CYERA

INDUSTRY WHITEPAPER

How Cyera Enhances Data Security for Microsoft 365

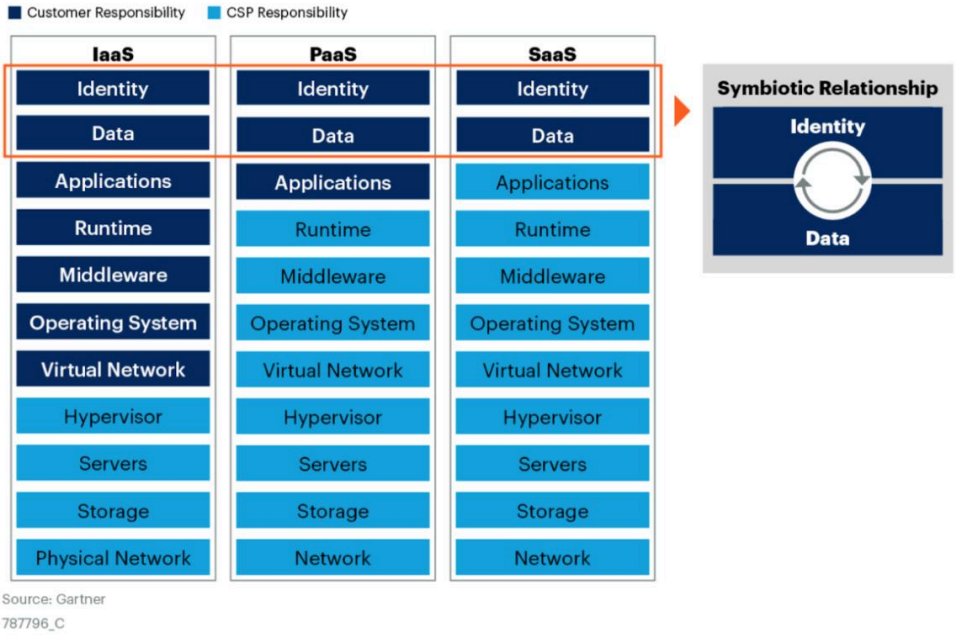
Data Protection and Secure Access

With over 300 million users worldwide, Microsoft 365 (Microsoft 365) stores some of the most highly sensitive data in the world, including private customer information, employee details, intellectual property, and other business secrets. It's critical that the enterprises that own it, protect it.

Under Gartner's Shared Responsibility model, Cloud Service Providers (CSPs) secure the infrastructure of the SaaS or cloud environment—think of physical servers, network hardware, and the overall maintenance of the cloud platform. The customers, on the other hand, bear the responsibility of protecting the data they place within that environment and ensuring secure access to it. This critical distinction is often misunderstood.

The result: significant security gaps.

For example, the lack of essential security measures like multi-factor authentication can leave the door open for unauthorized access. In platforms like Microsoft 365, to help security teams ensure proper controls are in place, users are typically responsible for manually tagging files as sensitive—a process that's not only time-consuming but rife with human error. These errors expose critical data to a potential incident. As a result, it's imperative for organizations to actively validate security controls on their side of the Shared Responsibility model. Doing so effectively requires high levels of confidence in the identification of sensitive data.



