OPSWAT.

BROCHURE

MetaDefender Storage Security™

Proactive Backup Protection for Your Cyber-Resilient Backup & Recovery Strategy

Table of Contents

OPSWAT.

01

The Gap in Traditional Backup

Recent data reveals an alarming escalation in cyber threats: over 93% of ransomware attacks now deliberately target backups during cyber-attacks*, transforming what should be your last line of defense into a primary attack vector. While some backup vendors have added malware scanning into their portfolios, either bundled or through an integration with anti-virus engine, their offering for ransomware protection is still based on immutable backups, while true malware detection capabilities are limited beyond ransomware.

1.

Standard anti-virus scanning usually misses evasive malware, zero-day exploits, or latent malware hidden in backup files, especially in archives, databases and machine images.

2.

Polymorphic ransomware that bypasses signature-based detection, requiring advanced methodologies like heuristics analysis, anomaly detection or entropy analysis.

3.

Latent threats within backups, will easily bypass in-line scanning, making periodic rescans a mandatory requirement.

4.

Subtle but malicious file modifications.

5.

Stringent regulatory requirements (e.g., GDPR, PCI DSS, SOX... and Sheltered Harbor), which explicitly demand robust backup security, verifiable data integrity, availability guarantees, and proven recovery processes.

Organizations like financial institutions, where minutes of downtime translate to millions in losses, cannot afford disruption of any kind. More critically, they cannot risk their ultimate safety net - their backups - being compromised.

*: New Veeam Research Finds 93% of Cyber Attacks Target Backup Storage to Force Ransom Payment

OPSWAT.

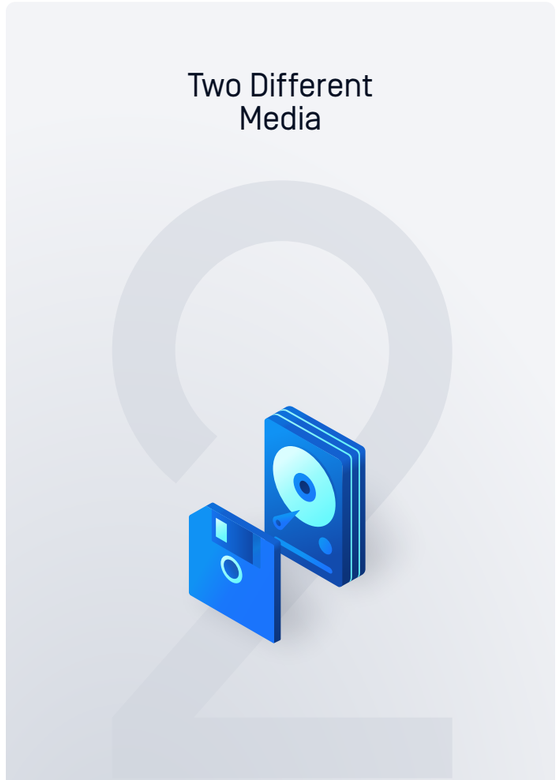
02

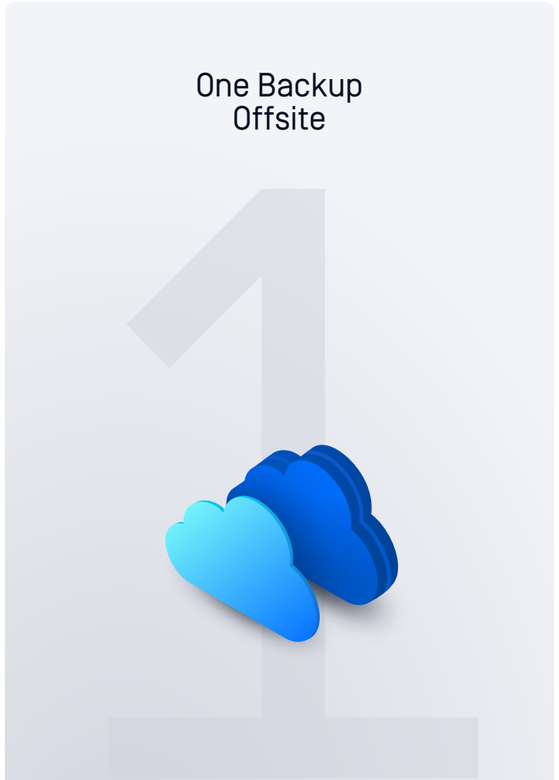
Importance of a Robust Backup and Recovery Strategy

