FORTRA

# How Fortra Data Loss Prevention Outperforms Microsoft Purview

# How Fortra DLP & Purview Integrate

On its own, Microsoft Purview Information Protection (known as MPIP or simply Purview) provides organizations with a set of data protection solutions integrated into and focused on the Microsoft environment. While this may be enough in a perfect world, in reality, organizations increasingly find this to be limiting, as their infrastructure extends beyond the Microsoft environment to include Linux, MacOS, Firefox, Safari, and various other applications depending on the types of data being handled and which regulatory requirements those data types are bound to.

Fortra Data Loss Prevention helps organizations enrich their existing Purview tools by extending the protection they afford to the rest of their environments—including non-Microsoft operating systems, browsers, and applications—ensuring complete data protection. When integrated, Purview and Fortra DLP work together to deliver the most comprehensive data protection for modern enterprises, ensuring employees are educated on corporate policies, that those policies are consistently followed, and that organizations' data remains in the right hands.

Purview users will quickly find that Microsoft's data protection tools work strictly within the Microsoft environment, but Fortra DLP picks up where they drop off. Our DLP solution extends Purview's data protection capabilities to cover organizations' full corporate environments—from network-based users to work-from-home employees—and integrates with its pre-existing sensitivity labels, meaning ease of use isn't sacrificed as coverage extends.

Using Purview's sensitivity labels, Fortra DLP sets hard and soft limits on specific data actions, blocks overtly suspicious actions, and prompts users to acknowledge corporate policies when potentially risky actions are taken. As corporate data policies evolve, Fortra DLP then automatically updates and applies them, reducing the administrative overhead on information security teams.


When a user attempts to upload an unlabeled document to a web-based email client, Fortra DLP will prompt the user to label the document in your organization's data classification tool, including MIP.

# Where Purview Falls Short

Because Microsoft's Office 365 products are all but ubiquitous across organizations globally, it's understandable that many have come to think of Purview as the "default" data protection platform. However, as organizations familiarize themselves with Purview, several of its hidden pitfalls quickly become evident when used on its own:

## Overhead & Poor Customization

For a product that is often touted by Microsoft for its simplicity and positive user experience, Purview can be difficult to implement and manage relative to its somewhat basic features. Not only is Purview's protection limited to the Microsoft environment and related applications, but users often find that it lacks both granularity and scalability. Organizations with complex data handling policies, elaborate labeling schemas, and the need for customizable alerts may find Purview's "out-of-the-box" templates to be inadequate, if not completely unusable. And because Purview tools do not extend across tenants, administrators are forced to manually enter security policies and rules—many of which require fine-tuning—for each new environment they need to secure.

## Lack of Support

What's more, due to a severe lack of continuity between Purview customers and Microsoft's rotating customer success teams, even small problems that arise can become massive undertakings to fix. Microsoft's customer success and managed services teams are outsourced to third parties whose knowledge and expertise in DLP, the nuances of your organization's needs, and your organization's security architecture are questionable at best. This questionable knowledge, compounded by their massive customer bases, can lead to issues taking months or even years to resolve.

## Limited Reporting Functionality & Hidden Costs

While Microsoft will tell potential customers that they offer customized reporting capabilities, in reality, this feature is only available through an integration with Microsoft Sentinel—a paid service. Generally speaking, Microsoft's claim that Purview is a free offering is misleading due to its highly obfuscated pricing model. While Purview comes bundled with E3 and E5 packages, organizations often face unforeseen expenses associated with "premium" features (many of which come included with a more comprehensive DLP solution), integrations like Sentinel, and extra pay-per-use charges. For example, Purview's optical character recognition scanning, which allows Purview to scan images for sensitive data, is a paid feature that employs a pay-per-use model. Depending on how many images your organization needs to scan on a regular basis, you could be looking at hundreds or even thousands of extra, unanticipated charges.

