

Data Access Governance

Visibility and control for unstructured data

With the continued pace of digital transformation, unstructured data—data stored in SharePoint, file shares, collaboration platforms, NAS devices and more, both on-premises and cloud-based—accounts for 80% of enterprise data and will continue to grow exponentially. Governing access to that data is a challenge for organizations, as there is often no easy way to provide insight into where the data resides, who has ownership and who is entitled to access the data.

SecurID® Governance & Lifecycle delivers a next-generation open framework to enable a sustainable model for data access governance. It provides visibility, monitoring, certification, remediation and reporting of user access permissions to data stored on file servers (Windows, Linux and Unix), NAS storage and SharePoint servers.

Secure sensitive unstructured data, reduce risk and address compliance mandates

Gaining control of the massive volume of unstructured data is a critical IT and business objective given the rapid pace of digital transformation, including the recent accelerated shift to people working beyond the traditional secure perimeter. The data access governance capability of SecurID Governance & Lifecycle empowers data owners to control access and map users, data owners and access permissions—all to eliminate the exfiltration of sensitive data, reduce threats and improve an organization's digital risk posture.

Flexible and scalable architecture

The SecurID Governance & Lifecycle data access governance architecture is a proven, scalable solution designed to meet a broad range of performance requirements across tens of thousands of file shares and millions of files.

Enterprise-wide visibility

SecurID Governance & Lifecycle collects, correlates and unifies user identities with Active Directory accounts and groups, SharePoint groups and access permissions across all Windows file servers, NAS devices and SharePoint servers.

Enhanced ownership and accountability

Leveraging of user activity and folder ownership helps suggest data resource ownership assignments.

Leverage data classification

The use classification of unstructured data influences and improves governance processes. Organizations can highlight in-review processes and dynamically adjust approval processes based on associated data classification.

Key features

- Risk-based access certification—Provides automated end-to-end data access certification, for a repeatable, auditable and business-oriented process.
- Configurable, graphical workflows—Can be configured to accommodate an organization's governance processes for review, approval, exception handling and remediation. Dynamically adapts to changing business processes based on data classification.
- Integration with leading user provisioning and help desk systems—Routes changes to appropriate individuals or access-change fulfillment mechanisms.
- Controls automation—Enables business and IT teams to easily define the business rules that automate monitoring of inappropriate access permissions (including SoD violations).
- Automated remediation of user access permissions—Is supported via email, ticket system integration and task notification. Closed-loop validation ensures accurate revocation of permissions within target data resources.

Key benefits

- Unmatched visibility—Know who owns enterprise data, who has access to data resources, how they got it and whether they should have access across file shares.
- Automated certification process—Generate actionable reviews that are simple, intuitive and effective for business users to provide evidence for audit teams.
- Identification of data owners—Review data ownership to ensure accountability over the governance of unstructured data.
- Enforcement of compliance—Apply easy-to-use business rules to automatically enforce compliance policies associated with users or groups.
- Leveraging of existing security investments—Leverage AD group-based data access lifecycle management.

SecurID Governance & Lifecycle

SecurID Governance & Lifecycle delivers continuous risk-based access assurance for organizations to ensure their users have the proper level of access to systems, data and applications. By providing visibility across islands of identity in today's blended cloud and on-premises environment and combining that visibility with risk analytics, the solution enables prioritizing high-risk access situations and empowers business users to quickly and easily address those of highest impact to reduce business risk and ensure compliance.



About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com.