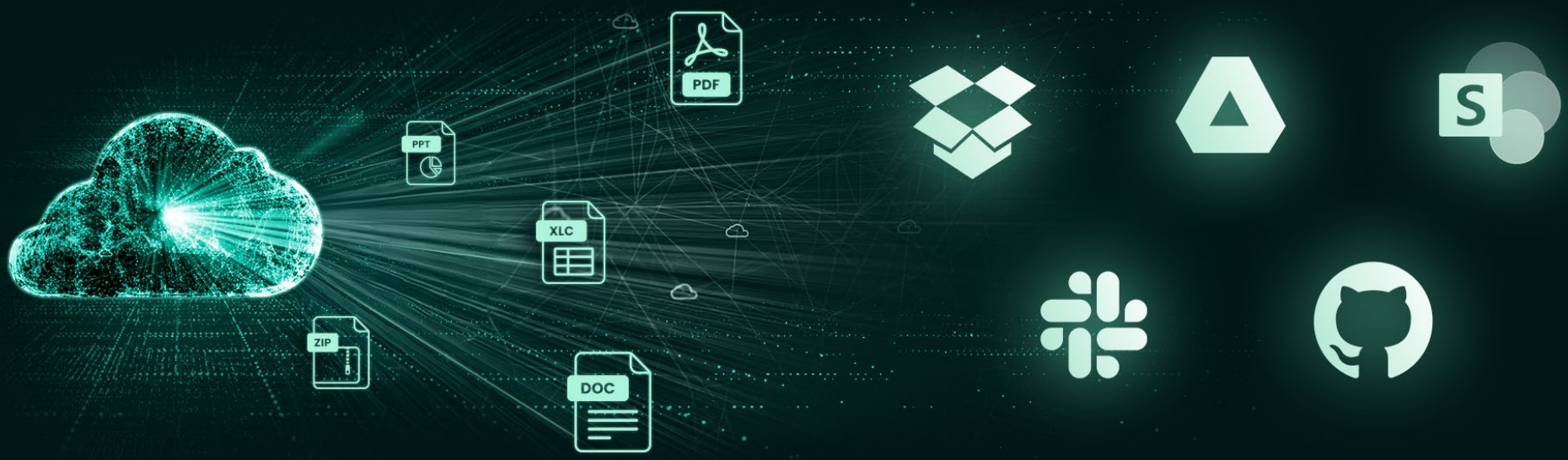
# Fortra DSPM

## Data Security Posture Management

Fortra DSPM gives you the complete visibility you need to stay ahead of data risk by first shining a light on every piece of sensitive information across your hybrid and multi-cloud environments.

Our DSPM automatically discovers real-time inventory of data – whether it lives in sanctioned apps, shadow IT or AI workflows – and intelligently classifies what is sensitive, regulated, or business-critical so security teams can focus on what truly matters.

This rich, context-aware classification then becomes the policy "brain" for downstream controls, seamlessly feeding Fortra's integrated DLP to enforce precise protection that keeps critical data safe from endpoint to cloud while reducing noise, complexity, and operational overhead.



## Data Is Everywhere

**90%** of the world's data was created in the past 2 years. Data environments are larger and more complex than ever.

## AI Is Booming

**80%** of AI data is unprotected. Data governance has quietly become the greatest risk for most organizations.

## Legacy Tech Can't Keep Up

**75%** of organizations lack visibility into data created in their own environment, let alone how it is used, stored, or moved.

