

METADEFENDER STORAGE SECURITY™

# Backup Storage Scanning Solution

Continuous and Compliant Backup Protection for Cyber-Resilient Businesses

Built for speed, compliance and confidence, the Backup Storage Scanning solution built into MetaDefender Storage Security adds deep and comprehensive security for your data backup and recovery strategy.

**89%** of organizations had their backup repositories targeted by threat actors

**44%** of organizations had backup copies and assured cleanliness

**39%** of organizations restored data directly to the production environment

**ONLY 13%** were able to recover all impacted data following a ransomware attack

## Challenge

Many leading backup vendors leave room for dormant threats, including ransomware, to silently wait in archived files. Traditional backup solutions often lack comprehensive malware scanning during backup creation and restoration processes.



Limited Threat Detection



No Pre-Restore Scanning



Compliance Gaps



Hidden Malware Risk

## Features

### Centralized Storage Units Page

Connect and monitor all backup targets from one place. Support for NFS, SMB, and S3 storage types with real-time status monitoring.

### Identity-Based Scanning

Track and report on scans by user identity, enabling better visibility into who accessed or modified files across your storage infrastructure. Provide detailed metrics for compliance and security auditing.

### Backup Versioning Support

Scan by point-in-time restore with full version tracking. Automatic version detection for incremental/differential backups.

### Scan Analytics Dashboard

See threat types, scan outcomes, and storage usage at a glance. Interactive pie charts and trend analysis for comprehensive visibility.

### Flexible Scheduling Engine

Automate scans by policy, event, or custom cron rule. Support for periodic, post-backup, pre-restoration, and compliance-based schedules.

### Advanced Threat Detection

Metascan™ Multiscanning with 30+ engines, Deep CDR™\*, Proactive DLP™, Vulnerability Assessment and Adaptive Sandbox for comprehensive malware detection.

\*available in the next release

## Benefits

- Accelerated Compliance
- Clean Restores, Every Time
- Policy-Driven Automation
- Comprehensive File-Borne Threats Detection
- Scan and Recover at Enterprise Scale

## How It Works

01

### Connect Your Storage

- Add NFS, SMB, or S3 storage using the centralized dashboard
- Monitor status in real time [Operational, Error, Offline]

02

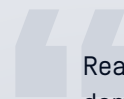
### Set Your Scan Policies

- Schedule automated scans: post-backup, pre-restore, or custom timing
- Stay compliant with less manual work

03

### Monitor and Act

- Use the analytics dashboard for clear scan results, threat categories, and coverage rates
- Confirm 99.9% scanning completeness across all backup units



Real-world testing with our 381,000-file dataset demonstrated a reduction from 23 minutes to just 42 seconds for backup rescanning—a 33x improvement that transforms our recovery time objectives.

### Enterprise Customer PoC Results