6 reasons to demand Redstor's malware detection for backups

AI enables malware-free recoveries

*NEW - now supports Microsoft 365 & Google Workspace

Most organizations will have a form of anti-virus and malware protection in place, but cyber-criminals are becoming increasingly adept at infiltrating systems and hiding their activities.

Here we outline the six main reasons why Redstor's additional layer of protection for backups can help provide you with peace of mind in a rapidly changing world where malware is growing in scope and sophistication.

1. 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.

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.

Redstor has developed an advanced, machine-learning model to detect and quarantine malicious files within backups from servers and laptops, Microsoft 365 or Google Workspace. So you can rely on a clean and safe recovery.

When customers purchase automated malware detection as an added feature, every backup will be checked for files that resemble malware in appearance or behaviour.

2. Demonstrate compliance

The National Cyber Security Centre specifically advises organizations to use different products to increase overall detection capability, stating: “Deploy antivirus and malicious code checking solutions to scan inbound and outbound objects at the network perimeter."

By deploying Redstor’s malware detection and removal for backups as a complementary additional layer of protection, you will be following NCSC guidance.

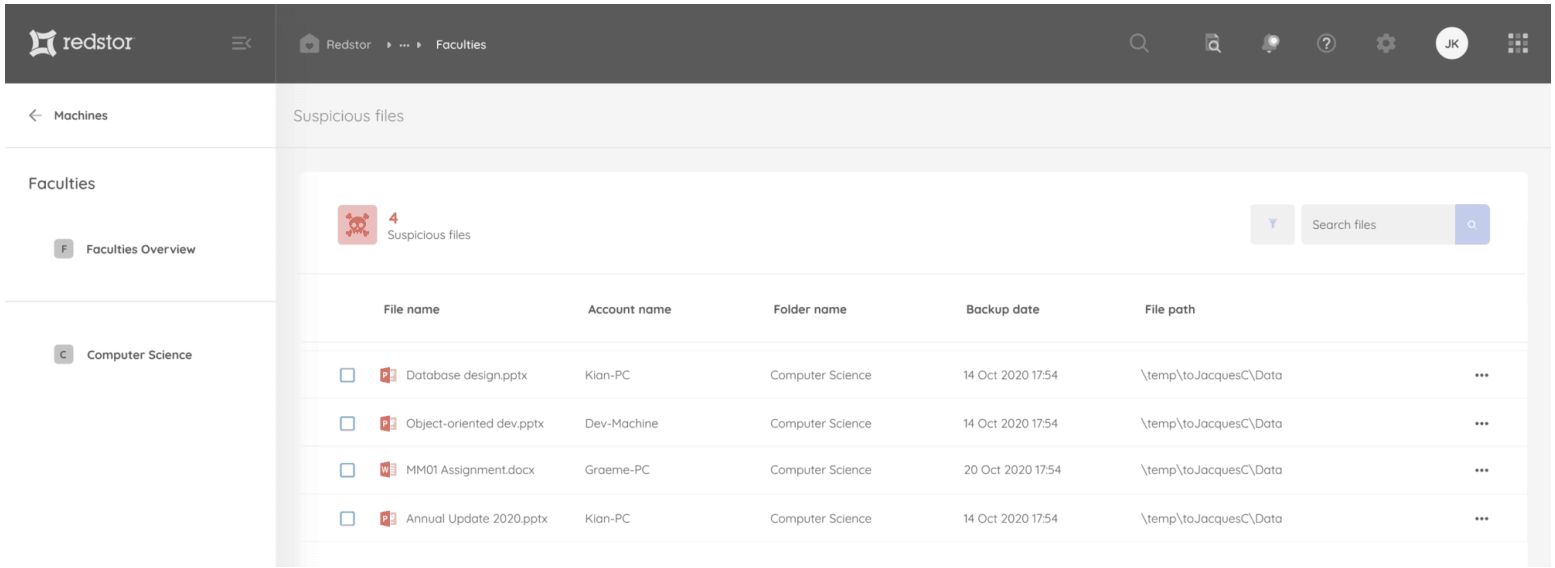
This recommends: “Where host-based antivirus is used it may be sensible to use different products to increase overall detection capability. Any suspicious or infected malicious objects should be quarantined for further analysis.”

3. Act quickly and decisively

Redstor will immediately quarantine suspicious files if they are detected in backups from servers, laptops, M365 or Google Workspace.

