ASSURESTOR BACKUP2CLOUD + ZADARA ZCOMPUTE

Backup2Cloud

Guest-level agentless backup for Zadara zCompute instances

Powered by Asigra Tigris: deploy once inside your VPC via the marketplace template, protect every instance without installing a single agent.

AGENTLESS VIA NATIVE APIS | MARKETPLACE TEMPLATE | INLINE MALWARE SCANNING | COVERT PROTECT AIR-GAP | DATA SOVEREIGNTY

HOW TO POSITION IN 30 SECONDS

PROBLEM	RISK	OUR DIFFERENCE	OUTCOME
Zadara snapshots stay inside the same failure domain	Platform issue or attack impacts both production and snapshots	Independent, agentless backup running inside the customer VPC	Fully isolated, encrypted backup outside Zadara control plane

TALK TRACK

> *"Zadara snapshots are useful, but they stay tied to the platform. Backup2Cloud gives you an independent copy, deployed directly inside your VPC without agents. Data is encrypted before it ever leaves your environment and stored off-platform, so even a platform-level incident doesn't impact your recovery. It's complementary to snapshots but solves the gap they can't."*

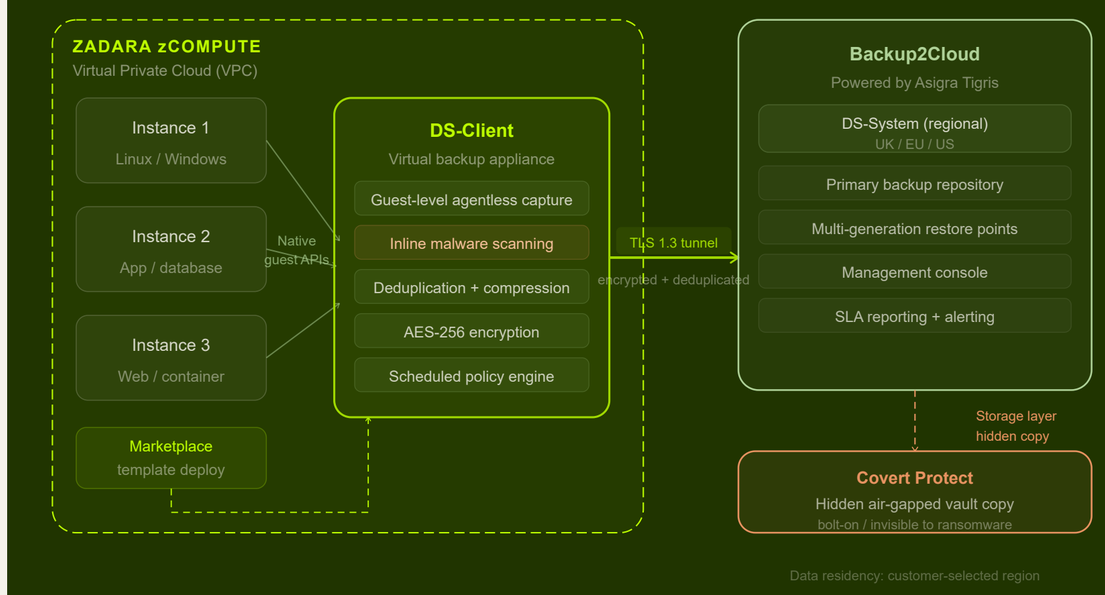
WHY BACKUP2CLOUD FITS ZCOMPUTE

- Agentless technology connects at the guest level using native operating system and application APIs with no agent software installed on any instance.
- No dependency on Zadara snapshot functionality or hypervisor integration, keeping backup fully independent of the underlying platform.
- A single DS-Client virtual appliance, deployed inside your VPC from the Zadara marketplace template, protects multiple instances simultaneously.
- Backup data is encrypted within the DS-Client before it leaves the VPC boundary.
- Additional DS-Clients can be provisioned from the same marketplace template as your instance footprint grows.

AGENTLESS ADVANTAGES

- No agent installation, patching or version management across your instance fleet.
- Consistent protection across Windows and Linux instances without per-OS agent configuration.
- Application-consistent backups via native guest APIs for databases, mail systems and file services.
- Reduced attack surface: no agent process on production instances provides an additional foothold to ransomware.
- New instances can be protected immediately upon DS-Client configuration, no agent deployment step required.