Source: Gartner
787796_C

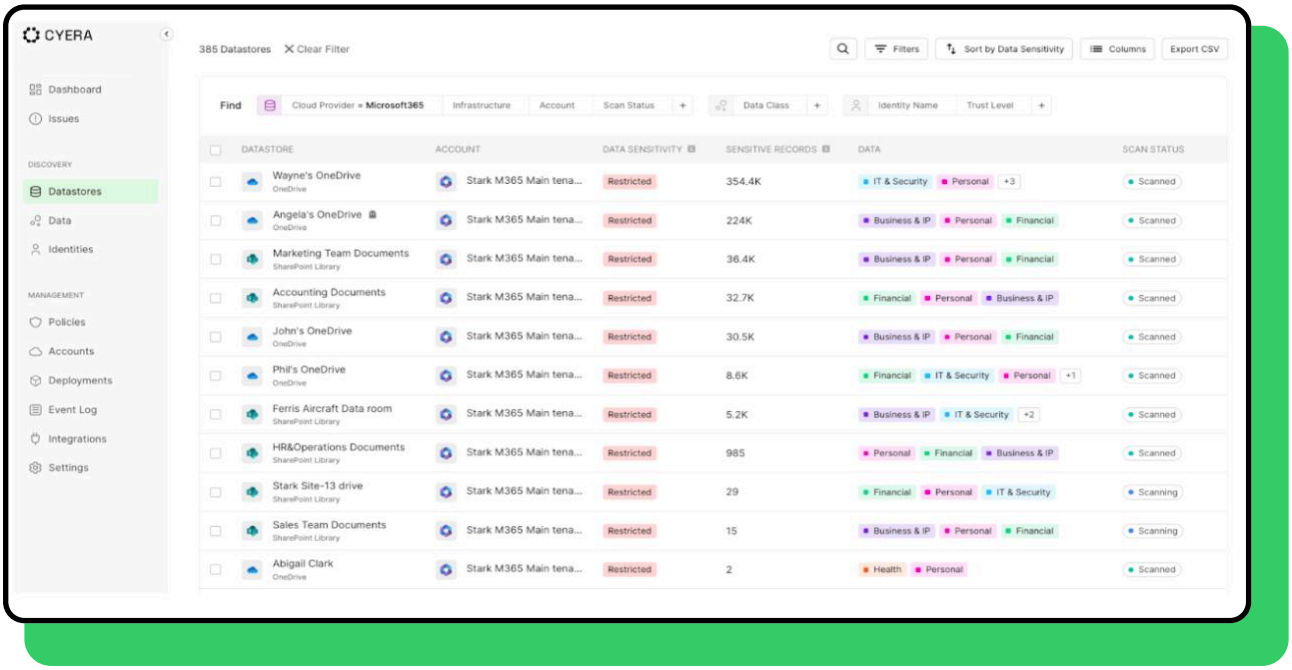
Cyera Data Security Use Cases for Microsoft 365 Customers

Cyera enables data security leaders to discover and classify data with high precision, at scale and with speed. In doing so, the platform automatically assesses your data security posture, enabling the protection of your most sensitive data across environments, including Microsoft 365.

Cyera helps you extract even greater value from your Microsoft 365 enterprise licenses, helping customers to:

Uncover Sensitive Data Within Your Microsoft 365 Environment

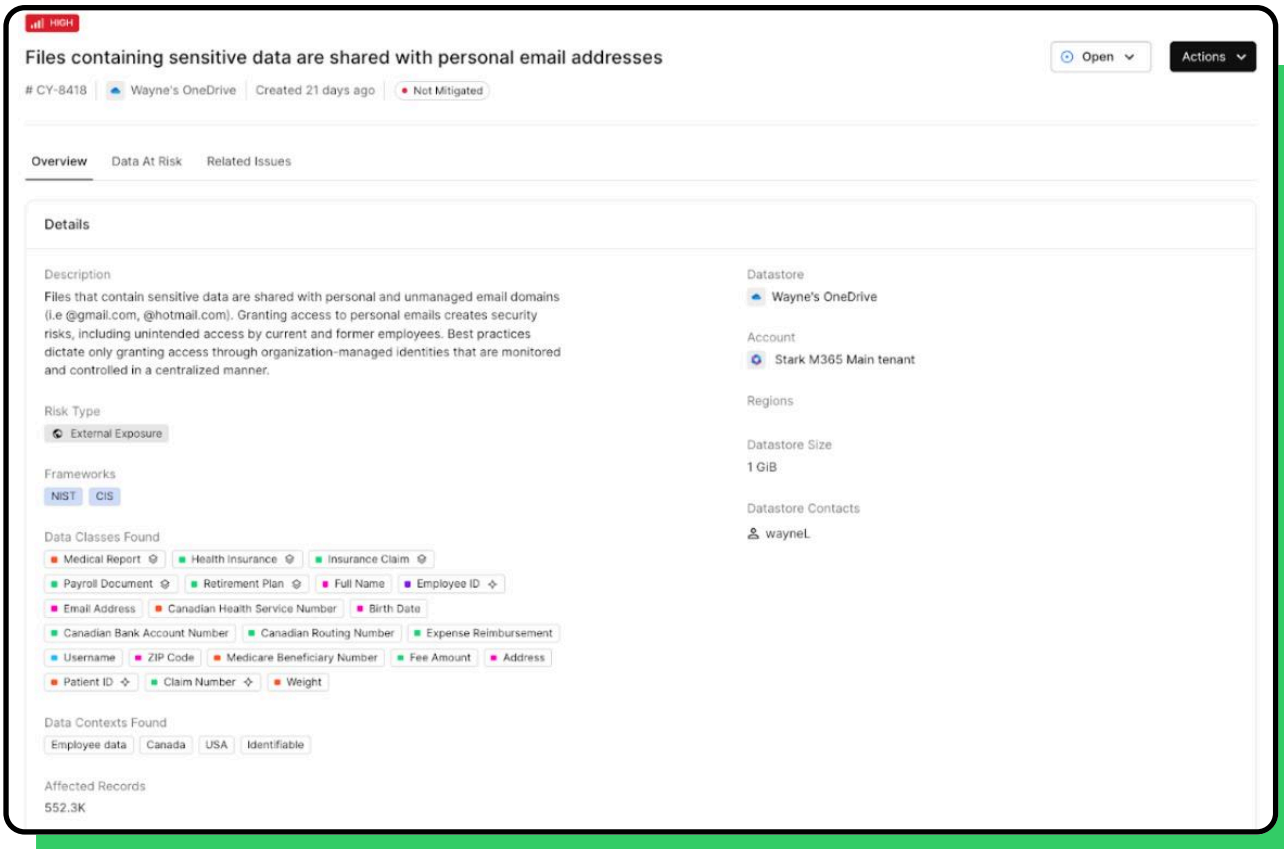
Cyera connects to your Microsoft 365 tenant via API before scanning the environment for sensitive data. Once scanned, Cyera has a full inventory of the data within Microsoft 365. Cyera classifies the data with high precision and provides vital context around it, including class, residency, sensitivity, identifiability, and more. Simultaneously, existing Microsoft sensitivity labels are identified and pulled into the Cyera platform. And with the insights uncovered by Cyera, Microsoft sensitivity labels are validated and any overlooked sensitive documents are automatically labeled.