If you subsequently confirm a file as malicious there is the option to delete it and revert to a previous safe state or if you need to check further, you can leave it while you consider what action to take.

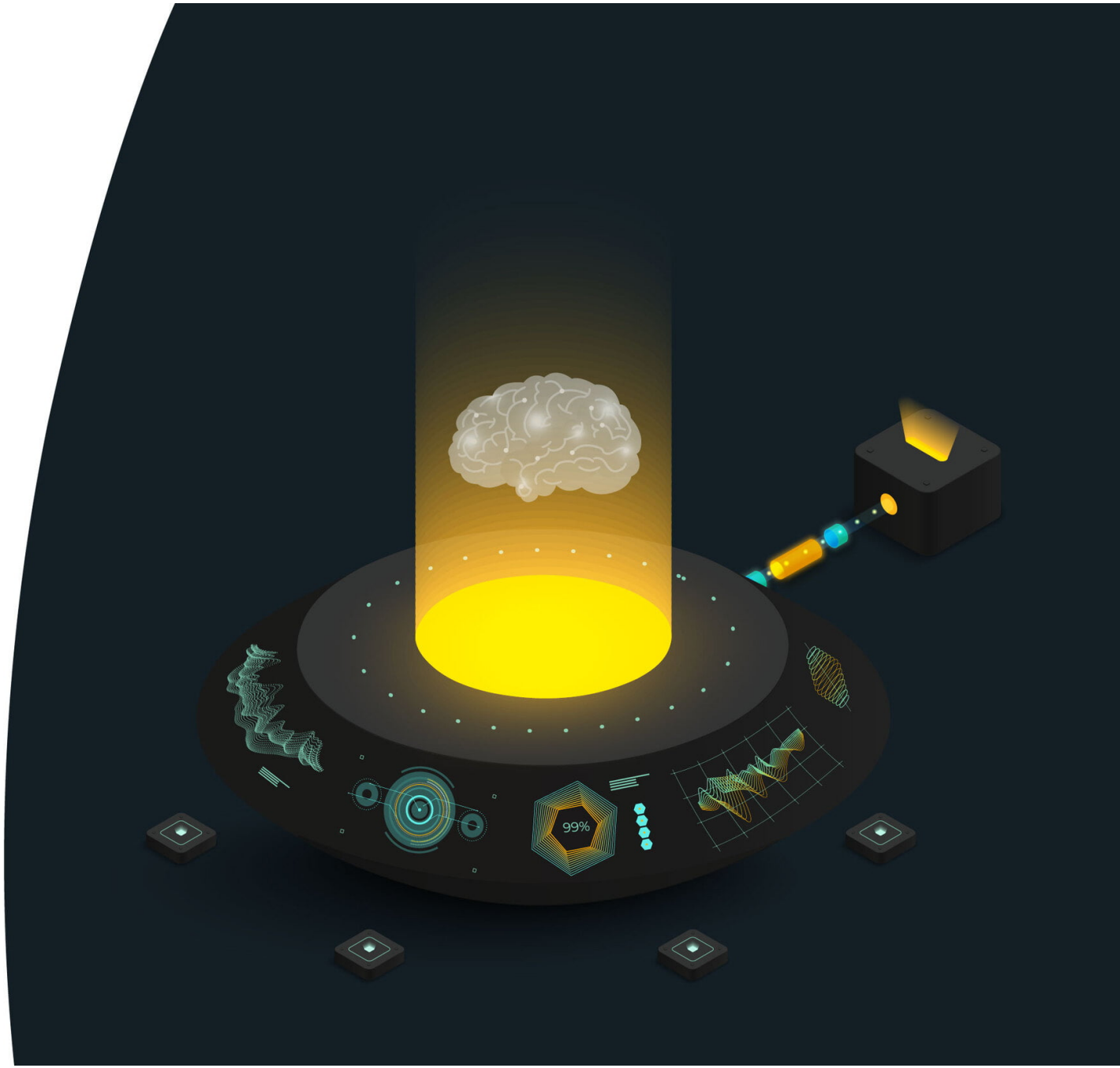
Alternatively, you can mark individual or multiple files as safe before releasing them into the new backup set.



4. Unlock the power of machine learning

With Redstor's malware detection and removal you are benefiting from the constantly evolving power of machine learning to identify threats within backup data.

