Storage-Layer Malware Control MSPs Can Operationalize

CLOUD STORAGE SECURITY

aws PARTNER

Challenges
Malware enters cloud storage quietly and persists

Cloud storage functions as a durable system of record. Files arrive through applications, user uploads, partner transfers, automation, migrations, and recovery workflows. Once written, those files are retained and reused across systems, often without additional validation.

When malware reaches storage, it frequently bypasses endpoint controls and remains undetected. It propagates into backups, resurfaces during restores, and complicates investigations long after the initial entry point. Without a control at the storage layer, risk accumulates over time rather than being contained.

The Cloud Storage Security Solution
Insert malware scanning into any workflow integrating cloud storage

Cloud Storage Security Antivirus introduces malware scanning at the point where data becomes persistent. Scanning integrates directly into cloud storage workflows without disrupting applications or performance.

The platform supports multiple scanning models to align with how data enters storage:

- **API-based scanning** inspects files before they are written to storage with minimal application changes
- **Event-based scanning** evaluates new and modified objects and scales automatically with data volume
- **Scheduled and on-demand scanning** inspects existing data to support compliance and hygiene requirements

All scanning runs close to the data and entirely within the customer environment.

All scanning runs close to the data and entirely within the customer environment.

Benefits

Files are inspected using multiple malware detection engines, including Sophos, CSS Secure, and CSS Premium. Using more than one engine reduces reliance on a single signature set and improves confidence in detection outcomes.

When malicious content is identified, policy actions apply automatically. Files can be tagged, quarantined, deleted, or routed into existing response workflows. Scan results remain available to support investigation, audit, and review.

In-tenant malware scanning
Inspection runs inside the customer account and region. Data does not leave the environment for scanning, supporting data residency and compliance requirements.

Centralized deployment and management
A single deployment manages protection across accounts, regions, and supported storage services. Policies remain consistent without operating separate tools per environment.

Multi-engine scanning reduces false positives
Multiple detection engines inspect each file, reducing the likelihood of undetected threats compared to single-engine approaches.

Predictable economics
Unlimited scanning supports large and data-intensive environments without per-GB penalties, enabling repeat inspection without cost uncertainty.

How the Platform Operates at Scale

Cloud Storage Security Antivirus is designed for environments where storage spans multiple services, accounts, and regions. The platform deploys centrally and discovers storage resources automatically, allowing consistent controls to be applied without managing individual tools per account or workload.

Scanning agents run close to the data and scale independently based on activity and volume. This avoids bottlenecks during peak ingestion, large transfers, or bulk restores, while keeping inspection isolated within each customer environment.

Operational Characteristics

Operational Model

Cloud Storage Security Antivirus is designed to run in environments that do not stay still. Accounts get added. Regions expand. Storage grows unevenly. Data shows up in ways that were not planned six months earlier.

The platform adjusts to those changes without needing rework. New storage resources are picked up automatically and brought under the same policies already in place. There is no need to re-architect workflows as environments evolve.

Built to Hold Up Over Time

Many storage-scanning approaches depend on custom glue code. They work until volume spikes, file sizes grow, or workflows change. At that point, they either fail quietly or get turned off.

This platform avoids that pattern. Scanning capacity expands and contracts with demand. Bulk restores, migrations, and high-throughput ingestion do not require special handling.

Predictable Behavior During Incidents

When malware is found, the response should not depend on who is on call. Actions are defined once and applied consistently. Files are handled the same way every time.

Results are recorded and available later. This matters during investigations, customer conversations, and audits, when teams need to explain what happened without reconstructing events by hand.

Designed for Continuous Use

Storage malware risk does not end after onboarding. Files get reused. Old data comes back into scope. One-time scans age quickly.

The platform supports repeated inspection over time without cost spikes or operational tradeoffs. That makes malware scanning something that stays on, not something that only runs when there is concern.

Why This Fits Managed Environments

This is not a tool that needs daily attention. Policies remain stable. Behavior stays predictable. Coverage expands as environments grow.

That makes it suitable for managed delivery, where consistency matters more than constant tuning

Most Subscribed Container Solution on AWS Marketplace

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

Built by the team that won three 2024 Cybersecurity Excellence Awards for cloud data security, AWS security, and antivirus.

See Success Stories

ANDPAD Inc.

MYOB Technology Pty Ltd

ikeGPS Group Limited

Get started with Cloud Storage Security solutions on AWS

Visit AWS Marketplace to start a Free Trial today.