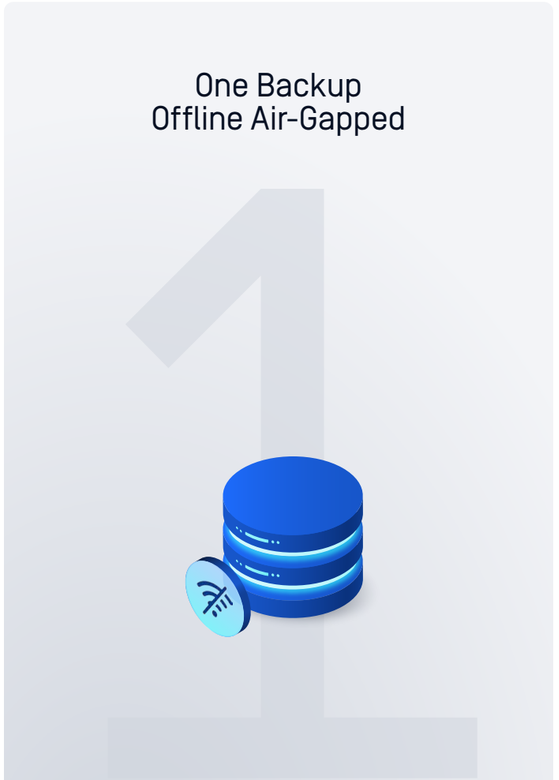
Recommended by NIST, the 3-2-1 model ensures redundancy and availability by maintaining three copies of your data, stored on two different media, with one kept offsite. The enhanced 3-2-1-1 strategy goes a step further by adding an air-gapped, offline, or immutable copy that's isolated from network access. This extra layer creates a critical backup workflow and drastically reduces the risk of malware spreading across all backups in a single event.

Having multiple backups is only half the equation. Organizations must focus equally on Recovery Time Objectives (RTOs), defining how quickly and safely critical services can be restored. In a disaster scenario - whether ransomware, sophisticated threats, or targeted cyber-attacks - the ability to recover within minutes without reintroducing malware or violating compliance, is what separates a cyber-resilient organization from a vulnerable one.

The next planning stage is ensuring security, reliability, and readiness. This is where MetaDefender Storage Security plays a critical role.







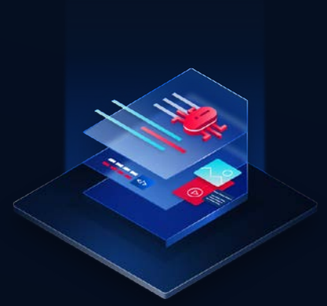
OPSWAT.

03

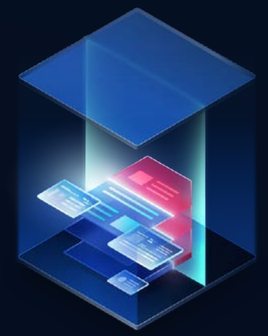
MetaDefender Storage Security – Enterprise-Grade Shield for Your Backup Data

MetaDefender Storage Security enables near real-time threat detection with a comprehensive solution tailored to validate and secure financial backups against modern cyber threats.

MetaScan™ Multiscanning leverages over 30 detection engines using machine learning, heuristics and signature-based analysis to deliver close to 100% detection accuracy for known malware and emerging malware variants.



Deep CDR™ technology disarms and regenerates clean, safe, and usable files when absolute assurance is required, such as post-ransomware recovery scenarios. This process neutralizes potential hidden threats without relying solely on static analysis, creating sanitized backup data for clean room recovery environments.



Adaptive Sandbox enables clean room for verification and dynamically identifies sophisticated threats through advanced entropy analysis, robust file and URL assessment, IoC extraction, and more.

Selectively scan only modified files by analyzing differentials and use **ETag validation** to skip unchanged files, ensuring thorough security checks while delivering on tight RTOs for critical workflows.

Leverage advanced content inspection and machine learning with **Proactive DLP™**, which detects sensitive, out-of-policy, and confidential data in files including PII, credit card numbers, and more. This enables rapid post-incident investigation, helping organizations pinpoint breach scope, assess compliance gaps, and demonstrate regulatory due diligence.