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.

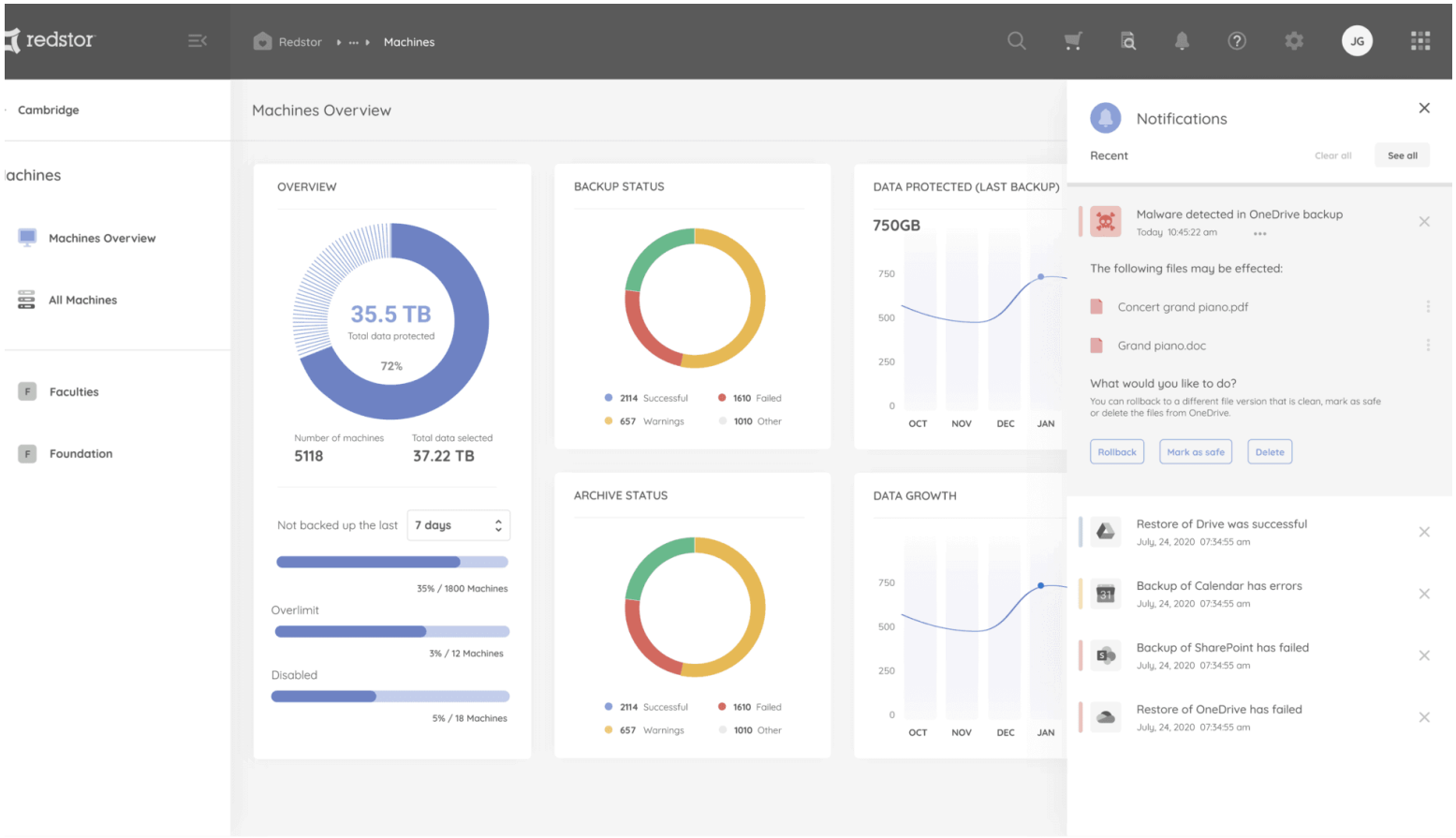


5. Save time with fast and easy set-up

Deploying malware detection is a simple matter of activating an add-on when you are a Redstor customer.

There is nothing for an IT department to configure, install or upgrade. No user intervention is required until a suspicious file is detected. Alerts are then sent via the Redstor control center and mobile app along with various recommended options to keep backups safe.