# How Fortra DLP Enhances Purview

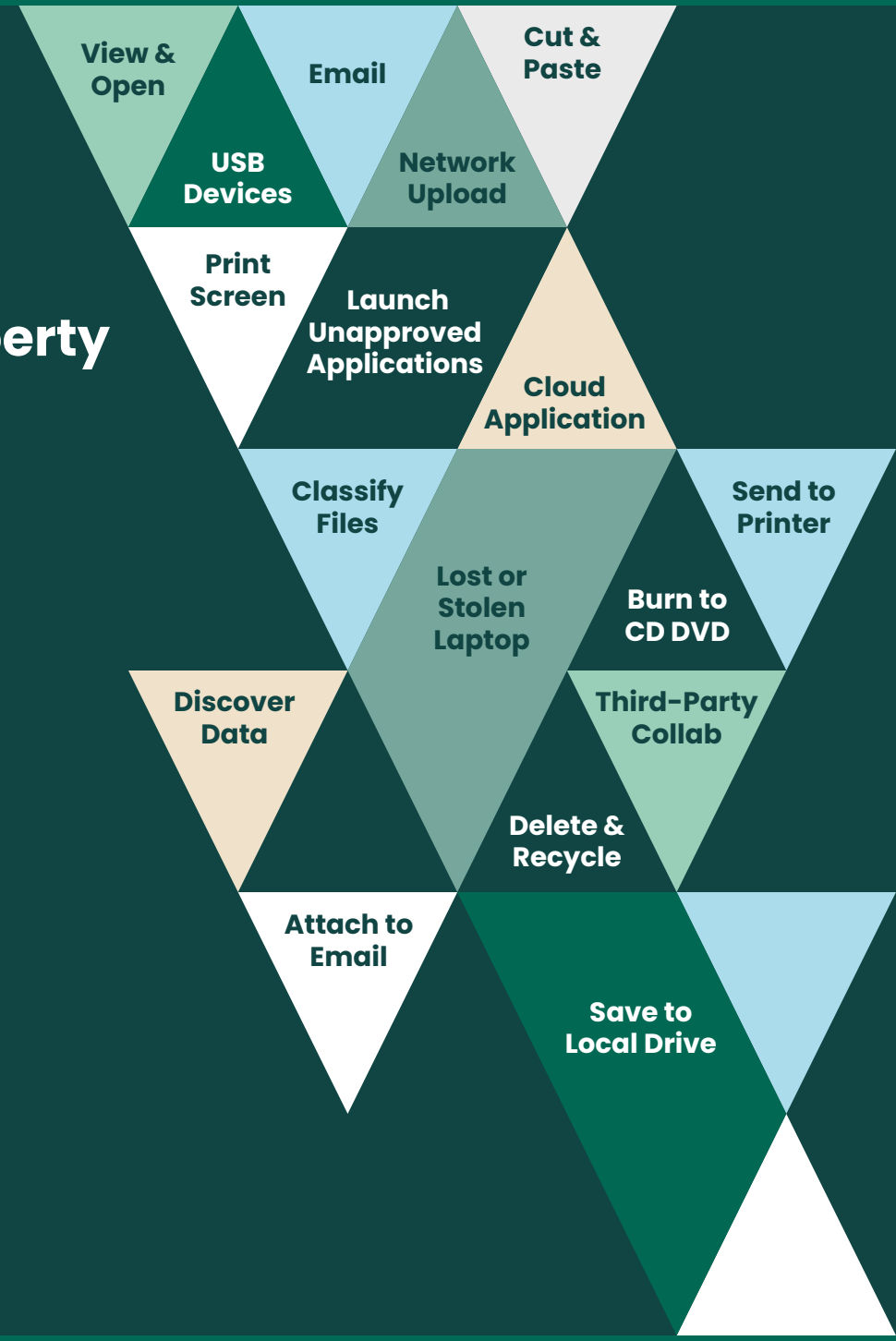
## Coverage Beyond Microsoft's Environment

Fortra DLP extends Microsoft's coverage to ensure that all of your organization's data is seen and protected. Purview is designed to cover Windows 10, Edge browser, and Office applications, while Fortra DLP expands that coverage to include your corporate network, traditional endpoints, and cloud applications on Windows, Mac, and Linux operating systems. Fortra DLP aims to protect organizations' sensitive data across a wide variety of environments regardless of how complex their data handling policies are and which types of data they handle.

