RSA® IDENTITY GOVERNANCE

Gain Control and Visibility - Who Has Access to What

KEY BENEFITS

- Unmatched Visibility – Enables information security and compliance teams to know definitively who has access to what information resources; how they got access; whether they should have access; and who approved it, across all information resources.
- Automated Access Certification - Generates actionable reviews that are easy for business users to understand and work with.
- Assurance of Correct Access Changes – Tracks and audits access changes through integration with existing user provisioning and IT service management systems, or directly performs changes through RSA Identity Lifecycle. Either way, RSA ensures correct execution of access changes, ensuring that security and regulatory requirements are met.
- Enforcement of Compliance Policies – Easy-to-use access rules enable business and compliance policies associated with users, roles and entitlements to be easily tested and automatically enforced.
- Purpose-Built, Scalable Architecture – A highly-scalable solution designed for rapid deployment and high performance across hundreds of thousands of users, thousands of applications and millions of entitlements.
- Flexible Deployment Model – Supports on-premise or SaaS-based deployment.

RSA® Identity Governance simplifies how user access is governed across the enterprise, making it possible to achieve sustainable compliance by fully automating the monitoring, reporting, certification and remediation of user entitlements.

With RSA Identity Governance, Organizations Can:

- Gain enterprise-wide visibility into all user access privileges.
- Identify orphan user accounts and inappropriate user access.
- Automate user access review and certification processes.
- Manage and audit all entitlement changes through integration with enterprise-wide access fulfillment and enforcement systems.
- Implement security and compliance controls such as segregation of duties (SoD) and ensure that policy and control objectives have been met to provide evidence of compliance.
- Deploy efficient and consistent processes around Joiner, Mover, and Leaver access lifecycle events.

Capability Highlights

Rapid Time to Value – Deliver value quickly through an approach based on "configuration, not customization." By reducing project cycle times, RSA's solution quickly enables automated, auditable business processes for the management, monitoring, reporting and remediation of access rights to enterprise information assets.

Enterprise-Wide Visibility – Achieve deep visibility into "who has access to what", using RSA's patent-pending unification process, which automatically collects, aggregates and correlates user identities with account, group, role and entitlement data across all enterprise information resources. Comprehensive reporting features provide the transparency that security, risk management and compliance teams require.

Access Certification – An automated end-to-end solution for access certification enables information security to deploy a repeatable, auditable and business-oriented certification process. Up-to-date information about user accounts, groups, roles and entitlements is collected, and reviews are created automatically. Access data used in the review process is presented in a business-friendly context that is easily understood by reviewing managers. By automating the certification process, RSA Identity Governance enables security teams to drive accountability for governing access into the business, while reducing the organizational burden, complexity and cost of access compliance. Changes resulting from the certification process are tracked, validated and can be audited easily.

Configurable Workflow – Visual workflow can be easily configured to accommodate an organization's unique access governance processes for review, approval, exception handling and remediation. Changes can be fulfilled through integration with RSA Identity Lifecycle's provisioning capability, IT help desk systems or other access change fulfillment tools. Regardless of fulfillment mechanism, RSA Identity Governance provides a closed-loop access change validation process to ensure that entitlement changes occur correctly in target information resources.

Reporting – An extensive set of built-in reports, together with ad hoc reporting, delivers detailed and summary analyses of review certification status across all users, information resources and entitlements. Reporting dashboards help Information Security personnel understand the status of certifications and escalations. Archived certifications and a complete audit trail provide the evidence of compliance needed by auditors.

Policy Automation – Business and information security teams can easily define business rules that automate the monitoring of user entitlements and roles for early identification, notification and remediation of inappropriate access including segregation of duties (SoD) violations. Easy-to-use business rules enable security and compliance policies associated with users, roles and entitlements to be tested or automatically enforced. Control remediation capabilities provide a risk acceptance process and a complete audit trail for access decisions. Continuous access compliance is enabled through automated detection of Joiner, Mover, and Leaver lifecycle events, coupled with automated responses (such as an incremental access review).

Risk Analytics – In addition to providing comprehensive insight into the state of access privileges, RSA Identity Governance provides information security, compliance, audit and risk management teams with the metrics and decision support to make access risk management actionable. Risk sensitivity ratings can be applied to high-risk users, roles, information resources or events and then tied to specific controls, which enables access risk to be effectively mitigated or remediated.

Remediation – Automated remediation of user access privileges is supported across the enterprise via email and task notification, through integration with an organization's existing identity management and IT change management infrastructure, or directly through the RSA Identity Lifecycle solution. A closed-loop validation process ensures that entitlement revocations occur correctly and quickly, and provides automated escalation if changes exceed a target timeframe.

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 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 Data Access Governance – Provides visibility, business ownership identification, and control over access to data resources, including file shares and Microsoft® SharePoint®.

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.