KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger
December 15, 2020

Atos DirX Audit

DirX Audit is the Access Intelligence and Analytics solution within the Atos DirX portfolio. It provides insight not only in risks related to static entitlements, but also can analyze concrete access. It comes with dashboard, KPI, and reporting capabilities, providing flexible insight and a high level of detail on audit-related data. Furthermore, it can collect data from a wide range of applications, further enhancing insight into access risks.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

1 Introduction 3

2 Product Description 5

3 Strengths and Challenges 8

4 Related Research 10

Content of Figures 11

Copyright 12

1 Introduction

Access Governance & Intelligence is an IAM focused risk management discipline that facilitates business involvement in the overall management of access rights across an organization's IT environment. Access governance provides necessary (mostly self-service) tools for businesses to manage workflows and access entitlements, run reports, access certification campaigns, and SOD checks. Access intelligence refers to the layer above access governance that offers business-related insights to support effective decision making and potentially enhance access governance. Data analytics and machine learning techniques enable pattern recognition to deliver valuable intelligence for process optimization, role design, automated reviews, and anomaly detection.

Access Governance concerns the access mechanisms and their relationships across IT systems and thus is instrumental in monitoring and mitigating access-related risks. These risks most commonly include information theft and identity fraud through unauthorized changes and/ or subversion of IT systems to facilitate illegal actions. During the last few years, many prominent security incidents originated from poorly managed identities and proved the need to address these issues across all industry verticals. Data thefts, loss of PII (Personal Identifiable Information), breach of customer's privacy, and industrial espionage are becoming common security risks in virtually every industry today.

Access Governance, an IAM focused risk management discipline, focuses on providing answers to three key questions:

- Who has access to what?
- Who has accessed what and why?
- Who has granted that access?

That is done via a set of functionalities, which include the following features:

- Access Warehouses: Collecting current and previous access information from different systems. The collection can be done via direct or extensible connectors using established standards such as HTTP or webservices. Provisioning connectors or flat file imports are commonly used for the purpose.
- Access Certification: Requiring the responsible persons (such as resource owners or application managers) to do scheduled or ad-hoc reviews of the current status of access controls and request changes if required.
- Access Analytics and Intelligence: Analytical capabilities to facilitate business-friendly understanding

of the current status of access controls, sometimes complemented by adding real-time monitoring information about access to IT assets.

- Access Risk Management: Using a risk-based approach to evaluate and assign risk score for access requests and invoking relevant access workflows and notifications based on configured policies.
- Access Request Management: Providing interfaces to request access to specific information or systems including workflow policy configurations to define and manage request flows.
- SoD controls and enforcement: Definition and enforcement of business rules to identify and prevent Segregation of Duty risks.
- Enterprise Role Management: A complementary technology given that roles are the typical method used to manage access. Thus, Enterprise Role Management, including the capability of analyzing and defining roles, is mandatory.

Access governance is one of the key IAM technology for any organization due to the massive impact of potential security risks arising from the lack of proper access governance controls. Access risks can have a severe operational impact and can be derived from organizational-wide security risks – the Barings Bank incident and the Société Générale scandal being prominent examples of such risks that could have been prevented with appropriate access governance in place. There are several other access-related security risks in today's organizations that have a direct impact on business, including but not limited to, intellectual property theft, occupational fraud in ERP systems including SOD conflicts and other policy violations, reputational damage due to the loss of customer information and privacy-related data, and many more. Thus, an adequate access governance framework is essential for organizations dealing with continually changing paradigms of security and risk management.

In this Executive View report, we look at Atos DirX Audit, which is a solution targeting specifically the field of Access Analytics and Intelligence, with other capabilities such as Enterprise Role Management and SoD controls being supported by Atos DirX Identity.

2 Product Description

In contrast to most other vendors, Atos has taken a somewhat different approach for segmenting overall IGA capabilities (Identity Governance & Administration, consisting of Identity Lifecycle Management, Provisioning, and Access Governance) into products. This is partially caused by the history of these products, with DirX Identity being available way ahead of DirX Audit, which had been added for additional capabilities around auditing of access and the related features around Access Intelligence and Analytics. However, we recently are observing a growing number of vendors that adds such capabilities as separate offerings, instead of fully integrating these into their established IGA solutions. Either way has its strengths and weaknesses. In sum, Atos is able to offer a comprehensive portfolio of IGA capabilities as part of the overall DirX product portfolio, that also serves the Access Management and Directory Service market segments.