## Delivers Enhanced Features

While many of Purview's "premium" features are considered add-ons, such capabilities are often already included in comprehensive, modern DLP solutions like Fortra DLP. We provide organizations with a policy-driven approach to DLP via a single agent, network appliance, and management console, packed with custom reporting capabilities, advanced analytics, Secure Service Edge (SSE) for endpoint-to-cloud protection, and AES 256-bit encryption via Fortra Secure Collaboration.

- Trade Secrets & Intellectual Property
- Custom Data
- Engineering Drawings
- PHI & PII Data
- Credit Card Data
- Source Code
- All Unstructured Data

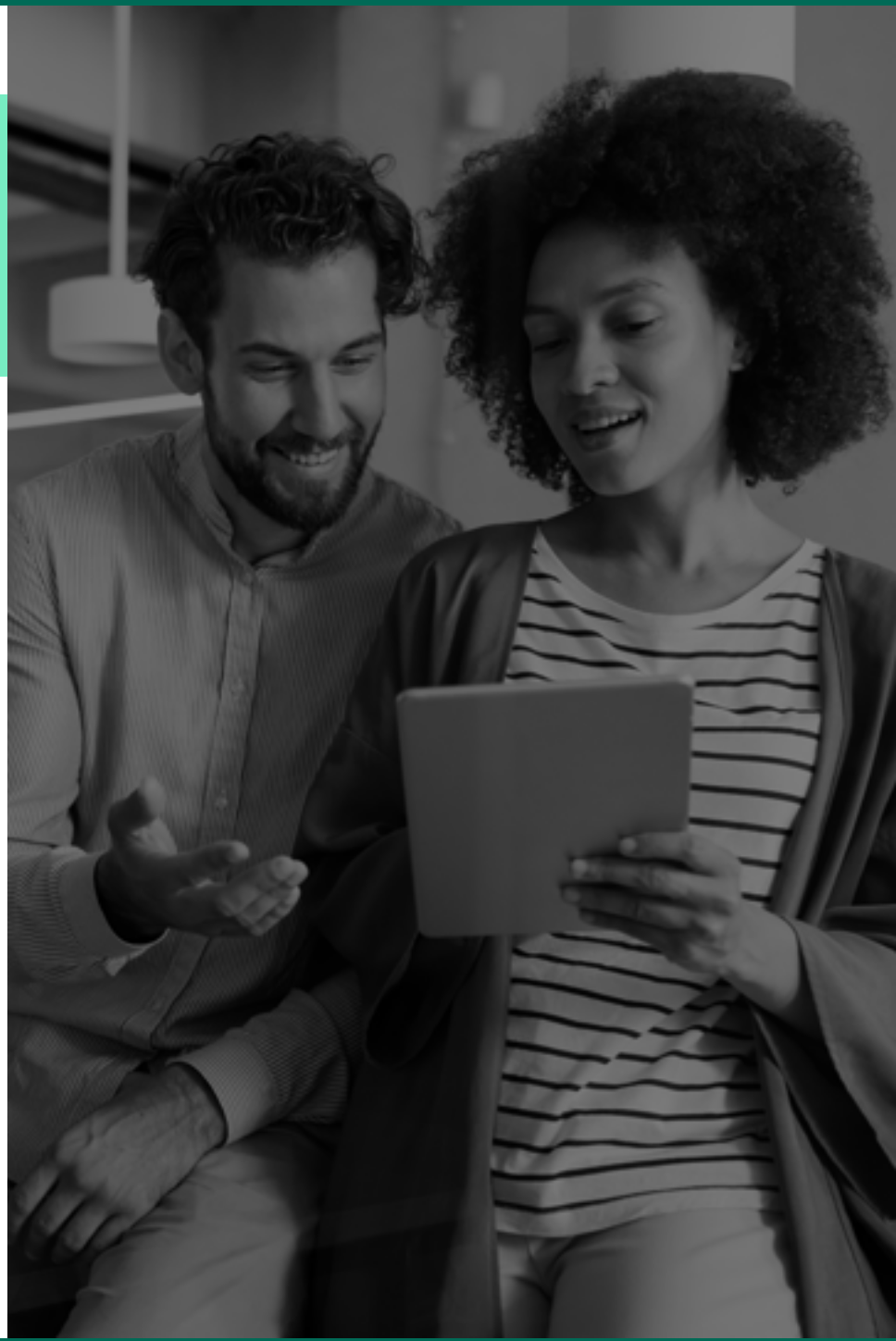


## Transparent Pricing

Perhaps even more importantly, all of these enhanced features come in a single package with a transparent