redstor™

Detect and remove malware from backup data

Identify and remove threats, using artificial intelligence, to ensure safe recoveries

An additional layer of protection

Unleash the power of machine learning to detect malware within backups – the data you will rely on in the event of a disaster.

Most organisations will have a form of anti-virus and anti-malware protection in place, but on average it takes 200 days or more to uncover a malicious attack, longer than a lot of typical retention policies.

In this case malware will be present within all backups as well as the live environment. This makes it impossible to perform a malware-free recovery.

You need to know you are restoring from backups that are regarded as safe.

Redstor has developed an advanced, machine-learning model to detect, isolate and delete malware from backups, providing that additional layer of protection and peace of mind.

Machine learning

Purchased as an add-on, Redstor's malware detection supports servers, laptops or any end-point machines.

Our machine-learning model:

- searches for key indicators exhibited by malware
- 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
- avoids the need for a user to configure or install anything or carry out upgrades
- continues to train itself, based on results and the latest real-world events and threats, refining and improving its accuracy

How it works

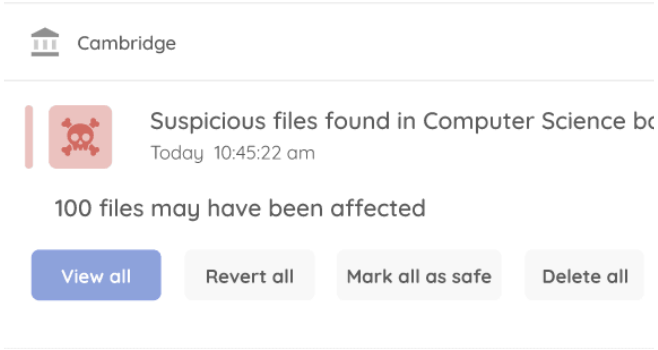
Data from each backup and supported file types is sent to a malware engine where a machine-learning model acts and reports on key indicators.

Redstor's AI-driven technology:

- checks for signs of malware
- pinpoints files that resemble malware in appearance or behaviour
- flags up any suspicious files

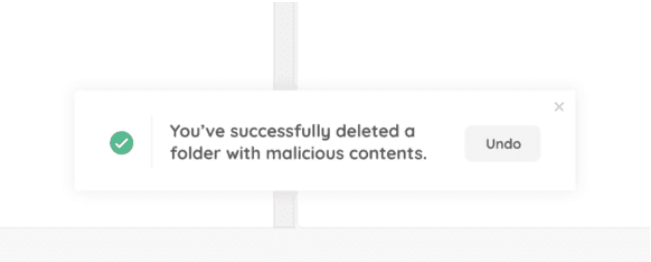
When suspicious files are detected, Redstor:

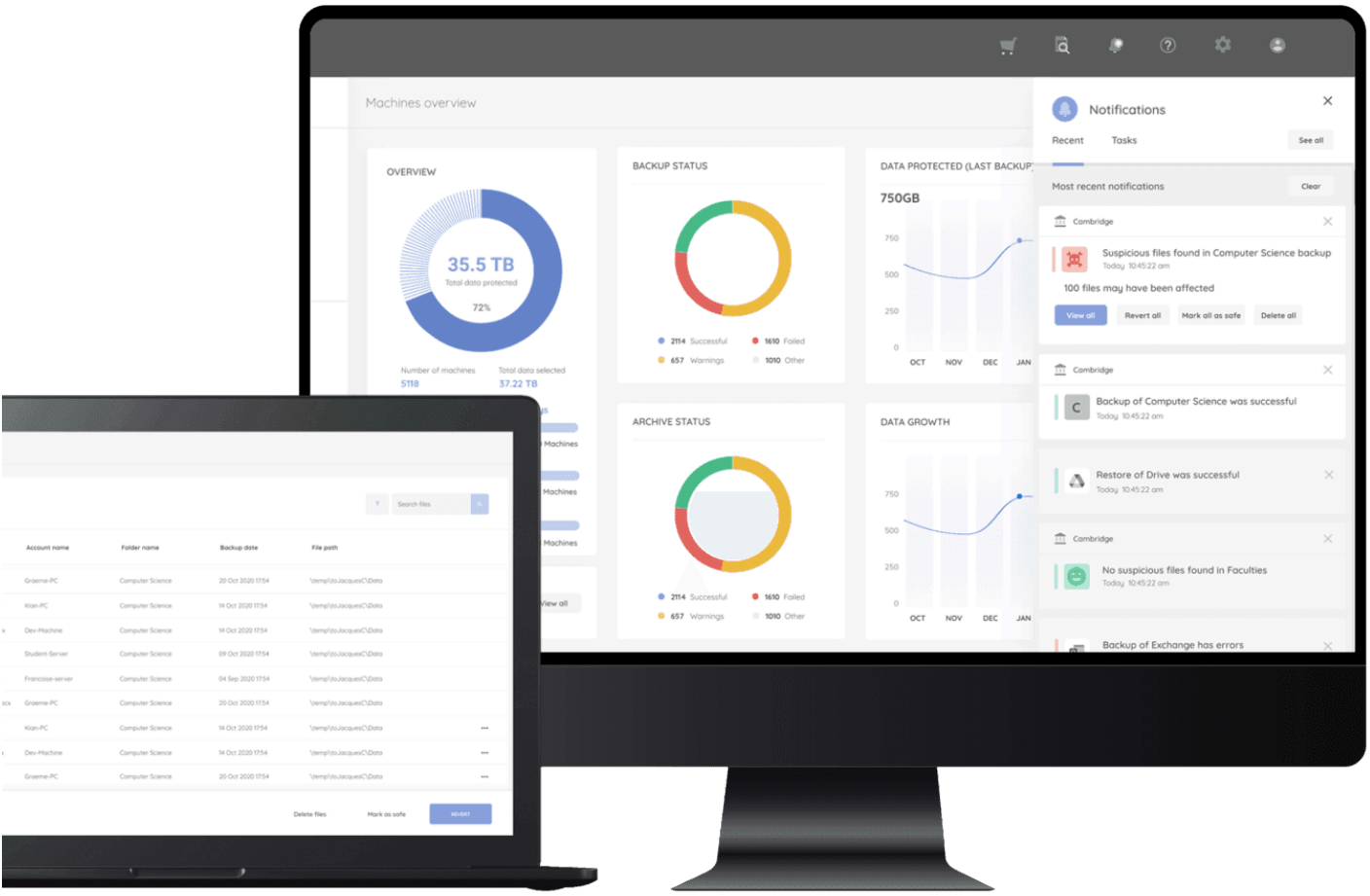
- quarantines them before they infect systems
- notifies you via the Redstor control centre and mobile app
- recommends actions to keep backups in a safe state



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





Keeping backups safe

Redstor's machine-learning model detects and isolates malware after every backup. So even if your 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).

Thank you for reading

Malware detection for backups - datasheet