The focus of DirX Audit, as for any other solution in that particular market segment, is on complementing existing IGA solutions and providing answers on questions that are commonly raised by auditors, and that must be provided for enforcing regulatory compliance. Additionally, the insight provided also can help organizations in streamlining access, e.g. by removing unused access, and in increasing their security and cyberattack resilience.

DirX Audit differs from many of today's solution in the area of Access Intelligence in the fact that it not only supports the analysis of static access entitlements, but also user behavior analytics, i.e. the analysis on which data has been accessed by which users in the past.

DirX Audit collects the information from other DirX modules, enriches the data e.g. with additional data on the users, and transforms the raw audit data into structured and actionable data. This provides information on

- Which applications have been used
- When resources have been accessed
- Who accessed the resources
- Which concrete operations have been performed or which data has been accessed

This then is correlated and additional information such as

- Who managed the user's access entitlements
- Who approved access

is provided. DirX Audit supports a broad range of capabilities, some of these – such as out-of-the-box key performance and key security indicators – being rather unique.

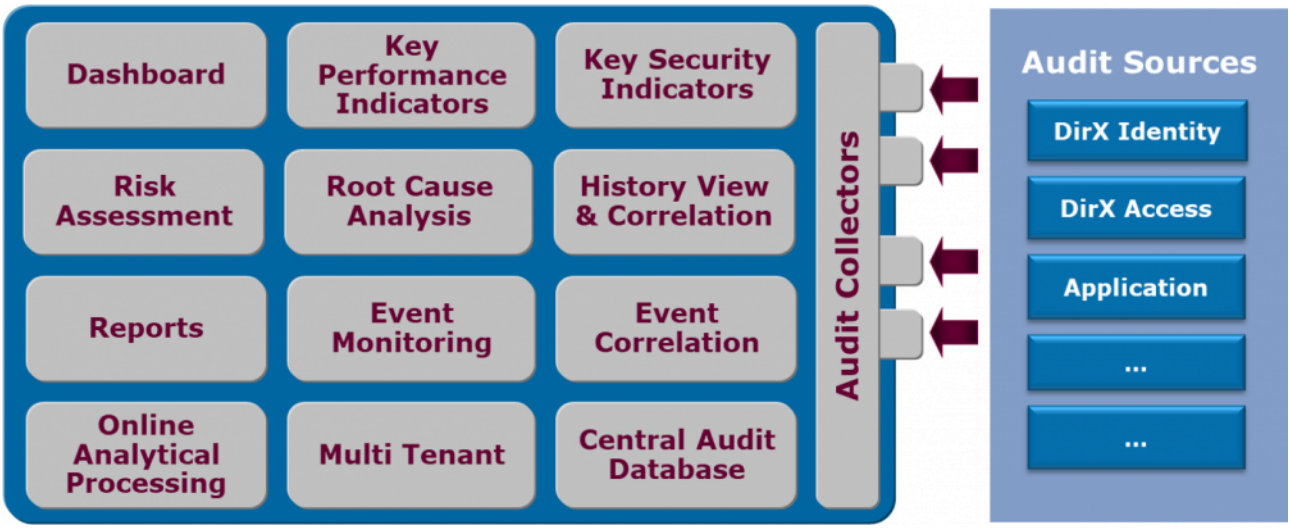

Figure 1: DirX Audit comes with a broad range of capabilities (Source: Atos).

Technically, the solution collects data from DirX Identity, DirX Access, and from applications and other sources through collectors. There are standard connectors for the DirX products, while data from applications is collected either via file transfer and imports, or via JMS (Java Message System), i.e. using an Enterprise Service Bus (ESB). The latter allows for continuous delivery of audit data from source systems. Data is then enriched and correlated, and processed in various ways. Integration of other sources will require a certain amount of configuration, for normalizing and correctly mapping the data. This includes historical data, KPIs (Key Performance Indicators); and reports. Data is stored in a database and can be accessed and managed via the DirX Audit Manager.

