SCALITY ARTESCA

SOLUTION BRIEF

Your backups are a target. Make them a dead end.

Scality ARTESCA as the immutable backup target for your Cohesity estate

Scality ARTESCA is the immutable S3 target that holds the copy you actually restore from.

An attacker who reaches your backups inherits their credentials

An attacker who reaches your backup environment inherits its credentials, and from that moment, anything the backup application can delete, they can delete. Encrypted or emptied backups are the point of the exercise, not a side effect. So the copy that survives is not the one with the best retention policy; it is the one the storage layer itself will not let anybody change. That is the job ARTESCA is built for. Backup buckets are created as immutable buckets using native S3 Object Lock, and critical data is held in compliance mode, where the guarantee is a property of the storage, not a permission someone can be trusted with.

Compliance mode, in the product documentation's own words

"Object Lock provides mathematically enforced immutability, making your backups tamper-proof. In Compliance mode, no user — including the root administrator — can alter, overwrite, or delete the object until the defined retention period strictly expires."

Source: *Scality ARTESCA Security Implementation Guidelines, Ransomware Neutralization via Immutability. ARTESCA product documentation 4.3.1.*

Holding the copy is half the job

The other half is getting it back fast enough that the business notices a delay rather than an outage, which is why ARTESCA publishes a documented restore rate for every configuration.

What the threat actually looks like

89%
of organizations had backup repositories targeted

34%
average share of an affected organisation's repositories modified or deleted

$1.53M
mean recovery cost, excluding any ransom

Source: *Veeam, 2025 Ransomware Trends: From Risk to Resilience, report body page 13. Sophos, The State of Ransomware 2025, June 2025.*

> **94% of IT leaders already rely on immutable storage or plan to within 12 months, and 69% call it essential to their cybersecurity strategy.**

Source: *Scality and Vanson Bourne survey of 500 IT leaders across the US, UK, France and Germany: scality.com/press-releases/immutable-storage- cybersecurity-survey. The survey does not publish a separate breakdown of "already rely on" against "plan to".*

© 2026 Scality · For partner and customer use

The stack

Cohesity manages the estate: policy, cataloguing, scheduling and recovery orchestration. Scality ARTESCA is the immutable target: 3 nodes on HPE hardware, S3 Object Lock in compliance mode, with room to grow to six.

Purpose-built, not adapted. Object storage first, not a general-purpose array with an object protocol layered on, and not sharing controllers with the primary workloads it is meant to protect.

Backed by $100,000, in writing. The ARTESCA Cyber Guarantee pays the customer directly if an external attack destroys or encrypts immutably-stored data. Conditions below.

Certified where it counts

ARTESCA's public overview page names eight certified backup applications, Cohesity among them, and the certification programme publishes what each tier covers. Validated Design, the top tier, carries integration documents, supported architectures, performance data, bills of materials and tuning procedures. Underneath that the platform presents 100% S3 API fidelity, so an application that speaks S3 and Object Lock is not relying on a bespoke connector.

Source: Certified applications and the tier definitions: artesca.scality.com/overview. S3 API fidelity: Scality ARTESCA product documentation 4.3.1.

Three things worth checking before you choose

Their guarantee may not cover the tier you are buying

Guarantees attach to specific product lines, not to vendors.

Scality ARTESCA pays a **$100,000 Cyber Guarantee** directly to the customer if an external cyberattack destroys or encrypts data stored immutably on ARTESCA. Conditions, all of them required: a commercial licence in production, a 50 TB minimum, v4.1.3 or higher kept current, protected data stored using S3 Object Lock in compliance mode, and recommended practices followed.

NetApp's Ransomware Recovery Guarantee covers "FAS, AFF A-Series, AFF C-Series, ASA A-Series or ASA C-Series running ONTAP based storage array system, with ONTAP One", capped at $5,000,000 per incident per array. StorageGRID, NetApp's object platform, does not appear in that eligible-systems list. The guarantee also requires the Recovery Assurance Service, ONTAP 9.12.1 P1 or later, patches within 60 days and AutoSupport always on. Insider threats are excluded.

Source: Scality: cyber-guarantee conditions stated verbatim at artesca.scality.com/en/cyber-guarantee. NetApp: Ransomware Recovery Guarantee additional terms, netapp.com, document dated May 2024, read live 2026-08-17.

Immutability documented and bounded, or left for you to discover

S3 Object Lock is a standard and both platforms implement it. What differs is how much the storage vendor writes down about how their implementation behaves, and where it stops.

Scality ARTESCA documents it at the platform, for any S3 client. The security implementation guidelines cover ransomware neutralization via immutability and direct compliance mode for critical data. The Object Lock reference states the limits plainly rather than leaving them to surface in deployment, including that cross-region replication is not supported on Object Lock buckets. ARTESCA also publishes a certification programme naming which applications have passed Validated Design testing, and what that tier covers.

NetApp does not cover it in the joint report. NetApp's own StorageGRID and Commvault technical report does not address Object Lock, immutability or WORM. It does state one architectural limit: StorageGRID as a primary backup target "cannot be used for live mount or live recovery operations", and is "ideal for streaming restore operation and for long-term retention". Stated fairly: StorageGRID does support S3 Object Lock, in both Compliance and Governance modes. The point is not capability. It is whether the configuration you deploy is already published and tested, or becomes an integration exercise on your time.