pricing model. While Purview's add-on features will almost certainly add unwanted variability to organizations' budgets, Fortra DLP's pricing model allows those organizations to budget safely in the knowledge that they won't be faced with unexpected fees.

## Reliable Professional Services

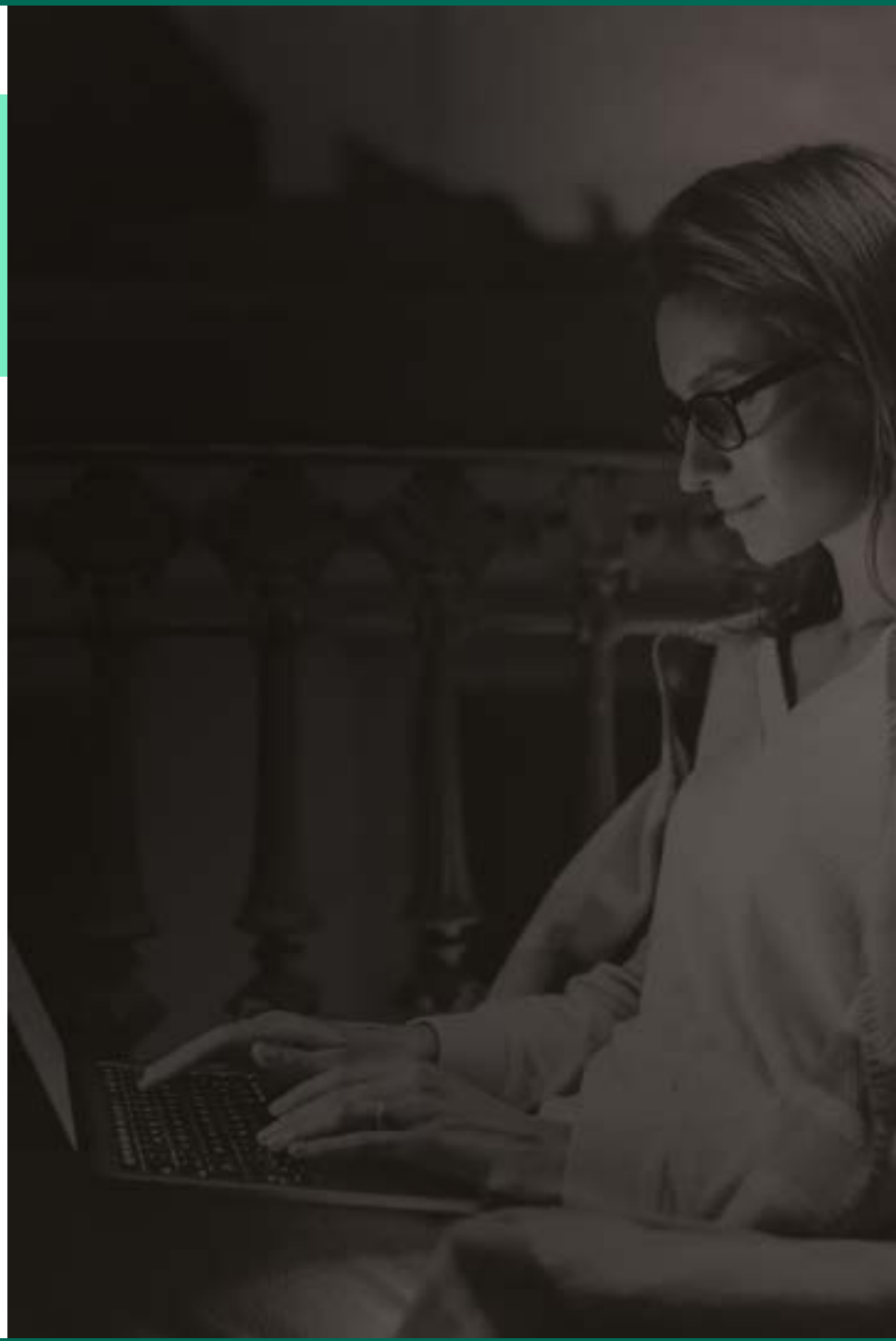
Unlike Microsoft, whose managed services are nearly entirely operated by third parties, Fortra DLP's managed services, including the support, product, R&D, and engineering teams that work in close collaboration with one another, are all in-house. Fortra provides integrated support and years of experience specifically in DLP, meaning organizations can thoroughly trust that our experts will do much of the heavy lifting and that customer issues will be solved swiftly and efficiently.



