opentext™ | Cybersecurity

Data Sheet

NetIQ Identity Governance

NetIQ Identity Governance accelerates access certification, reduces risk of inappropriate access, provides analytics for users in technical and business roles, and satisfies auditors

Are You Governing Who Has Access to What Effectively?

Satisfying identity governance regulations and managing risk requires organizations to inventory, analyze and manage their users' access privileges. Failure to manage users' access to sensitive resources places companies at increased risk for negative audit findings, fraud or data breaches

Access review and recertification campaigns are an essential part of an overall identity governance program. Yet answering the critical question "who has access to what?" is a challenge. The line between the typical employee's work and personal persona, along with their use of mobile devices, cloud computing and social media, are shifting workforce trends. Add to this the increasing numbers of contractors, partners and service providers and this is causing organizations to seek more efficient ways to conduct access certification campaigns that encourage participation by line of business (LOB) managers.

Product Overview

NetIQ Identity Governance by OpenText™ is a solution that helps any organization run effective access certification campaigns and implement identity governance controls to meet compliance mandates while proactively mitigating risk. Built to get organizations up and running in hours vs. the weeks or months of traditional legacy vendors, NetIQ Identity Governance replaces error-prone, time-consuming manual methods that can expose your organization to compliance violations and risk from excessive access.

NetIQ Identity Governance provides a way to quickly identify and revoke access to resources users don't need—such as when users change positions in a company and inadvertently accrue too many privileges. NetIQ Identity Governance collects user entitlement information across multiple systems, applications, and data into a consolidated view. These capabilities provide easy-to-understand reports for LOB managers to validate whether existing employee access privileges are appropriate and initiate immediate action to revoke any access, if necessary.

Key Capabilities

- **Collect and review entitlement data** across the infrastructure, including on-premises, hybrid and cloud applications, so you have accurate visibility into who has access to what resources.
- **Leverage analytics and role mining** to identify commonalities in entitlements, perform "what if" analysis, and produce compliance metrics and reports.
- **Conduct access certifications** with campaigns that stay on schedule through automatic reminders and progress updates, including decision support for approvers and issue escalation for administrators.
- **Define controls to detect and handle violations and exceptions** such as SOD violations or orphaned accounts to reduce risk.
- **Set business-based role and attribute authorization models** to reduce the scope and duration of access certifications and access request and approval processes. This allows a focus on exceptions, rather than all entitlements.
- **Close the loop on remediation**, including integration with service desk solutions such as ServiceNow or Remedy for automated ticketing, or automated fulfillment via integration with NetIQ Identity Manager by OpenText™.
- **Conduct reviews prioritized by risk scoring** based on attribute value, group membership, management relationship, application, permission, cost, risk and other criteria, providing focus where most needed.
- **Report on identity governance** with out-of-the-box support for scheduling and distribution that includes entitlements, certification status, request and approvals, and policy violations to make audit reporting easier.

Key Differentiators

- **Real time adaptive governance enables continuous risk reduction.** Competitive solutions collect entitlements at a point in time, but this leaves organizations blind to risk until the next collection. NetIQ Identity Governance adapts to changes and events as they happen and can trigger a review to ensure compliance.
- **Drive better access decisions through business insight.** Provide business context information such as risk and cost of access, comparisons to users with similar responsibilities and other pertinent information directly in the review and approval interfaces. This arms your business users with the knowledge they need to make better decisions regarding user access.

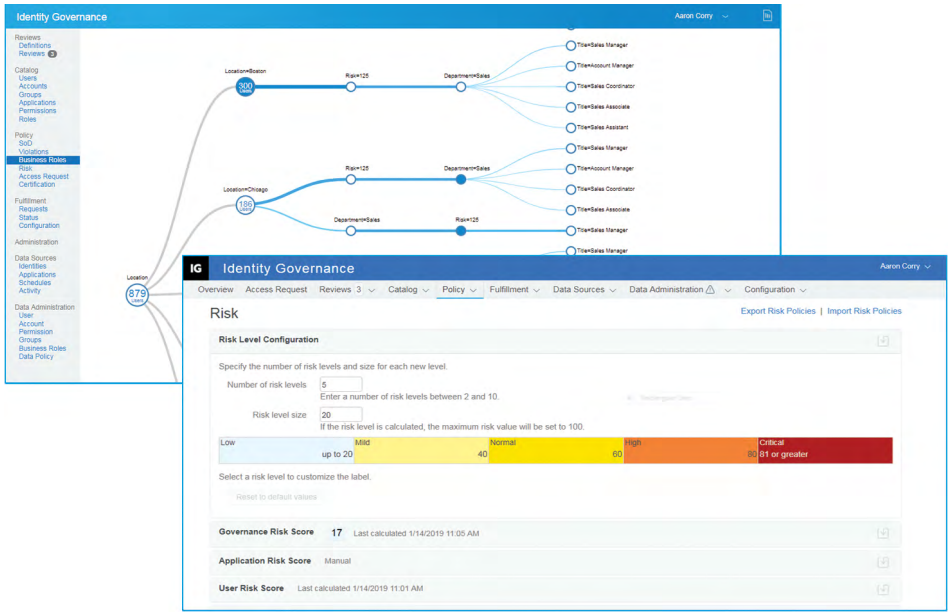

Figure 1. NetIQ Identity Governance can perform role mining to identify commonalities in entitlements, and display analytics to report on role leverage.

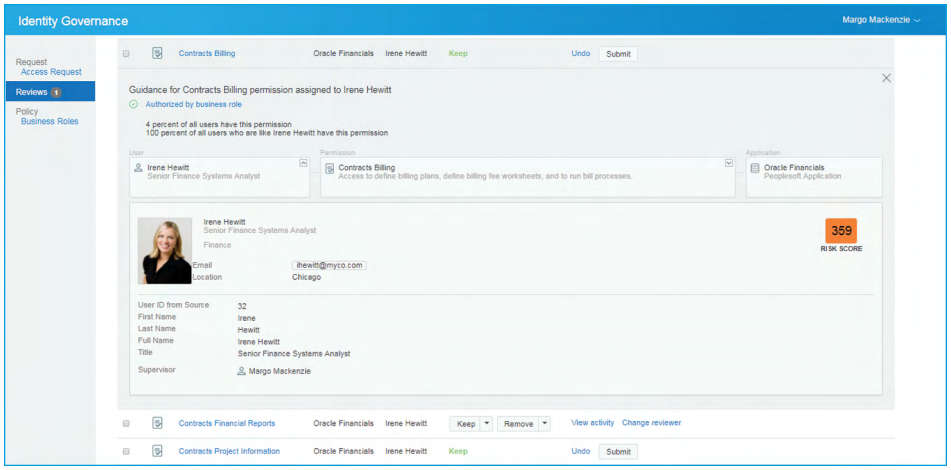

Figure 2. NetIQ Identity Governance provides line of business managers with decision support during access certification so they can understand whether the access is out of the norm, high risk, etc.

NetIQ Identity Governance offers flexibility of delivery options and can be deployed on-premises or via public/private cloud, Managed Service Provider, or Software as a Service (SaaS).

To learn more about NetIQ Identity Governance, go to: **www.microfocus.com/en-us/cyberres/identity-access-management/identity-governance**

Connect with Us
www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

760-000004-005 | O | 10/23 | © 2023 Open Text