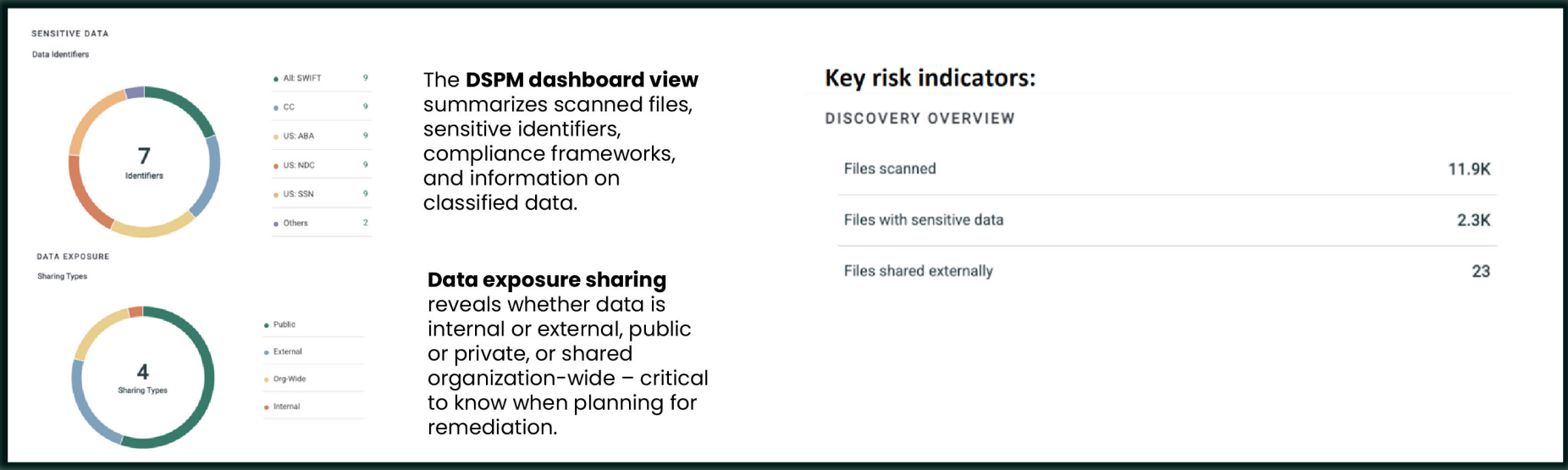
---

Fortra DSPM lets you **discover** your data wherever it lives, **classify** it no matter what it is, and **protect** it with unmatched control.

## Discover

## Classify

## Protect




The **DSPM dashboard view** summarizes scanned files, sensitive identifiers, compliance frameworks, and information on classified data.

**Data exposure sharing** reveals whether data is internal or external, public or private, or shared organization-wide – critical to know when planning for remediation.

**Key risk indicators:**

DISCOVERY OVERVIEW

| | |
|---|---|
| Files scanned | 11.9K |
| Files with sensitive data | 2.3K |
| Files shared externally | 23 |

FORTRA

# Fortra DLP

## Data Loss Prevention

Fortra DLP gives you immediate visibility into your organization's assets and helps provide a streamlined path to security maturity.

We know data loss prevention can be complex... but it doesn't have to be.

Our market-leading DLP is backed by decades of focus, solving real use cases. From basic data protection requirements to today's common cloud, hybrid, and remote work environments, we can help you protect workflows across your entire organization.

600 customers worldwide use Digital Guardian to discover, monitor, log, and block threats to their data with pre-built policies that help them avoid gaps and comply with evolving regulatory changes.

aws **Available in AWS Marketplace**

Know what you need to protect? Have use cases to meet? Just trying to discover and better understand your data? Fortra's data protection experts will work with you to customize rules and policies for both bottom-up and top-down approaches.


## Sensitive data comes in many forms

Fortra DLP helps organizations identify and mitigate risks to all types of sensitive data, including source code, credit card info, HR details, intellectual property, and more.

### ENDPOINT DLP

- Stop the printing of HR files – even printing to PDF
- Stop the saving of critical documents to USB drives unless explicitly authorized

### NETWORK DLP

- Avoid accidental emailing of sensitive documents to competitors or across national borders
- Only enable approved AI tools and stop copy & paste of important stuff like source code.
  ChatGPT, Google Gemini
- Identify outside impersonation attacks and provide effective remediation
  Microsoft Teams, Slack

### CLOUD DLP

- Protect data stored in both sanctioned and unsanctioned apps
  SharePoint, Google Workspace
- Manage file uploads to cloud storage according to your business policies
  Box, Dropbox


# Endpoint DLP

Delivers the deepest visibility available on the market. Our agent captures and records all system, user, and data events – on or off the network.