## Extended Protection Beyond the Corporate Network

With many companies still operating in a hybrid work environment, organizations need comprehensive data protection that protects data wherever it goes, wherever a user is working. Fortra DLP extends Purview's capabilities to ensure data remains protected wherever it moves outside of the corporate environment, regardless of whether that data is being handled by remote employees, partners, or external third parties.

The process of classifying documents is only the first step in this process. The next step is in establishing controls in the form of what can or cannot be done with a document based on the classification metatags. For example, one control may prevent data handlers from printing unlabeled documents or uploading them to cloud applications. Another control could prevent data handlers from emailing or externally saving (e.g., to a thumb drive) documents labeled as having 'sensitive information'. Fortra DLP can manage these controls from a centralized management console with robust policy management capabilities, integrating Microsoft's labeling with Fortra's expansive document control.



## Context-Aware Data Protection

Fortra DLP can also help to verify Microsoft labels based on documents' contents. If, for example, Fortra DLP recognizes that a user classified a document as 'public' but it actually contains sensitive Personally Identifiable Information (PII) like Social Security numbers, users will be prompted to update metadata labels while restricting how that document can be shared.

Furthermore, beyond Fortra DLP's ability to identify sensitive content, it's also a particularly robust solution in that it is also context-aware. In other words, beyond identifying the sensitive data itself, Fortra DLP identifies indirect indicators of sensitive data like relevant applications, users and identities, networks, data classifications, and event types.

