ink&r

the
Incubator
team

SOLUTION BRIEF

Cloud-Native Data Protection

Key Benefits

For enterprises that are moving beyond IaaS and into broader cloud offerings, a cloud-native data protection solution should be an imperative. With this approach, an organization can achieve the following benefits:

- Applies continuous data protection for ALL new or existing in-scope cloud assets (IaaS, PaaS) according to policy
- Establishes guardrails to limit policy circumvention while providing deliberate capability for exception handling
- Builds a Product Mode discipline to allow for structured lifecycle management, which in turn promotes innovation
- Ensures auditable compliance and governance traceability using process maps that connect to repositories
- Further establishes a discipline of cloud automation with pullable code artifacts

ADDRESSING GAPS

Data Protection for Cloud

New architectural patterns such as Elastic Microservice Architectures (EMA) and Staged/Event-Driven Architectures (S/EDA), CSP innovations across their portfolios (Silicon, forked services, PaaS services), and corporate cloud assurance strategies such as frequent service repaving, have challenged the leaders in Gartner's Magic Quadrant for Data Center Backup and Recovery Solutions to provide comprehensive cloud data protection coverage.

Enterprises embracing these new paradigms are finding a ***growing gap with their current data protection vendors***, and the asymmetry is driving the need for native protection options that combine ongoing detective/corrective actions, automation ease for Product Team engagement, and complete compliance/audit traceability for assurance.

Our cloud-native data protection solution addresses this gap by focusing on the following areas:

- **Mapping cloud services that may persist data** – whether through established assertions or through discovery initiatives, we will separate cloud services into the following cohorts:
  - In-scope assets that may persist data
  - In-scope assets that may persist data but require exception
  - Assets that do not persist data and should therefore be out-of-scope
- **Building Functional (FR) and Nonfunctional (NFR) requirements** – FR/NFRs define the solution expectation that are articulated through use cases and are backed by thorough test cases which demonstrate adherence to each requirement. This provides a confidence in the overall solution, and establishes a Product Mode discipline

Source Site: https://ink8r.com

For more information, please contact us:

Satbir Sran
satbir@ink8r.com

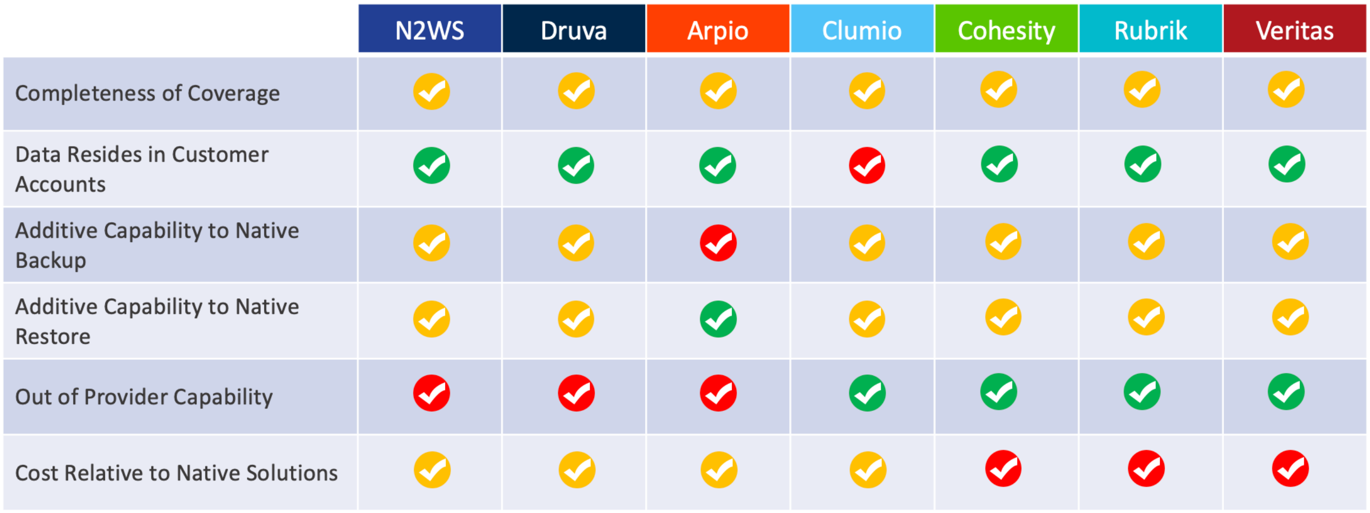
Darren Boyd
darren@ink8r.com

- **Delivering automated protection controls (centralized and/or decentralized)** – after establishing whether the solution is managed by an enabling team (Platform Engineering), the developer community (Product Team), or some combination – Insight will automate a codified solution to continuously protect all new and existing in-scope cloud assets
- **Balancing guardrails with a degree of flexibility** - through cultivation of detective/preventive/corrective controls, and ensuring a solution that works with declarative and/or imperative cloud deployment methods, our solution elegantly balances governance mandates with degrees of flexibility
- **Developing compliance & governance traceability** - our solution produces a traceability matrix that ties Control Statements together with FR/NFRs, through to detective/preventive guardrails and alerting mechanisms, demonstrating a complete end-to-end audit trail for ease of reporting

Vendor Comparison to Native Offerings

Commercial vendor solutions tend to have initial *coverage* gaps with respect to cloud-native services, thought they typically have high *compliance* adherence for the services they cover. This presents an interesting trade-off. Cloud-native solutions have capability to provide some inherent modicum of protection for their solutions but lack many tunable elements to effectively adhere to enterprise IT narratives.

Below is a relative contrast between several vendors against a representative enterprise customer with over 100 approved cloud services in use across a multi-cloud environment.



