

Barracuda Data Inspector

Discover sensitive data and undetected stored malware.

Sensitive or private data—Social Security numbers and credit card information, network credentials, and more—can be scattered all over your infrastructure, tucked away in rarely visited files.

Furthermore, many SharePoint and OneDrive deployments are hosts to dormant malware that can go undetected by native security and now wait for one wrong click to activate them.

Barracuda Data Inspector automatically scans your OneDrive for Business and SharePoint data for both sensitive information and malicious files. Take control of your environment, ensure ongoing compliance, and cut the risk of hefty regulatory fines and loss of reputation.

Insight into what sensitive data has been found

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.

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 and eradicate it at the source. 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.

Solution 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 customer to define their own data classifiers to identify specific information types, such as employee or student IDs, project codenames, or other proprietary information
- 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 Office 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
- 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



 Data Inspector 
 ddemo@datainspectordemo.onmicrosoft.com

Cases Settings

Total Items Scanned 128,425
 Issues Found 138
 Users Monitored 1826

USER	DATE DISCOVERED	CLASSIFICATIONS	SHARING DETAILS	SOURCE	ITEM PATH	PREVIEW	ACTIONS
 Data Inspector	March 22, 2021 10:56:26 AM EDT	3 Credentials			ddemo@datainspectordemo.onmicrosoft.com /creds3.txt	REVIEW	DISMISS
 Data Inspector	March 18, 2021 2:36:17 PM EDT	2 Passport			ddemo@datainspectordemo.onmicrosoft.com /passport.png	REVIEW	DISMISS
 Data Inspector	March 18, 2021 2:36:16 PM EDT	1 Personal ID			ddemo@datainspectordemo.onmicrosoft.com /Lost and Found.docx	REVIEW	DISMISS
 Data Inspector	March 18, 2021 2:36:15 PM EDT	1 License Number ...			ddemo@datainspectordemo.onmicrosoft.com /mi-dl.jpg	REVIEW	DISMISS
 Data Inspector	March 18, 2021	3 Credentials			ddemo@datainspectordemo.onmicrosoft.com	REVIEW	DISMISS