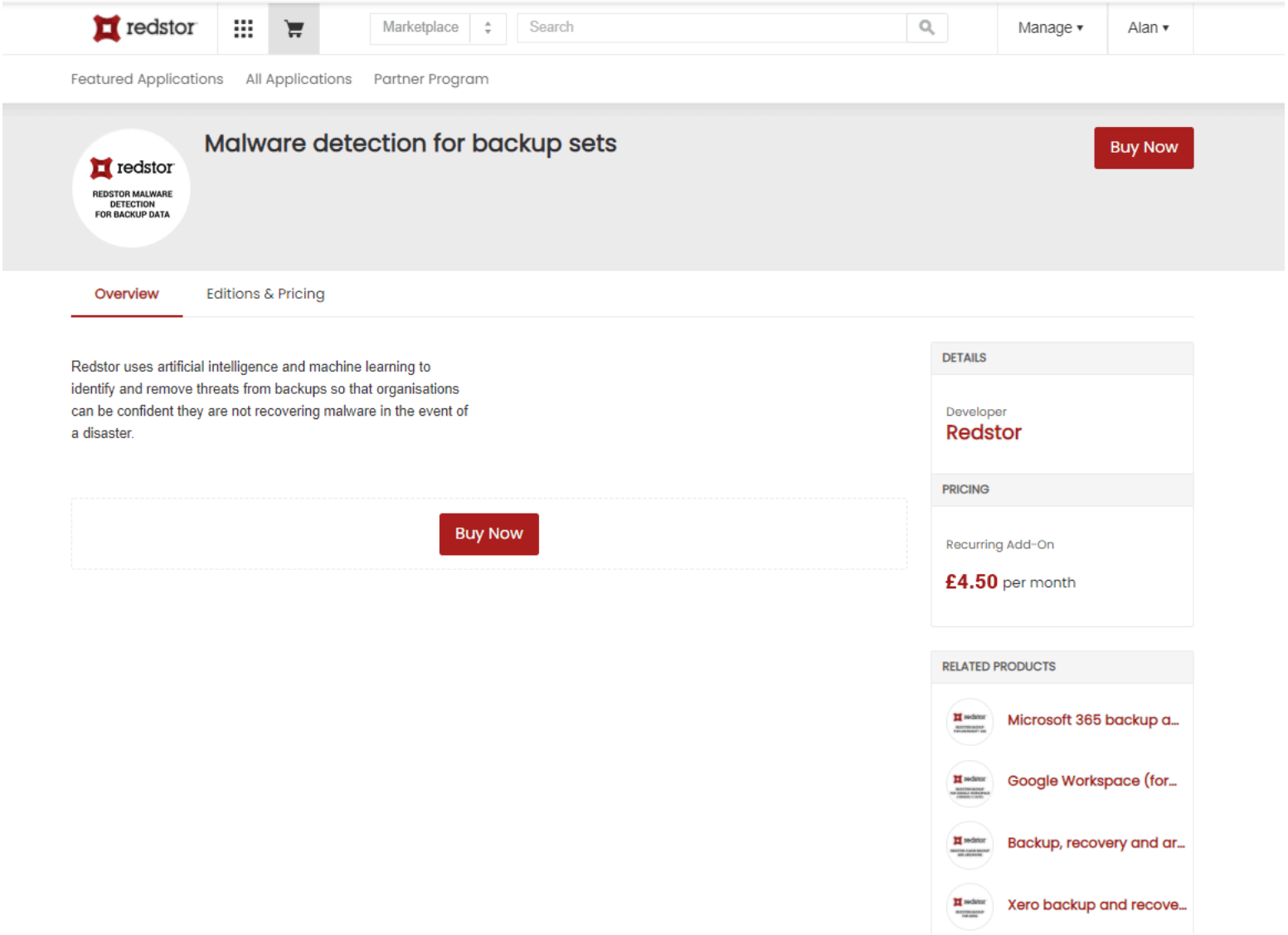
Take control with a single application that provides a comprehensive overview of everything you are protecting with Redstor and drill down to take action without switching between different products and credentials.



6. Avoid impact on your resources

Redstor's malware detection and removal for backups can be purchased and deployed quickly and easily through the AppDirect marketplace. Alternatively, our operations team can enable it through the Redstor storage platform console.

Either way, the service has no impact on your resources. All checks for malware in backups are made outside of your environment.



Thank you for reading

Malware detection for backups - brochure

www.redstor.com