A key capability of such audit and analytical solutions is collecting historical data. That data is used for analytics, but e.g. also can be used to compare different states of access entitlements for forensic reasons and other activities. Historic data can be queried by name, data, and other attributes, and is displayed on a graphical timeline indicating various events within the time intervals. Reference links allow for drilling down into further details on such data. This e.g. enables auditors to understand the cause of assignment, by mapping audit events to the related access requests, approval and provisioning events.

Another functional area is the risk assessment and management. DirX Audit supports such assessments per users, building on a broad range of risk factors such as the number of active accounts, the applications a user has access to, non-mitigated SoD violations, and many more. These factors then are used to calculate a risk level and risk score, building on the standard deviation.

As other solutions in this market segment, DirX Audit also provides a dashboard for delivering rapid insight into the access risk status across all applications that provide data to the solution. This information is

represented in form of a series of graphics, which then again allow to drill down into the details, e.g. the events causing a certain risk. The dashboard provides a pragmatic perspective on the risk status, not shining with a great appeal in the representation of the data in form of specialized graphic formats with bubbles, meshes, or other formats.

As mentioned earlier, a specific strength is the KPI generator, that provides information about a range of KPIs, with many pre-configured KPIs being available for accounts, users, role assignments, password changes, certification status, and many more. These also can be customized, as well as the way they are displayed in the DirX Audit dashboard.

DirX Audit also comes with a feature that is titled Event Monitoring. Factually, this is not a permanent monitoring of events combined with alerting based on thresholds, but the ability for searching and filtering events to e.g. identify critical events or to perform forensic activities. Results can be put into reports.

Reporting anyway is a strong capability of DirX Audit, delivering more than 70 pre-configured reports and supporting a range of formats such as HTML, PDF, and Excel. There are various report templates per object type such as users, logins, access requests, or group memberships. Some of the reports are also related to specific regulations such as GDPR (General Data Protection Regulation). Reports can be created automatically based on a schedule, and sent to defined recipients such as the internal audit, administrators, or role owners.

Furthermore, access certification can be managed directly from DirX Audit, as well as the status of such campaigns can be tracked centrally.

3 Strengths and Challenges

Overall, DirX Audit is a very powerful solution that complements DirX Identity and DirX Access. It provides a broad set of capabilities for analyzing access entitlements, but also the concrete use of such entitlements. With the integration of this form of user behavior analytics, DirX Audit goes well-beyond what is found in many other Access Intelligence solutions, which rely only on the analysis of static access entitlements, but can't take further information into account.

DirX Audit also goes beyond several other offerings in the market by not only using data from other DirX products, but also being able to consume relevant events from other systems. Thus, access risk can be evaluated at various levels, down to the specific details within critical systems.

From a functionality perspective, the number of pre-configured reports is rated very positive, as well as the pre-defined KPIs and the ability for
customizing the dashboard. Even while other solutions shine more in the user interface, DirX Audit provides a pragmatic and efficient way for identifying access-related risks, including drill-down to the very detail behind such risks.

DirX Audit, from our perspective, is a must-have add-on for customers using DirX Identity and/or DirX Access, by providing the required insight into the concrete access risks and thus building the foundation not only for rapidly answering audit requests and meeting regulatory compliance requirements, but also for continuously optimizing access entitlements.

Strengths

- Mature solution for Access Intelligence and Analytics
- Large number of pre-configured reports, and flexible customization of reports
- Standard reports for certain regulations such as GDPR available
- Supports measurement of KPIs
- Integrates user behavior analytics, beyond just analyzing static entitlements
- Architecture built for large-scale environments
- Flexible importing capabilities, beyond just DirX products, allows for direct import from other source systems
- Strong professional services at global scale via Atos

Challenges

- Dashboard might benefit from broader variety of graphical representations
- No AI-/ML-based capabilities yet available, but on roadmap
- Does not support ongoing auditing, event monitoring, and alerting

4 Related Research

Executive View: Atos DirX Directory – 80421
Executive View: Atos DirX Identity – 80166
Executive View: Atos DirX Access - 80167
Leadership Brief: 10 Top Trends in IAM – 80355
Leadership Brief: Identity Fabrics – Connecting Anyone to Every Services – 80204
Leadership Brief: Access Reviews Done Right - 80195
Leadership Compass: Identity as a Service (IDaaS) IGA – 80051
Leadership Compass: Identity Governance & Administration – 71135
Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) – 71141

Content of Figures

Figure 1: DirX Audit comes with a broad range of capabilities (Source: Atos).

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.