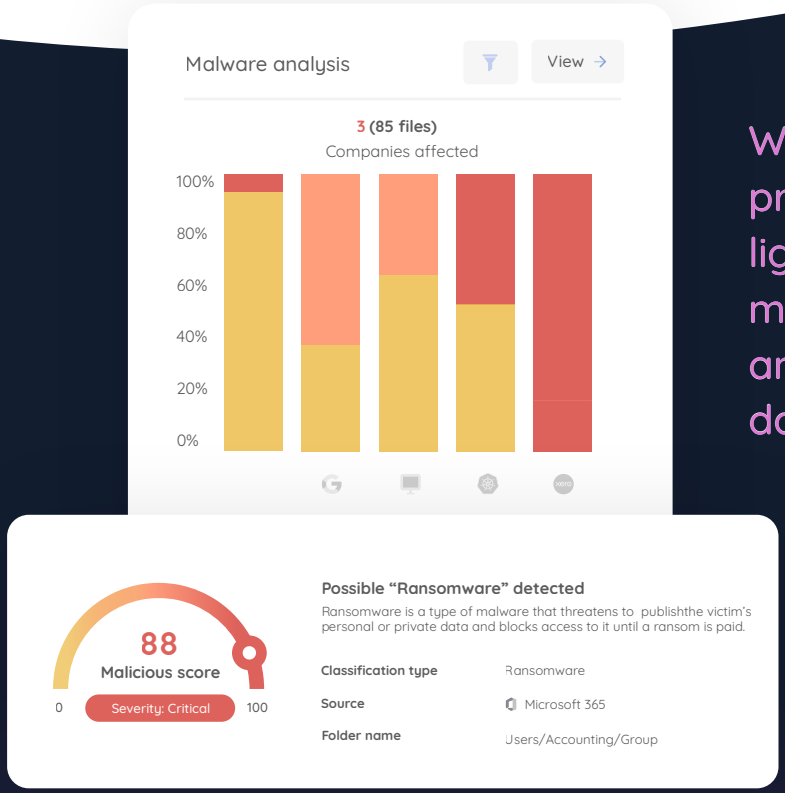
AI-malware detection

Identify and remove threats from backup data, using AI, to ensure malware-free recoveries – at no extra cost.

Most organizations will have antivirus and anti-malware protection in place, but cyber-criminals are becoming increasingly adept at infiltrating systems and hiding their activities, which is why best-practice is to adopt a 'defense-in-depth' approach, using layers of defense with several mitigations at each layer.

Whatever you are protecting – physical, virtualized or cloud infrastructure, Microsoft 365, Google Workspace, desktops, laptops or other sources of data – you need to know that you can recover free from malware in the event of a disaster.

Redstor achieves this by identifying malware within backup data, providing a second opportunity to identify malware within live data.



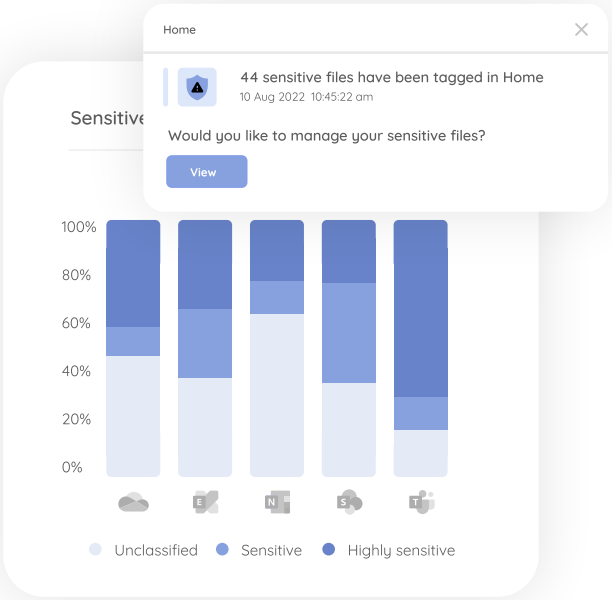
With Redstor you get same-day protection, smarter management, lightning-fast recovery, AI-powered malware detection and removal, and data tagging for improved data risk management

Ensure malware-free recoveries

Outsmart cyber-criminals by neutralizing suspicious files before they become attacks. Unlike many other cloud backup technologies, Redstor's automated AI-powered malware detection technology scans data at point of backup and not at point of recovery, by which time it can be too late. Our proprietary, smart, machine-learning model isolates suspicious files for review, constantly improving its accuracy, based on shared community insights. This provides enhanced protection against 'zero-day' threats and leaves you free to recover malware-free. There is nothing to configure, install or upgrade and the feature is included by default, at no extra cost.

When a threat is detected, alerted users simply mark a suspicious file as safe or remove it and revert to a previous, safe version.

Since launch in 2021 our model has scanned over 100 million items and has a 100% success rate of protecting Redstor customers from the threat of malware.



Automatically tag sensitive data

AI woven into Redstor's app automatically identifies whether backed up data should be classed as highly sensitive or sensitive, enabling management of the concentration and exposure of sensitive data, facilitating protecting it more effectively – again, for no additional charge.

Identify the danger lurking in the background

Many organizations have 90-day or 180-day retention periods for their data. However, it can typically take 200 days to uncover an attack, longer than most organizations' retention policies.

Even if malware is hiding in live data, with Redstor's smarter service you can prevent it slipping into backups - as well – a nightmare scenario that would make it impossible to perform a clean recovery.

Demonstrate compliance

By deploying Redstor's smart malware detection and removal for backups as a complementary additional layer of protection, you will be following best practice. Where a host-based antivirus is used it is highly recommended to use different products to increase overall detection capability.