Determine Your Microsoft 365 Data Security Posture

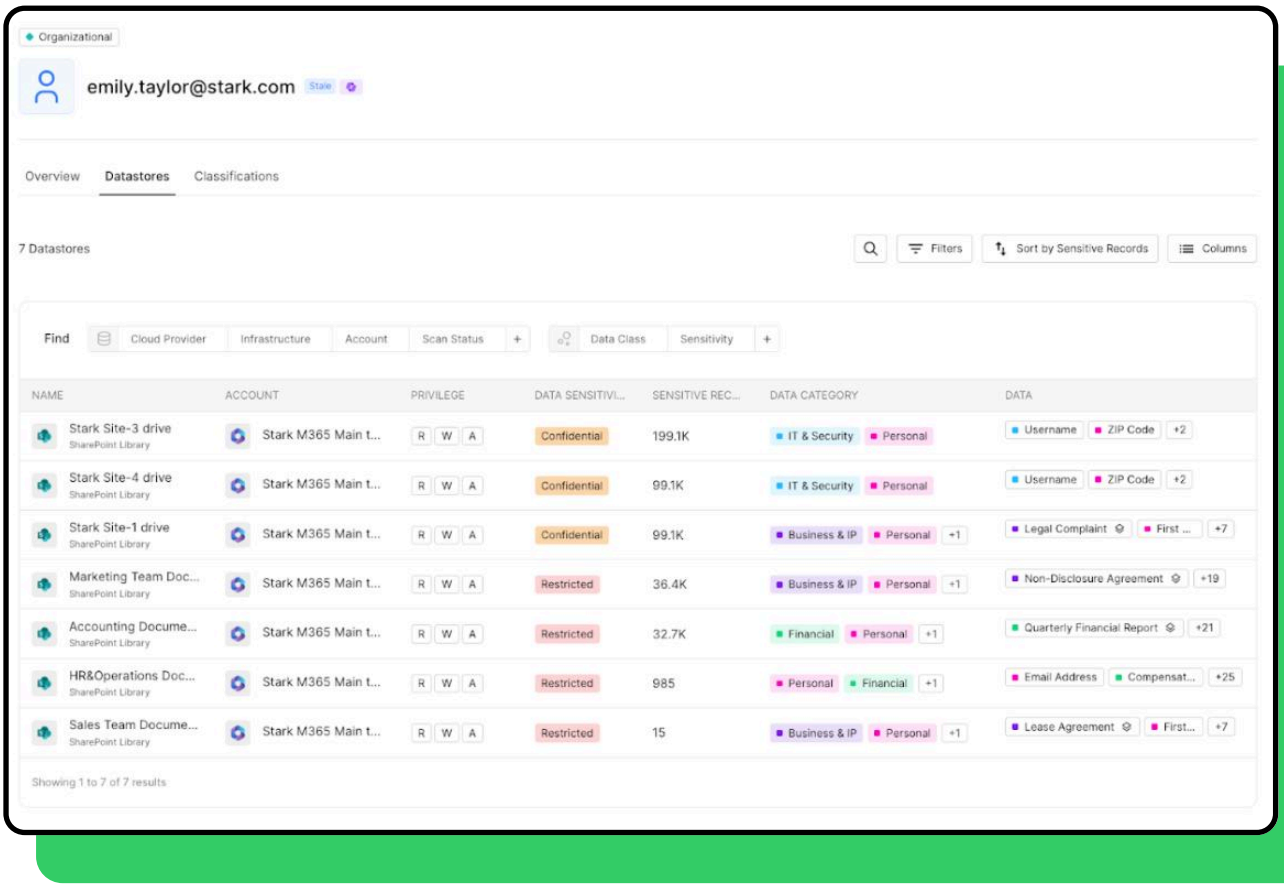
Our policy engine, which is aligned to established compliance frameworks and security best practices, triggers alerts to help your data security team identify and prioritize risks. These issues include data drifting to unapproved locations, the misuse of data, sensitive data being shared with unauthorized entities, sensitive data exposed in plain text, or many other risks that weaken your Microsoft 365 data security posture. Other Cyera policies detect additional issues that fall on the customer side of the Shared Responsibility model, such as:

- Unencrypted consumer financial information
- Unencrypted personal information or protected health information
- Social Security Numbers accessible through Copilot
- PCI data stored outside of cardholder data environment
- Files containing sensitive data shared with personal email addresses
- Files containing sensitive data shared with an unauthorized external organization
- Sensitivity labels do not match file sensitivity
  Sensitive data is stored in a OneDrive of an employee no longer with the company



Determine Which Users Have Access to Sensitive Data Stored Within Microsoft 365

Cyera also has the ability to determine the human identities, or non-human identities (like Microsoft Copilot), that have access to sensitive data within Microsoft 365. In the example below, Emily Taylor works for Stark Industries. Emily is discovered by Cyera, a trust level is assigned to her, and her level of access to the 467.74K sensitive data records is determined. Security admins can then assess this level of access to identify any issues.