BACKUP2CLOUD FOR ZCOMPUTE SERVICE TOPOLOGY



COVERT PROTECT BOLT-ON: HIDDEN AIR-GAP AT THE STORAGE LAYER

Covert Protect is an optional bolt-on that operates entirely at the storage layer beneath the Backup2Cloud platform. It creates a complete hidden copy of the entire backup vault that is invisible to the operating system, backup application and any ransomware process running above the storage layer. Because the copy is made at the storage level rather than through the backup software, it cannot be enumerated, targeted or deleted by an attacker who has gained access to the backup environment. The result is an effective air-gapped recovery copy with no additional hardware, no tape and no manual intervention, providing a last line of defence when all other copies have been compromised.

ULTRA-SECURE CAPABILITIES: BACKUP2CLOUD PLATFORM

Inline malware scanning
Backup stream scanned for malware at ingest within the DS-Client before data is committed to the vault, preventing a poisoned backup being used to reinfect a recovered system, coupled with a second scan for restore operations.

Covert Protect air-gap
Storage-layer hidden copy of the complete vault, invisible to ransomware and any process above the storage tier, delivering a recoverable copy even when the primary repository has been attacked.

AES-256 encryption
Data is encrypted within the DS-Client before transmission. Encryption keys are held by the customer and never transmitted to the DS-System, meaning Assurestor has no access to plaintext data.

Zero-knowledge key model
The encryption passphrase is never sent to the DS-System. Full zero-knowledge architecture protects against supply-chain compromise and insider threat at the service provider level.

Multi-factor authentication
MFA enforced on the management console and on restore operations, preventing unauthorised recovery or policy changes even if credentials are compromised.

Data sovereignty
Regional DS-System deployments across the UK, EU and the US ensures backup data never leaves the customer's required jurisdiction, supporting GDPR and UK GDPR compliance.

TLS 1.3 in transit
All data in motion from DS-Client to DS-System is protected by TLS 1.3. No plaintext traversal of the internet occurs at any point in the backup or restore workflow.

Role-based access control
Granular RBAC with least-privilege separation between backup administrator, restore operator and compliance auditor roles, reducing the blast radius of a compromised account.

Anomaly detection
Platform detects abnormal data change rates, a common indicator of ransomware encryption activity, and raises alerts before a compromised backup set is committed to the vault.

COMMON OBJECTIONS AND RESPONSES

OBJECTION	RESPONSE
"We already use Zadara snapshots, why do we need this?"	Backup2Cloud is entirely independent of Zadara snapshot functionality and does not rely on it. It provides offsite encrypted copies with malware scanning, multi-generation restore points and a hidden Covert Protect copy that snapshots cannot offer. The two are complementary, not competing.
"We are concerned about backup data leaving our cloud environment."	The DS-Client sits inside your own VPC. Data is encrypted with your keys before it leaves the environment. You choose the DS-System region and data never crosses a jurisdictional boundary without your explicit configuration.
"Agent-based solutions give us more granular control."	Agentless does not mean less granular. The DS-Client uses native guest APIs to deliver file-level, volume-level and application-consistent backups across Windows and Linux with no agent lifecycle to manage and no additional attack surface on your instances.
"How does this fit into our standard deployment workflow?"	The DS-Client is available as a Zadara marketplace template and provisions as a standard VM inside your VPC using the same workflow as any other instance. There is no out-of-band tooling or professional services engagement required to get started.

COMPETITIVE DIFFERENTIATORS

- Only agentless backup solution with inline malware scanning available as a Zadara marketplace template.
- Covert Protect storage-layer hidden copy is unique: no equivalent exists in commodity cloud backup tooling.
- True zero-knowledge encryption with no shared-key model that creates a service provider backdoor.
- UK-headquartered Assurestor provides global support, data sovereignty, along with strong compliance for security over multiple regions, including full GDPR compliance and industry leading SLAs not available from hyperscaler-native tools.
- Platform-independent backup: no reliance on Zadara APIs, snapshots or hypervisor hooks means protection survives platform-level incidents.

IDEAL CUSTOMER PROFILE

- Zadara zCompute users with data sovereignty, GDPR or other compliance requirements.
- Organisations running mixed Windows and Linux workloads needing unified agent-free coverage.
- Infrastructure and DevOps teams wanting backup provisioned at the same time as new instances via the marketplace.
- Any organisation with ransomware resilience as a board-level or cyber-insurance requirement.
- Managed service providers managing multiple Zadara customer environments from a single management console.