

RSA[®] IDENTITY GOVERNANCE & LIFECYCLE

VARONIS DATAPRIVILEGE[®] IMPLEMENTATION BLUEPRINT

AT-A-GLANCE:

The Varonis DataPrivilege[®] Implementation Blueprint is a packaged solution, which RSA Professional Services has created to reduce implementation time and cost regarding visibility into unstructured data.

Why?

- Reduce the application and audit of your unstructured data
- Lower administration costs regarding unstructured data authorization management
- Streamline user authorization requests and processes regarding your unstructured data (e.g. Joiners and Leavers)

What?

- Provide governance capabilities and lifecycle automation for unstructured data
- Gain visibility and control of user data and access permissions

How?

- Automate the user provisioning process based on groups, policies and approval workflows
- Provide user access reviews for users and their access to unstructured data
- Simple to use access request forms

SUPPORTED VERSIONS*

This has been validated to work on:

- RSA Identity Governance & Lifecycle v7x
- Varonis DataPrivilege 6.3 and above

**Please always check and confirm, as this solution may have been updated since this was created*

OVERVIEW:

Together, Varonis and RSA Identity Governance and Lifecycle deliver an enhanced data access governance solution that allows centralized management and control of unstructured data, to quickly detect and mitigate access risks, ensuring continuous compliance.

This Implementation Blueprint will help the business to quickly detect security and compliance access risks and amend access entitlements issues associated with unstructured data.

Closed-loop validation and user access reviews will help the business to get unstructured data under control, and provide clear visibility into who has access to what.

FEATURES & BENEFITS:

This Implementation Blueprint provides the following benefits:

- Enhanced visibility and control of unstructured data, directly within RSA Identity Governance & Lifecycle.
- Ensures users are granted appropriate access permissions in accordance with the organization's access policies.
- Reduces the attack surface and enhances regulatory compliance by limiting access privileges and deactivating stale and/or orphan accounts.
- Automation of the de/provisioning of access permissions

Key Use cases

- Unstructured data access certifications
- Self service access request for unstructured data
- Data owner approval for access requests
- Automate access provisioning and de-provisioning

For more details, please contact your local RSA Sales representative or RSA Solution Principle.