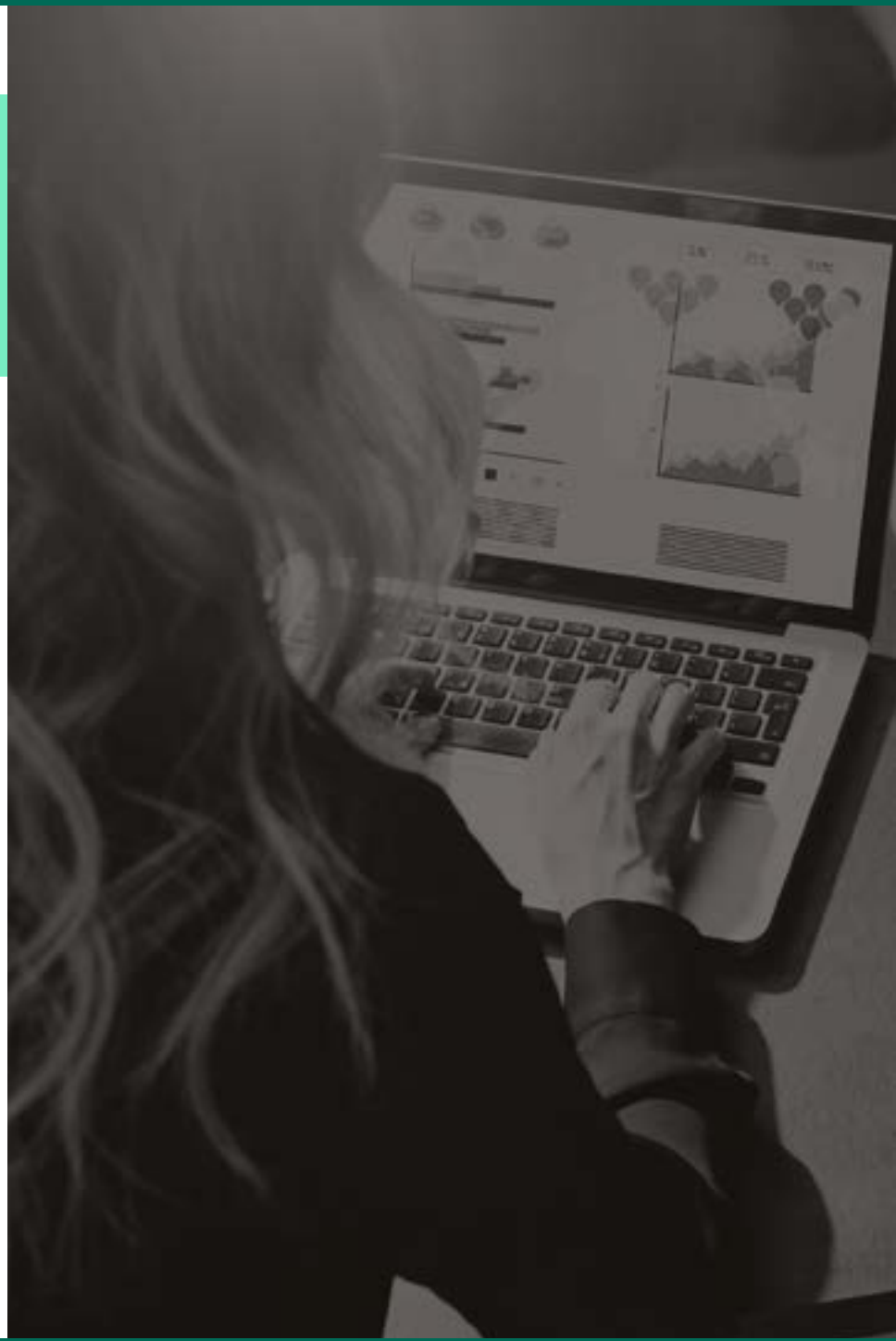

Even if a file is incorrectly classified as 'Public', Fortra DLP will inspect the content and origin of that file, and can determine that the file instead should be labeled differently before any further action is taken with that file and its data.