# Network DLP

Supports compliance and reduces data loss risks by monitoring and controlling the flow of sensitive data via the network, email or web.

# Analytics & Reporting Cloud (ARC)

Get fast and intuitive visibility to DLP actions, analytics, workflows, and reporting.

Unlike other “free” DLP tools, Fortra offers cloud-based analytics for which there are no unforeseen additional costs, and don’t require an external tool.

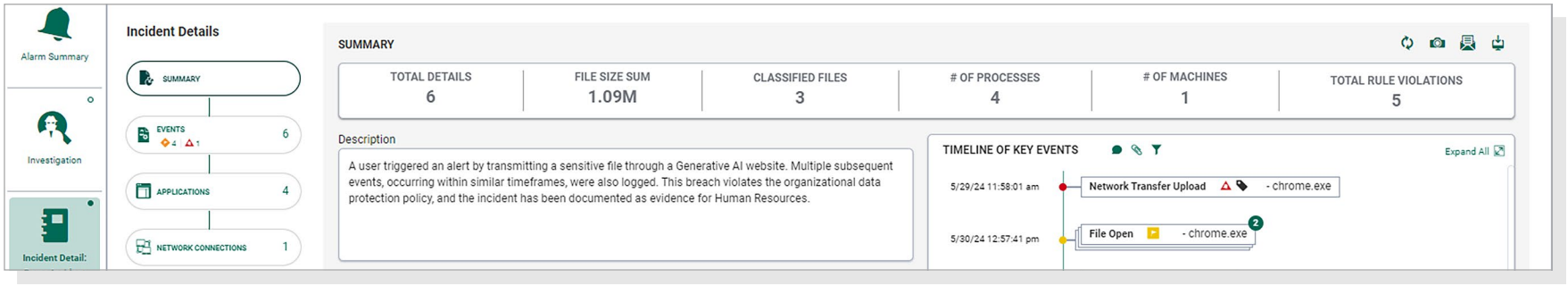
Running on Amazon AWS, ARC correlates and analyzes system, user, and data events  to provide the visibility and context you need to identify and remediate threats.

# Managed DLP

Focus on your core business and leave data protection to our security experts.

Even if your organization has a mature security team in place, it can still be difficult to stay on top of all today’s threats.

Let Fortra’s Managed Security Program fill your security talent gap and leverage our experience implementing mission critical data security, incident response, and compliance programs.