Maximizing Your Microsoft Purview Investment

Microsoft Purview is designed to help you manage and oversee your data. Its sensitivity labels help enforce data security policies, maintain compliance, and protect your information. These sensitivity labels support:

- Data Loss Prevention (DLP) by automatically applying policies to block or quarantine sensitive information based on its classification.
- Data Access Governance (DAG) by controlling access and encrypting data to ensure it is only accessible by those who need it.
- Data Compliance by specifying how sensitive data should be collected, stored, and processed in accordance with regulatory requirements.

However, without accurate labeling, these programs cannot function effectively. While Purview provides vital sensitivity labels, Cyera helps organizations implement them more efficiently and accurately.

Cyera and Microsoft Purview: Better Together

Cyera complements and enhances Microsoft Purview's capabilities with powerful data discovery and precise data classification. This enables more accurate and consistent sensitivity labeling to enhance your data security posture at scale. This leads to:

1. Faster Results

With high volumes of data, Purview classification can take many months to complete. Additionally, Purview often requires heavy Regular Expression (RegEx) and policy configuration to tune classification, which leads to heavy professional service hours. For many organizations, it takes months to see any actionable results. Cyera's AI-powered advanced classification capabilities automatically learns and applies classifications specific to your environment. This drastically reduces the manual effort spent tuning classifiers and greatly accelerates time to value.

2. Greater Data Visibility

Purview only connects to known datastores, meaning that discovering and classifying datastores you don't know about can be challenging. Additionally, Purview doesn't classify datastores in containers or third-party IaaS, PaaS, or SaaS environments. Cyera automatically identifies and classifies both known and shadow datastores across your Microsoft 365 environment–as well as containers and third-party environments. This helps ensure no sensitive data is overlooked.

3. Precise Data Classification

Purview's classification relies on RegEx and scans limited amounts of data. This often leads to high false positives, extensive tuning requirements, and incomplete data classes. Cyera leverages both pattern-matching and highly-trained LLMs to precisely classify structured and unstructured data. This eliminates the need for manual tuning and allows for the reliable implementation of sensitivity labels.

4. Accurate Sensitivity Labeling

Even with clear guidelines, users may mislabel data, letting sensitive information slip through the cracks. For example, did an end user apply an "Internal-All Employees" label to a file containing sensitive non-public financial information? Cyera automatically detects and corrects mislabeling of sensitive data to reflect its true criticality to your business. This proactive approach vastly reduces the risk of human error and enhances the effectiveness of DLP, DAG, and data compliance programs. Detecting mismatched sensitivity labels also presents an opportunity to conduct targeted education for users who repeatedly apply incorrect labels.

Cyera's Microsoft Sensitivity Label Remediation works by:

1. Collecting existing sensitivity labels
2. Analyzing label mismatch and missing issues
3. Applying corrected Microsoft sensitivity labels upon user approval

Together with Cyera, Purview can apply the necessary data risk management, data leakage prevention, and access controls as dictated by its policy engine, while Cyera's advanced classification engine automatically classifies data and applies sensitivity labels, allowing you to overcome many of the challenges of a user-driven, sensitivity-labeling implementation."

See Cyera in Action

To learn more about how Cyera helps you get the most out of your Microsoft investment and protect your Microsoft 365 data, request a demo today.

About Cyera

Cyera is reinventing data security. Companies choose Cyera to improve their data security and cyber-resilience, maintain privacy and regulatory compliance, and gain control over their most valuable asset: data. Cyera instantly provides companies with a holistic view of their sensitive data and their security exposure, and delivers automated remediation to reduce their attack surface.

Learn more at **www.cyera.io**, or follow Cyera on **LinkedIn.**

Trusted by:

SKECHERS · PELOTON · CHIPOTLE · AT&T · BlueCross BlueShield · Takeda · Constellation Brands · DELTA DENTAL · Rockwell Automation · Tyson Foods