



SCALITYDAY26



SCALITY

ARTESCA

veeam

Restart the Business, Not the Attack

*Building the Minimum Viable Business with immutable storage
and clean room recovery*



Edwin Weijdema
Field CTO EMEA
Veeam



Billy Cashwell
Director of Product Marketing
Scality

THE CONFIDENCE PARADOX

**Organizations believe
they are ready,
...until they are tested.**



Confidence is high. Outcomes don't match.

What more than 900 security leaders, from the C-suite to frontline security, told Veeam

90%



were very to extremely
confident they can recover
within their defined RTOs

Veeam Data Trust and Resilience Report 2026

42%



of organizations with
incidents reported customer
or constituent service
disruption

Veeam Data Trust and Resilience Report 2026

28%



of ransomware-affected
organizations fully recovered
all affected data

Veeam Data Trust and Resilience Report 2026



Article 12: Backup, restoration and recovery

Backup policies and procedures, restoration and recovery procedures and methods

Requires financial entities to establish comprehensive backup and recovery protocols to minimize downtime and data loss. This includes defining backup scope and frequency,



using segregated systems for secure restoration, and performing regular testing.

Data Backup

Data Recovery

Data Portability

Data Security

Data Intelligence



Resilience is often assumed, not validated.



**Backup presence mistaken
for recoverability**



**Limited or unrealistic
recovery testing**



**Fragmented ownership
across teams**



The Minimum Viable Business, written down

What has to come back first, and what the clean room must prove before it does. Decided before the attack.

WHAT COMES BACK	WHAT THE CLEAN ROOM MUST PROVE FIRST	WHY IT IS FIRST
1  Identity	No attacker accounts, no changed memberships, certificate trust intact.	Everything else authenticates against it.
2  Core network and DNS	Matches last known-good. No rogue entries.	Nothing reaches anything without it.
3  The system you invoice from	Data intact to a named recovery point, reconciled forward.	Cash.
4  The system you pay people from	The same, plus the bank files and signing keys.	People.
5  The backup infrastructure	The clean room server is clean and holds only read-only credentials.	Production's backup server was a target.

Everything not on this list waits. That is a business decision, not an IT one.

Illustrative. Yours will differ.



The copy nothing can alter

Every item on your list restores from this copy, so it must be the one thing an attacker cannot change.

IT REFUSES THE DELETE



S3 Object Lock, compliance mode

Locked on write. No one deletes or overwrites it before retention expires, the storage admin included.

Governance mode has an account that can lift the lock. Compliance mode has none.

IT SERVES THE CLEAN ROOM



Without production up, or trusted

A second Veeam server reads the bucket read-only. Production Veeam does not have to be running.

The road to your backups no longer runs through the server the attacker hit first.

WE PUT MONEY ON IT



\$100,000

Cyber Guarantee

Paid directly if an external cyberattack destroys or encrypts data stored immutably on ARTESCA.

Conditions: commercial licence in production, 50 TB minimum, v4.1.3 or higher kept current, S3 Object Lock in compliance mode, recommended configuration followed.



Who already trusts it

Piraeus Bank, a DORA-scope European bank: 577 TB of Microsoft 365 backups on ARTESCA, 12,000 users, 25 years retained.

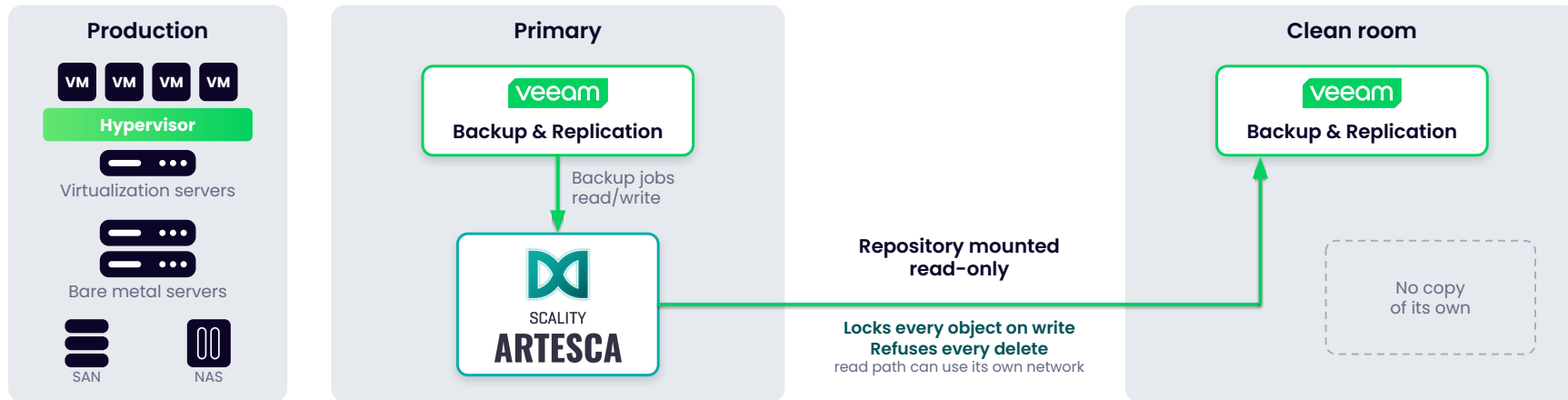
Veeam Ready Repository, Primary Target.

