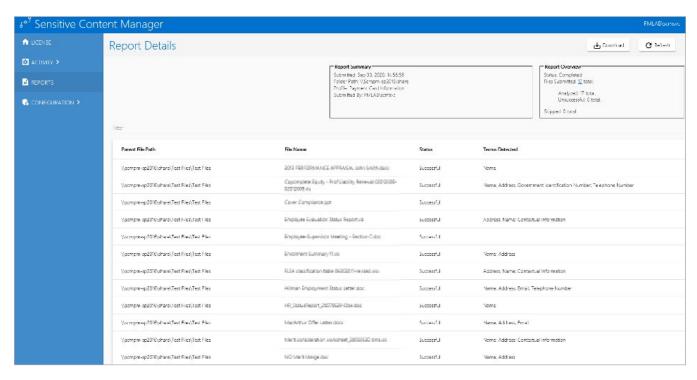# Sensitive Content Manager for Files

Scan and create reports for sensitive data in file shares for simplified management.

File shares are everywhere. Like it or not, everyone uses them to store personal and work files, adding additional stress to VPNs when required for work and creating potential security vulnerabilities. What if you could locate all potentially sensitive data in your users' file shares so it can be properly managed, whether prior to migration or in the event of an audit?

With Sensitive Content Manager for Files, you can scan for and report on sensitive data, including PII, PHI and PCI, in your users' various file shares. Rest assured that you can now locate all the sensitive files in your environment to protect against accidental or malicious leaks.

Benefits:

- **Prevent sensitive data from being accidentally or maliciously leaked outside the organization**

- **Keep sensitive content from being shared unnecessarily**

- **Ensure data is migrated responsibly**

- **Meet audit demands by accurately locating sensitive data so it can be retained or managed as needed**

Sensitive Content Manager for Files locates sensitive data in file shares and reports on the kind of data contained so you can manage it correctly.

Features

Comprehensive file scan

Find the unsecured sensitive content you're looking for with the ability to create custom search terms and scanning profiles, or get started immediately using out-of-the-box search profiles we've set based on common cases.

Simplified detection review

Review the detection report directly from Sensitive Content Manager or export results and distribute them to your team to make sure users know what was detected and where.

Migration planning with insights

Use the Sensitive Content Manager detection report to help clean up files that are a risk prior to migration. Better determine the security required in the target environment to safely manage the types of incoming content.

Integration with other Quest solutions

Don't wait until you've already migrated your content into the cloud to start looking for sensitive data like PII, PHI and PCI. Separate or tag sensitive data using search term filters during migration with Content Matrix or Secure Copy.

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

SYSTEM REQUIREMENTS

Operating system

- **Windows Server 2016, 2019 or 2022**

Operating system

- **Windows Server 2012, 2012 R2, 2016 or 2019**

Database

- **SQL Server 2016 or greater**

Software components

- **Microsoft .NET Framework 4.7.1 or later**
- **Microsoft .NET Core Hosting 6.0 (x64)**
- **Microsoft .NET Core Runtime 6.0**
- **Microsoft Visual C++ 2013 (x64) Redistributable**
- **Microsoft Visual C++ 2015 (x64) Redistributable**
- **Microsoft Visual C++ 2015-2019 (x64) Redistributable**

A complete list of system requirements is available at Support.quest.com.

Quest®