	N2WS	Druva	Arpio	Clumio	Cohesity	Rubrik	Veritas
Completeness of Coverage	🟡	🟡	🟡	🟡	🟡	🟡	🟡
Data Resides in Customer Accounts	🟢	🟢	🟢	🔴	🟢	🟢	🟢
Additive Capability to Native Backup	🟡	🟡	🔴	🟡	🟡	🟡	🟡
Additive Capability to Native Restore	🟡	🟡	🟢	🟡	🟡	🟡	🟡
Out of Provider Capability	🔴	🔴	🔴	🟢	🟢	🟢	🟢
Cost Relative to Native Solutions	🟡	🟡	🟡	🟡	🔴	🔴	🔴

Solution Overview

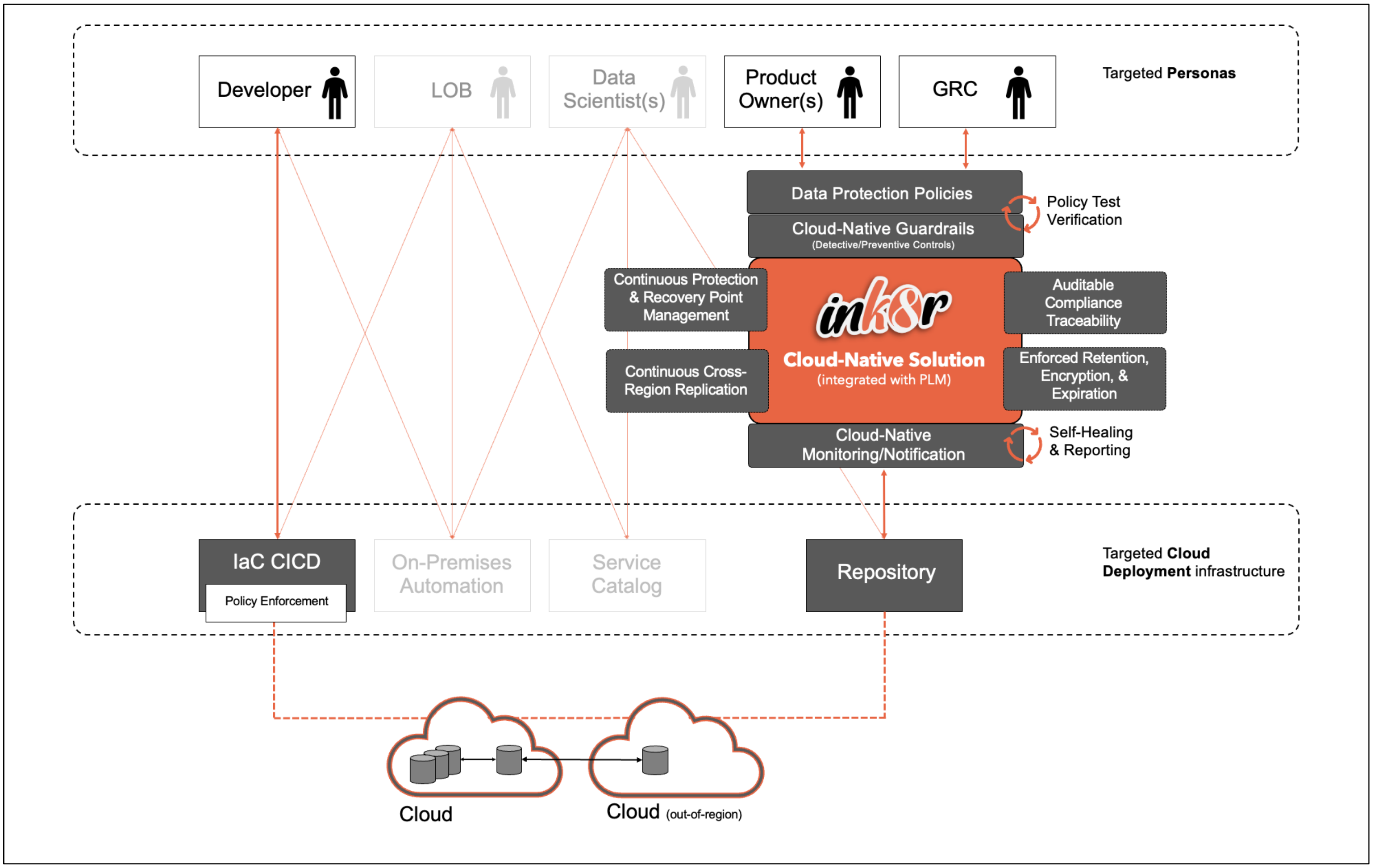
The solution below demonstrates the relationship between participating personas and a cloud-native data protection solution. Using methods described in this brief, we deliver solutions that maximize development time while ensuring all compliance and governance be met with respect to data protection.

All detective and preventative logic is codified and subject to Semantic Versioning 'SemVer' which is maintained by the Product Owner in collaboration with *Governance, Risk, Compliance* (GRC). Nested logic may be necessary to ensure conditionals are met around corner cases to meet the true needs of the organization.

Invocation of all codified artifacts happens through a tagging nomenclature which allows Product Teams to *declare* protection via *Infrastructure-as-Code* (IaC) enforcement, and/or Platform Engineering to enforce standards via detect/correct logic.

Solution nuances naturally exist based on cloud provider and additional solution options are available for self-healing mechanisms.

Deliverable artifacts tend to include source code, *Product Lifecycle Management* (PLM) advocacy program(s), and traceability and audit reporting.



Source Site: https://ink8r.com

For more information, please contact us:

Satbir Sran
satbir@ink8r.com

Darren Boyd
darren@ink8r.com