



SENSITIVE DATA DISCOVERY

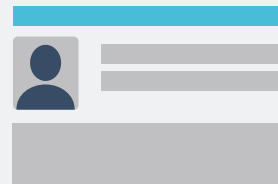
SENSITIVE DATA SCANNING & DATA CLASSIFICATION SOLUTION

CYRISMA's Data Sensitivity Scanning capability allows security teams to conduct quick scans on selected devices to find any sensitive data stored on them that needs to be protected. This data can then be graded and classified based on volume, type, and business impact, and either deleted or encrypted to protect against breaches and ransomware attacks.

CYRISMA's data sensitivity scan allows you to choose from 150 different file extensions in the cloud, on premise and within your own or your clients' email environment. Select systems and machines/targets to run scans on, include or exclude file types and folders, and select specific data categories to look from an extensive list of options.

CYRISMA also allows you to track month-on-month performance with easy-to-understand comparison charts, assign tasks to designated data owners, and schedule recurring scans to main a strong cybersecurity posture.

Popular search categories include passwords, bank account details, SSNs, credit card data and driver's licences.



The Power of CYRISMA

- 1 DISCOVER** files containing sensitive data such as financial information, PII, SNN's and more. Choose from 150 different file types and numerous data categories to scan for.
- 2 UNDERSTAND** what data you have found during the scan as sensitive and non-sensitive based on volume and type, and assign sensitivity grades to different categories.
- 3 MITIGATE** by reducing your sensitive data footprint by taking appropriate measures to protect, secure or hide this data.
- 4 MANAGE** and protect sensitive data and reduce your risk footprint to a tolerable level by conducting regular data sensitivity scans and comparing results over a period of time to assess performance and make improvements.



sales@cyrisma.com



(585) 460 - 1352



CYRISMA

www.cyrisma.com