© 2026 Scality · For partner and customer use

We publish restore rates, not just backup rates

Backup throughput decides whether the window closes, and it is the number most vendors publish. Restore throughput decides how long the business is down.

Scality ARTESCA publishes both, per node count, with test conditions stated: compression factor x2, 32 VMs and 32 threads, spinning disk, 25 Gbps. At a 3-node configuration that is 8 TB/h backup and 6 TB/h restore at 1 MB blocks, and 12 against 10 at 4 MB blocks.

NetApp publishes no figure in the StorageGRID and Commvault report, where StorageGRID is described as "capable of high performance and massive throughput". Its Veeam best-practices guide documents the tuning expected instead: 4 MB block size over the default, task-slot limits tuned after steady state, and per-appliance multi-object delete limits of 34, 75 and 200 per request on the SG5712, SG5760 and SG6060. Immutability, it notes, "generates an increased number of requests to the object store".

Source: Scality: ARTESCA product documentation 4.3.1, and the vendor-publishing point at artesca.scality.com/en/glossary/restore-throughput, read live 2026-09-21. NetApp, both read live 2026-08-17: Backup and recover data using StorageGRID and Commvault, docs.netapp.com, 2026-07-09; StorageGRID best practices for deployment with Veeam Backup and Replication, docs.netapp.com, 2025-09-19.

Worth asking either vendor

Which product line does your guarantee cover, and is the immutable copy we would restore from inside it?

Where is your Object Lock behaviour documented, where does it stop, and what has been tested with our backup application?

What backup and restore rate is documented for the exact node count and media you are quoting us, and under what test conditions?

Your configuration, documented

At 3 nodes and 1 MB blocks, the documented figures are **8 TB/hour backup and 6 TB/hour restore**, under a compression factor of x2, 32 VMs and 32 threads, spinning disk and 25 Gbps. With 4 MB blocks the same cluster reaches 12 TB/h backup and 10 TB/h restore.

ARTESCA CLUSTER	BACKUP (1 MB)	RESTORE (1 MB)	BACKUP (4 MB)	RESTORE (4 MB)
1 node	5.5 TB/h	4 TB/h	8 TB/h	6.5 TB/h
3 nodes, your configuration	**8 TB/h**	**6 TB/h**	**12 TB/h**	**10 TB/h**
6 nodes	12 TB/h	9 TB/h	18 TB/h	15 TB/h

Source: ARTESCA 4.3.1 product documentation, Veeam Backup and Replication performance information. Publicly readable with no login at downloads.scality.com/artesca-ova/doc/partner_applications/backup_and_archives/veeam_backup_and_replication/index.html, read live 2026-09-08. Basis: documented, under the vendor's stated test conditions. Node counts and capacity range: scality.com/products/artesca, read live 2026-08-27.

© 2026 Scality · For partner and customer use

Two things we will tell you up front

Deploy 3 nodes as 3 nodes. A natively deployed 3-node cluster gives 2+1 network erasure coding plus 9+1 local, tolerating the loss of a node. The documentation is explicit that "expansions from 1 node to 2 nodes, and from 2 nodes to 3 nodes have the same level of protection as a 1 node architecture", so a 3-node cluster grown from one node is not node-fault-tolerant.

Immutable and geo-replicated is not one thing. Cross-region replication is not supported on buckets with Object Lock enabled. Multi-site immutability is handled by configuring the backup application to write independent immutable copies to each site. **ARTESCA** does provide built-in multisite replication for geo-resilience, but that is not a route to a geo-replicated immutable vault.

Room to grow. **ARTESCA** deploys in 1, 3 or 6 nodes, from a 20 TB starting footprint to a validated cluster maximum of 8.5 PB. Capacity comes primarily from drive density rather than node count, so six nodes buys capacity and throughput while fault tolerance stays what it is at three.

Confidence is not recovery

Almost every organisation believes it can restore. Far fewer find out they were right. The gap is not in the plan, it is in whether anything upstream of the storage was able to protect the copy the plan depends on.

90%
say they are confident they can recover within their RTOs

28%
of affected organisations fully recovered all affected data

44%
of them recovered less than 75%

Source: Veeam, Data Trust and Resilience Report 2026, figures as published in the company's release of 2026-04-14: veeam.com/company/press-release/veeam-report-reveals-a-market-wide-shift-from-recovery-confidence-to-proven-data-resilience-amid-ransomware-threats-and-ai-adoption.html, read live 2026-09-21.

That is the gap an immutable target closes. A copy the attacker cannot reach, and a restore rate the vendor publishes rather than estimates, are what turn a recovery-time objective into a recovery time.

Proof

30%
TCO reduction
Piraeus Bank, on data protection: 577 TB of Microsoft 365 for 12,000 users, kept on premises.

70%
capacity savings
SI Cloud, through intelligent optimization.

70
countries
Scality customers, including 7 of the 15 largest banks.

Source: scality.com/customers/piraeus-bank and scality.com/customers/si-cloud, both read live 2026-08-27. Reach: solved.scality.com, Scality ADI: AI Data Infrastructure, which is company-level reach rather than an ARTESCA-only metric.

SCALITY
RELIABLE. SECURE. SUSTAINABLE.

The copy that survives is the one the storage layer itself will not let anybody change.

A 45-minute technical session covers sizing for your capacity plan, the Object Lock configuration for your Cohesity deployment, and the documented restore rate against your recovery-time objective. Contact your Scality account team or partner representative.

scality.com