Overview

https://campus.barracuda.com/doc/96016322/

Barracuda Data Inspector provides simple and intuitive data security management with no extra infrastructure or installation. See exactly what kind of data has been found, whether it has been shared and where it is located so you can decide what needs to be done. Data Inspector can even identify sensitive information from photos, screen shots and documents scans. And actions can automatically be taken by Data Inspector.

New issues are automatically identified without the need to configure scanners or schedules, and customizable email alerts keep you fully informed so you can respond quickly. Barracuda Data Inspector can also alert users when they are storing sensitive data on OneDrive, to help build security awareness.

Malware detection in SharePoint and OneDrive

With Barracuda Data Inspector, you can identify malware stored in SharePoint and OneDrive. This helps prevent accidental activations that can lead to ransomware or other attacks.

Regulatory compliance support

Barracuda Data Inspector lets you spot sensitive data as soon as it appears in OneDrive or SharePoint. Use it to develop policies that comply with GDPR, CCPA, and other data privacy regulations. You can further reduce your risk by improving end-user security awareness, with automated notifications whenever users attempt to store sensitive data on OneDrive or SharePoint.

Data residency

With seven worldwide centers to choose from, your data remains close to home.

Data Inspector data center locations:

- United States (Virginia)
- Canada (Toronto)
- European Union (Netherlands)
- United Kingdom
- Australia (New South Wales)
- Japan (Tokyo)

Key Features

- Scans OneDrive and SharePoint for sensitive information and malicious files
- Identifies sensitive information such as credentials, personal data, and financial data and shows where it exists and whether it is shared—inside or outside the organization
- Identifies suspicious or malicious files such as viruses and other types of malware
- Allows customers to define their own data classifiers to identify specific information types, such as employee or student IDs, project codenames, or other proprietary information
- Comes with more than 150 built in classifications
- Helps you identify the type of sensitive data at a glance
- Prevents further proliferation of found data by creating redacted previews
- Identifies sensitive information from photos, screen shots, documents scans, etc. thanks to advanced optical character recognition (OCR) capabilities
- Supports all common filetypes including Microsoft 365 documents, PDFs, ZIP files, and common image formats
- Supports automated email notifications for admins and compliance officers when sensitive information is identified
- Builds security awareness by notifying users when they store sensitive information in OneDrive or SharePoint
- Allows customers to create policies to automatically handle files based on classifier matches, file permissions, and file ownership/authorship
- Full Software-as-a-Service solution—no hardware or software to manage
- Takes only minutes to configure and start scanning and adds users automatically
- Enforces user-defined role-based access control
- Advanced encryption capabilities protect document previews from unauthorized access
- User-based licensing
- Now available in 26 countries worldwide

Get Started with Barracuda Data Inspector.

Barracuda Data Inspector Pages

- **Detections** – Files discovered to have sensitive data or are malicious.
- **File Details** – Information about a file's type, ownership, access, content violations, and more.
- **Audit Log** – All activities in Barracuda Data Inspector by date, category, description of the activity, user that took the action, user email, and remote IP address. Logged activities include changes to settings such as modifying user roles and adding/deleting classifier assignments, viewing the reports and previews, and more.
- **Scan Log** – Every action taken on each file, whether by the Barracuda Data Inspector or an admin remediation.
- **Settings** – Pages allowing you to configure other features and settings. For example: the ability

to select the geographic region that stores your data.