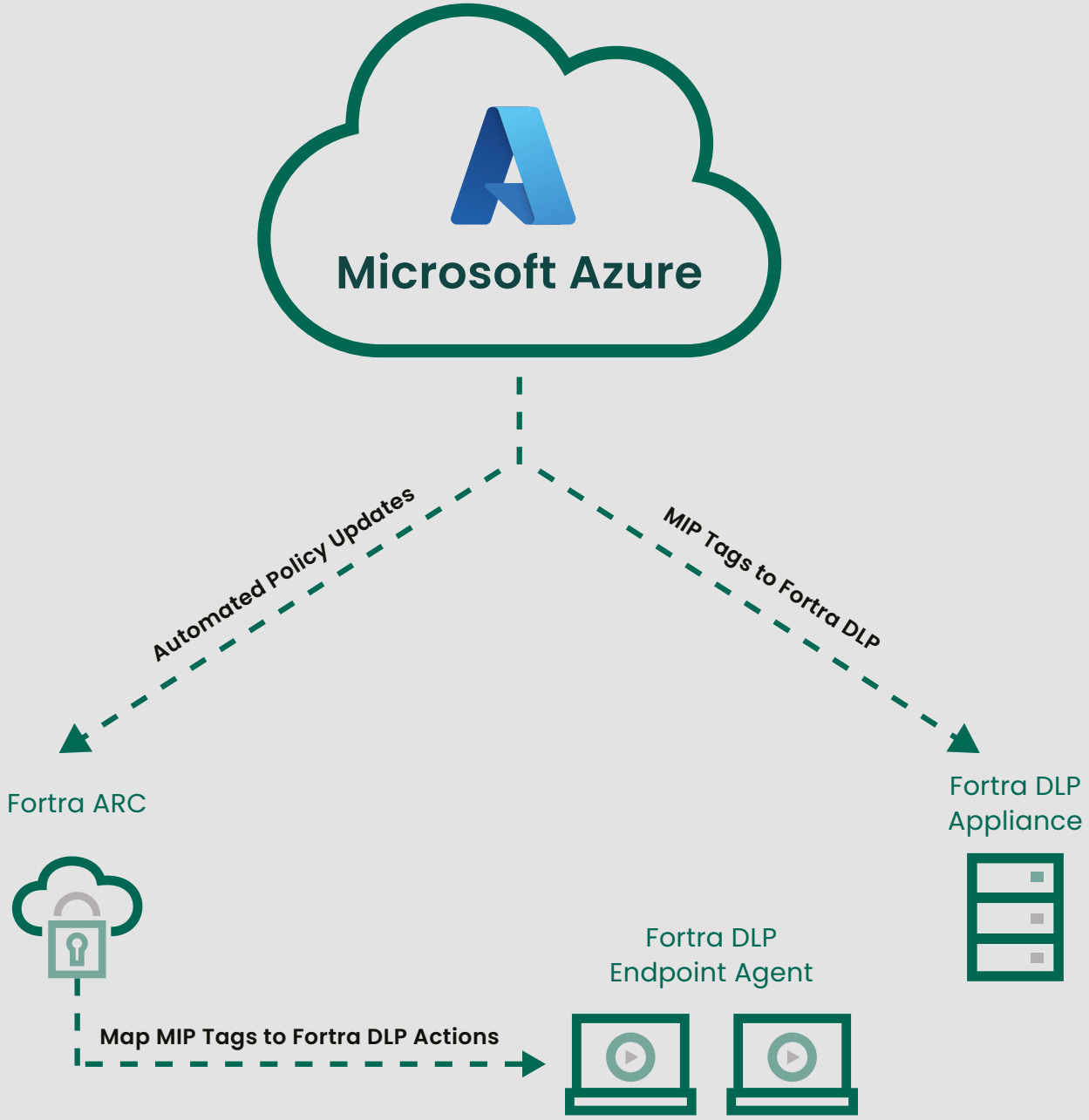
## Analytics: Measure, Track, Report

Fortra DLP offers an advanced analytics, workflow, and reporting cloud service that aggregates data from our endpoint agent and network appliance while also displaying Purview events. Organizations can track data events as they occur throughout the Fortra DLP and Purview environment, whether to demonstrate regulatory compliance to regulators or to show the company board that the proper measures are being taken to protect the organization's critical intellectual property (IP). Flexible and customizable dashboards complement the pre-built workspaces to deliver immediate and deep visibility.

**Interested in learning more?**
**Schedule some time with our team.**

**SCHEDULE A DEMO**




Microsoft Azure
Automated Policy Updates
MIP Tags to Fortra DLP
Fortra ARC
Fortra DLP
Appliance
Fortra DLP
Endpoint Agent
Map MIP Tags to Fortra DLP Actions

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-dg-gd-0325-r5-sv