RSA® DATA ACCESS GOVERNANCE

Access Control and Visibility for Unstructured Data

KEY BENEFITS

- Unmatched Visibility – Enables IT and the business to know definitively who owns enterprise data resources, who has access to what data resources, how they got access, whether they should have access, and who approved it across Windows file shares and SharePoint.
- Effective Access Certifications for Business Users – An automated access certification process generates actionable reviews that are simple and effective for business users to work with. A closed-loop workflow tracks and audits access changes, providing the evidence needed by auditors and regulators.
- Identification of Data Owners – Leverages user activity monitoring to determine who frequently accesses the data in question, which can be used to suggest owners.
- Enforcement of Compliance Policies – Easy-to-use business rules enable business and compliance policies associated with users, groups and access permissions to be tested or automatically enforced.
- Leverage Existing Security Investments – Leverages Microsoft AD group-based data access lifecycle management. Data classifications derived from DLP systems can be leveraged to determine controls and used for access risk management processes.

With the growth of the digital workplace, unstructured data such as documents, spreadsheets, images and media files accounts for 80% of enterprise data, and is continuing to grow exponentially. Governing access to data is an enormous challenge for organizations; there is often no easy way to understand where the data resides, who in the business has ownership of the data and who is entitled to access the data

RSA® Data Access Governance enables a sustainable access governance model by providing the visibility, monitoring, certification, remediation, and reporting of user access permissions to data stored on Microsoft® Windows®, Linux and Unix file servers, network-attached storage devices and Microsoft® SharePoint® servers.

With Data Access Governance Organizations Can:

- Gain visibility and ownership of user entitlements for Windows, Linux and Unix Servers, file shares and Microsoft SharePoint
- Automate the data access certification process for the lines-of-business
- Remediate inappropriate access and put in place a consistent methodology for group-based access to file shares and SharePoint
- Enable a closed-loop validation process for change to data access permissions
- Determine whether access policy and control objectives are being met
- Manage data access risk and provide auditable evidence of compliance

Capability Highlights

Scalable Architecture – The DAG architecture is a proven, scalable solution designed to meet the performance requirements of any size across tens of thousands of file shares and millions of files.

Enterprise-Wide Visibility – Automatically collects, correlates, and unifies user identities with Microsoft® Active Directory® accounts and groups, SharePoint groups and access permissions across all Windows file servers, network-attached storage devices and SharePoint servers. During collection DAG has a mechanism for metadata and classification discovery that can be used for access risk analysis.

Ownership & Accountability – A unique process for identifying business data owners and reaching out to them to validate ownership of the data, as well as metadata and classification information.

Access Certification – An automated end-to-end solution for data access certification enables IT Security to deploy a repeatable, auditable and business-oriented certification process. Up-to-date information about users, groups and permissions is collected from data resources and reviews are created automatically. Entitlement data used in the review process is presented in business friendly context.

Changes resulting from the certification process are tracked, and the system validates that they have been successfully made. Dashboards help information security personnel understand the status of certifications and escalations. Archived certifications and a complete audit trail provide the much needed evidence of compliance.

Configurable Workflow – Graphical workflow can be easily configured to accommodate an organization's unique access governance processes for review, approval, exception

handling and remediation. Integration with leading user provisioning and IT help desk systems routes changes to the appropriate individuals or access change fulfillment mechanisms.

Advanced Reporting – Ad hoc reporting, together with an extensive built-in reports, delivers detailed and summary analyses across all users, data resources, data entitlements and certifications.

Controls Automation – Business and IT teams can easily define data access business rules that automate the monitoring of inappropriate access permissions, including SoD violations, limiting the probability of business and compliance risks materializing. Compliance controls can be easily linked to the actual evidence.

Risk Analytics – In addition to providing comprehensive insight into the state of data access permissions, DAG provides IT security, compliance, audit and risk management teams with the metrics and decision support to make access risk management actionable.

Remediation – Automated remediation of user access permissions is supported via email and task notification, through integration with existing identity management and IT change management infrastructure, or through RSA Identity Lifecycle. A closed-loop validation process ensures that revocations of permissions occur within target data resources and enables an automated escalation process.

Part of a comprehensive Identity and Access Management Portfolio, RSA® SecurID® Suite:

RSA delivers a simple, secure, and efficient way to provide access to all of your users, no matter where they are, or what resources they are accessing. With a single, consistent approach, you can manage and control access for all of your users – internal and external, local and remote – across on-premise and SaaS applications and resources. With RSA® SecurID® Suite, you can easily ensure that users are properly authenticated, and have only appropriate levels of access throughout the identity lifecycle. You'll also be able to institute consistent governance and provisioning processes that help you efficiently deliver business user access, while maintaining continuous compliance with changing policies and regulatory controls.

RSA Identity Governance and Lifecycle Platform Automates the Complete Identity Lifecycle:

The RSA Identity Governance and Lifecycle platform provides robust capabilities to manage and automate the complete identity lifecycle. With this platform, organizations ensure that business users efficiently obtain access, while remaining compliant with security and regulatory policies. By streamlining access request and approval, simplifying access reviews, enforcing policies, and accelerating provisioning, organizations can reliably deliver business value from their IAM programs.

The RSA Identity Governance and Lifecycle platform comprises the following additional offerings:

RSA Identity Governance – Automates the monitoring, certification, reporting and remediation of user entitlements for on-premise and cloud-based applications.

RSA Identity Lifecycle – Delivers a streamlined request and fulfillment process with embedded policy controls to ensure that user access is appropriate, for on-premise systems, cloud-based applications, and data resources.

RSA Business Role Manager – Enables role discovery, modeling, management, and continuous lifecycle maintenance.

RSA Identity Governance and Lifecycle can be deployed on-Premise or as a Service (SaaS). This flexible deployment model gives you the choice of managing and governing identities and applications with on-premise hardware or software, or from the cloud.

RSA