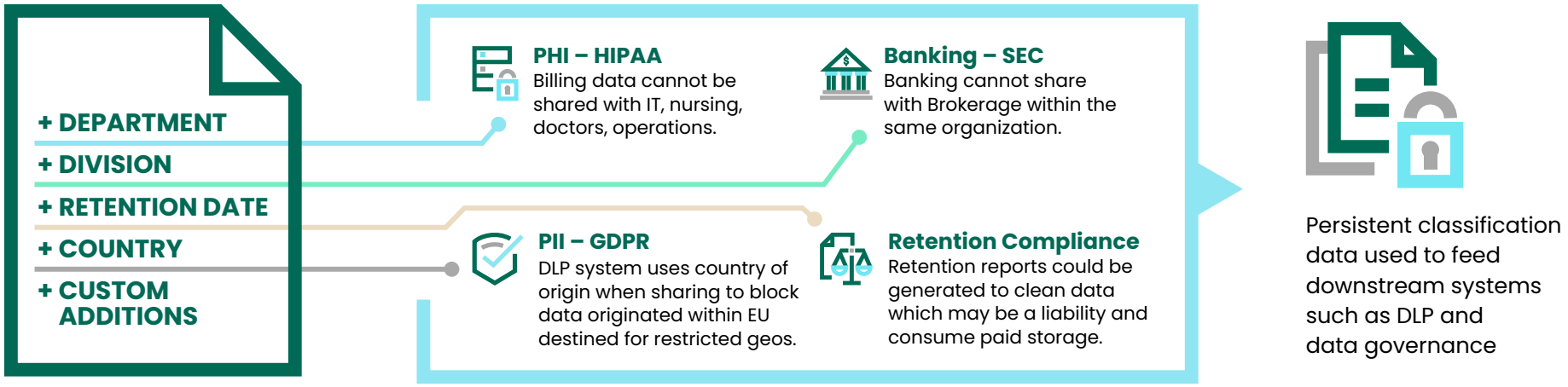


# Fortra Data Classification

## Data classification that keeps you secure, compliant, and in control.

Fortra Data Classification provides essential classification tools, with a straightforward experience for you and your users, on what should be secured and how to handle it. Give your data context so both people and systems understand how to use it.

Our tool embeds metadata attributes into email, documents and files at every stage of the content lifecycle and can automatically add visual markings to help organizations meet compliance and legal requirements.



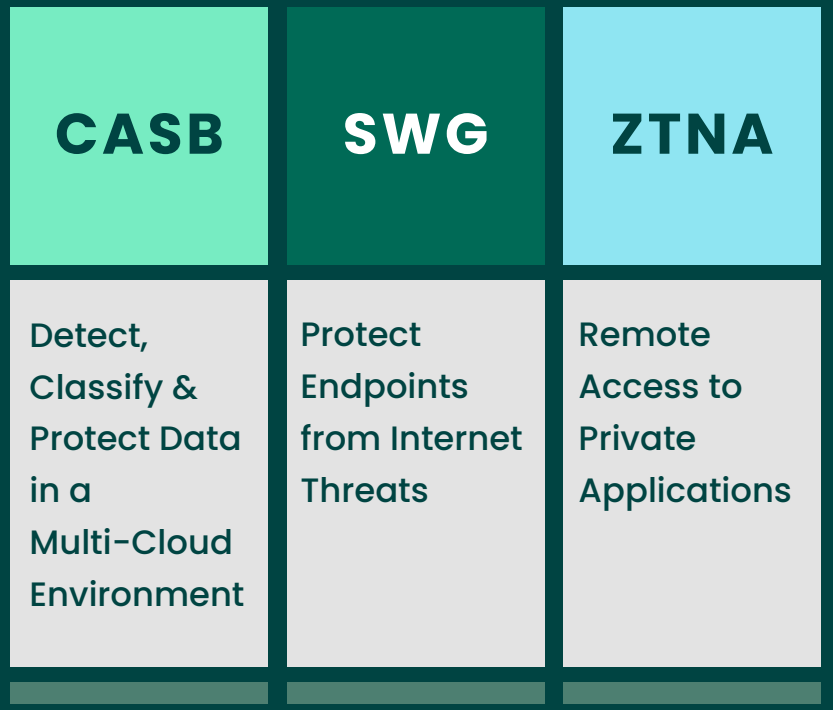

# How We're Different

Unlike other solutions that offer simplistic "sensitivity labels," Fortra Data Classification enables users to define and utilize a wide range of identifiers, including department, customer, and country, for precise data categorization. Fortra uses metadata as a fundamental part of the solution, and the solution, in turn, provides the structure of how the business should interpret the metadata. While Fortra can label document sensitivity, it goes beyond this functionality to address the complexities of today's regulatory environment. By leveraging Fortra Data Classification, organizations can achieve complete data protection and navigate compliance requirements with enhanced efficacy and precision.

# Fortra Cloud Data Protection

The rise of remote and hybrid work has driven a greater reliance on cloud and SaaS applications. As traditional office networks fade, security teams must secure multiple interconnecting environments and maintain control over sensitive data, all without disrupting workflows.

Fortra CASB, DSPM, SWG, and ZTNA extends data security to the cloud, web, and private apps, providing ultimate visibility into user activity across multiple environments, detecting and mitigating cyber threats, and protecting sensitive data throughout its life cycle.



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.

 | fta-dc-ds-0126-r5-as