Unlock the power of machine learning

Not only does our machine-learning model respond to updates of real-world events and new threats posed by the latest malware, it continually refines itself to perform with improved accuracy as files are confirmed as safe or malicious.

How it works

Data from each backup and supported file types is sent to a malware engine where a machine-learning model acts and reports on key indicators exhibited by malware.

Our machine-learning model:

• preserves the integrity of your data, which is encrypted at source, in transit and at rest
• checks for malware outside your environment, so there is no impact on your resources
• continues to train itself, based on results and the latest real-world events and threats, refining and improving its accuracy

There is nothing for an IT department to configure, install or upgrade. No user intervention is required until a suspicious file is detected and automatically quarantined before it can infect a system.

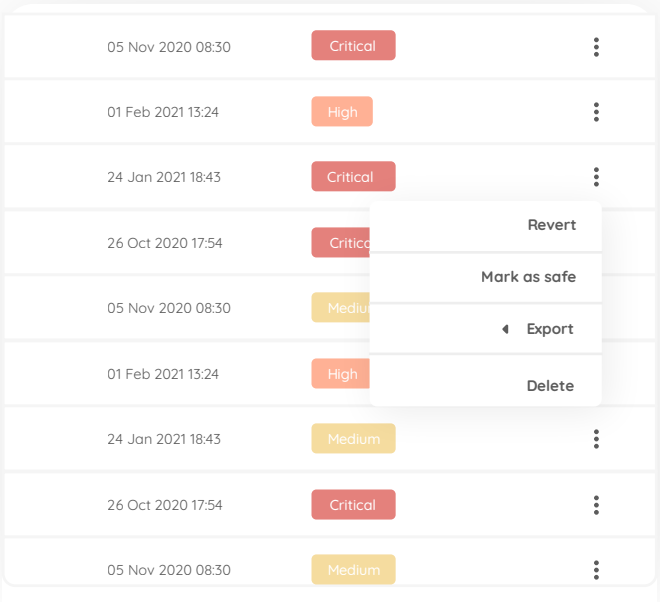
Alerts are then sent via the RedApp mobile app along with various recommended options to keep backups safe. After checking quarantined files and folders, you have the option to:

• validate individual or multiple files by marking them as safe before releasing them into the new backup set
• delete files completely so they are removed from the backup set
• revert the quarantined files to a previous 'safe' version
• leave files in the quarantined list

So even if live data has been infected, Redstor offers a ring-fenced known safe state for the backups you will rely on in an emergency.

What files are checked

Checks are carried out on all common file types, including: PDF, DOC, XLS, PPT, DOCX, XLSX, PPTX, DOCM, XLSB, XLSM, PPTM, RTF, DLL & EXE



Benefits of data tagging

With Redstor's smarter, AI-powered data tagging MSPs and their end users can see how much of their data being backed up is classed as highly sensitive or sensitive.

This allows them to better manage their exposure and concentration of sensitive documents and protect them effectively.

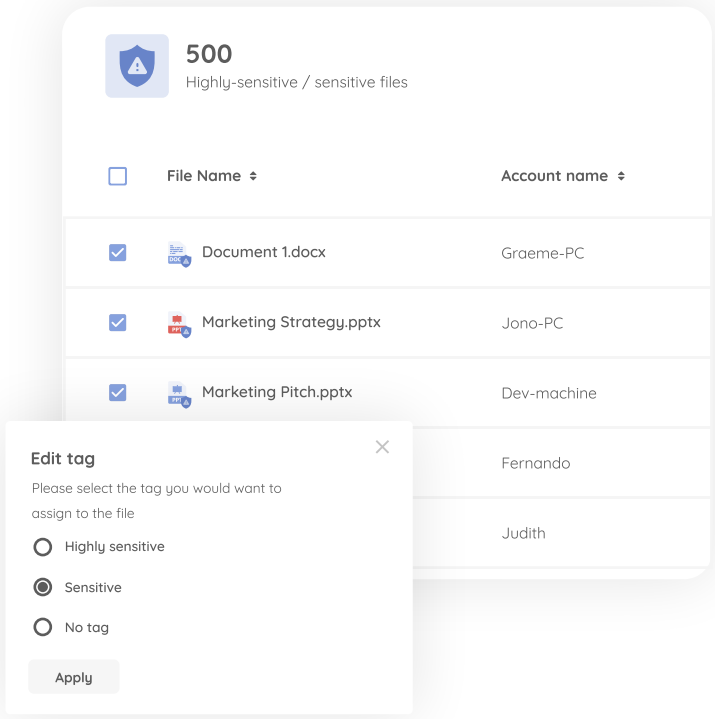
For example, it may identify that 90% of an organization's most sensitive files are stored on a single machine, or that 75% of data held within a Google Workspace user's account is highly sensitive.

Benefits include:

• Greater visibility of sensitive data being stored and backed up across customer platforms

• Completely automated process. No user input is required unless the customer would like to re-categorize a file classification. This can also be done in bulk if required

• Enables MSPs to provide recommendations, advice or even additional services to manage sensitive end users' data



How data tagging works

The data is decrypted and sent securely (using SSL encryption) to the feature extraction engine, where it is scanned within milliseconds.

The data remains encrypted on the customer machine and in the backup. Encryption keys remain encrypted using the OS API so that they cannot be accessed by anyone.

The data is then classified based on criteria outlined in the GDPR, FOI and POPIA regulations. Since the identifiers that make a file highly sensitive or sensitive are functionally the same for any data protection regulation, data tagging is also useful for organizations that aren't required to adhere to these regulations and legislation.