Refuses. Serves. Guarantees.



Production writes. The clean room reads.

Veeam 13.1 moves and reads the data. ARTESCA decides what can happen to it.



Reads everything, changes nothing

- ✓ Production writes to an immutable bucket, compliance mode
- ✓ The clean room mounts it read-only, no ownership transfer
- ✓ SureBackup rehearses; Threat Hunter and YARA rules scan

Gaps to close

- ! Every check loads the repository taking your backups
- ! Production knows where the repository is
- ! No copy of its own: ARTESCA Clean Room Pull closes this



Restart the business, in order

The right-hand column is what ARTESCA does at each step.

STEP	WHAT HAPPENS	WHAT ARTESCA DOES
0 The attack PRODUCTION	The attacker, holding admin credentials, tries to delete the backups, overwrite them and cut their retention short.	Delete a locked version: denied. Overwrite, or delete by name: adds a version or marker on top. The locked one stays. Shorten the retention: refused, for every account.
1 Identity CLEAN ROOM	Restored first into the isolated lab, scanned, attacker accounts removed.	Serves the locked copy to the clean room.
2 Network and DNS CLEAN ROOM	Checked against last known-good and the now-clean identity.	Serves the known-good recovery point.
3 Invoicing, then payroll CLEAN ROOM	Restored to a named point, reconciled, authenticated against clean identity.	Restores at documented rates, below.
4 The report EVIDENCE	What was tested, what was clean, which point, when. Then production.	Keeps every tested point locked until retention expires.

STORAGE IS NOT THE SLOW PART

ARTESCA documents Veeam restores at **6.5 / 10 / 15 TB/h** on 1 / 3 / 6 nodes.
The hours go into steps 1 to 3; rehearsing gets them back.

4 MB blocks, compression x2, 32 VMs, spinning disk, 25 Gbps network. ARTESCA product documentation.

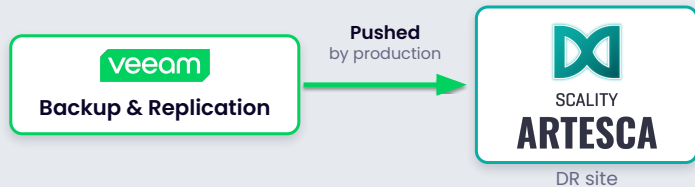


Can the attacker find your recovery copy?

Immutability protects the bytes. Invisibility protects where you recover.

PUSH · TODAY · BACKUP COPY JOB

Production sends the copy



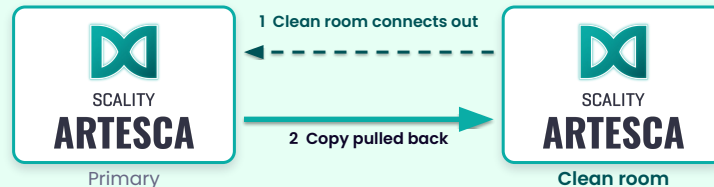
- ❗ Production's configuration has to name the target. Every push design does.
- ❗ The copy stays locked. The site around it becomes a target.

The attacker can find it.

Air-gapped

PULL · ROADMAP · CLEAN ROOM PULL

The clean room fetches the copy



- ✓ Air-gapped by design: no inbound connection, and its copy is immutable.
- ✓ Syncs on a schedule you set, so the load on your primary stays under your control.

The attacker cannot find it.

The repository you recover your list from should be one the attacker never saw.



The DR site of the future covers every disaster

Not just fire, flood and power loss. The attacker too.

THE DR SITE YOU HAVE

Built for natural disasters

- Designed for losing a site, not for losing trust in production.
- Nothing on it is immutable, and production can reach it.
- Rarely tested, because testing it disturbs production.

On the day, you still have to find out which copy is clean.

THE DR SITE WE RECOMMEND · BUILD IT TODAY

Built for every disaster

TODAY

Holds its own immutable copy on ARTESCA, at a separate site.

TODAY

Runs the heavy checks, YARA rules and restore tests, as often as you like, on a copy that takes no backups.

TODAY

Serves as your DR site and your clean room at once.

CLEAN ROOM PULL

Pulls its own copy, so production holds nothing that names it.

On the day, restart your list from a proven copy.

The restart is rehearsed long before you need it.



What to do Monday

Five things anyone in this room can start without buying anything.

01

Write the list

Applications, data, identities, services. In order, identity first. One page, an owner outside IT.



02

Write what must be proven

For each item, what the clean room must prove before it goes back. That is your rehearsal plan.



03

Check compliance mode

Not governance mode. And find out who can change retention.



04

Ask the two questions

Can you reach your recovery copy without your production backup server? Could an attacker in production find it?



05

Rehearse often, and report

On a copy that takes no backups, so it can run often. The report is your DORA or NIS2 evidence.





RESTART THE BUSINESS, NOT THE ATTACK

**After an attack, the question is not only
how fast you can recover.**

**It is whether you can restart the
business without restarting the attack.**



Questions and discussion · Find us at the Veeam stand



veeam



THANK YOU

SCALITY
DAY26