Flexible API-driven integration supports diverse backup workflows, storage targets, cyber vaults, tertiary vaults and recovery processes without operational disruption.

Secure backups across on-premises, cloud (IaaS/SaaS), and hybrid environments, including collaboration platforms.

04

Use Cases

Malware detection is a non-negotiable part of periodic recovery testing. Without robust malware scanning integrated into your backup verification process, even the most meticulous backup strategy can fail during actual recovery scenarios by reintroducing the very threats organizations are trying to recover from.

Continuous Backup Integrity Monitoring	Combines multiscanning, YARA-based detection, emulation-based sandboxing with entropy analysis, and real-time threat intelligence to uncover hidden malware in backup repositories. Optimized scanning workflows can be optimized by combining periodic deep analysis with diffs scan through metadata/hash lookups. Actionable intelligence that feeds into broader anomaly detection systems helps data examiners identify unusual patterns in backup activities.
Multi-Layered Backup Verification	Analyze entire backup sets using MetaScan Multiscanning and Adaptive Sandbox. Apply Deep CDR to critical files to eliminate hidden threats, active code, and embedded objects, ensuring only safe and usable content reaches your recovery systems. Once verified and sanitized, the clean data is pushed to a secure repository, preventing recovery loops caused by re-infection.
Rapid Change Detection	Implements periodic deep scans of backup repositories, and in the event of an incident, enables differential scanning based on integrity checks on known files to minimize Recovery Time Objectives (RTO) and ensure business continuity.

05

Smart Approaches Your Backup & Recovery Strategy

Approach	Scenario	
Quick Scan (Diffs Scan)	Generates ETags based on file metadata (modified time, size, path) for fast lookup.	Change detection, speed-sensitive scenarios Note: Deep Scan is still required for new files
Mid Scan (Content Hash Analysis)	Validates file contents via cryptographic hashing	Files drift detection/ file integrity monitoring/ immutable backup Note: Deep Scan is still required for new files
Deep Scan (Full Scan)	Metascan, YARA-based detection, Threat Intelligence and Sandbox	Needed for the base image and periodic rescans, or for high-risk scenarios (example: post-attack recovery validation)
Ransomware Recovery	MetaScan Multiscanning, Proactive DLP, Deep CDR	Compromised environment migration in which organizations must identify sensitive data and infected files to determine the root cause

Full Dataset First, Changes only After

Scanning large backup repositories can be both resource-intensive and time-consuming, especially when most files remain unchanged between scans. To address this challenge, we conducted internal benchmark tests on large backup datasets totaling 74GB and 381,000 files.

The goal: Validating the ability to maximize scanning efficiency while maintaining complete security coverage.

1.

Full Scan: Deep, Configurable, and Comprehensive

The initial scan covers the entire dataset with full forensic depth. It's powered by multiple virtual machines and is highly configurable through MetaDefender Core, ensuring defense-in-depth inspection for every file.

- Infrastructure: 9 VMs (8 vCPU, 8 GB RAM each)
- Duration: ~ 59 minutes
- Throughput: Full forensic analysis—no files skipped

2.

Diffs Scan: Smart Change Detection

Standard anti-virus scanning usually misses evasive malware, zero-day exploits, or latent malware hidden in backup files, especially in archives, databases and machine images.

- Infrastructure: 1 VM (8 vCPU, 8 GB RAM)
- Duration: ~4 minutes
- Throughput: ~5.2M files/hour (1.1 TB/hour)

06

Your Recovery Data Deserves Maximum Protection

For financial organizations, weak cyber resilience is a liability. With the rising tide of ransomware targeting backups, ensuring the integrity, availability, and recoverability of your data is critical to protecting customer trust, regulatory standing, and business continuity.

MetaDefender Storage Security empowers financial institutions with a proactive, multi-layered defense that safeguards backups against hidden malware, data drift, and targeted exploits—before, during, and after an attack. From rapid recovery validation to regulatory compliance (including DORA, PCI DSS, and SOX), our capabilities ensure your most vital assets remain uncompromised and your operations uninterrupted.

To see how OPSWAT's innovative solutions can keep your critical infrastructure safe, talk to an expert today.

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.