



# **Tuebora Product and Company Overview:**

Driving the 'Third-Wave' of Identity and  
Access Management



***Tuebora***

## Overview

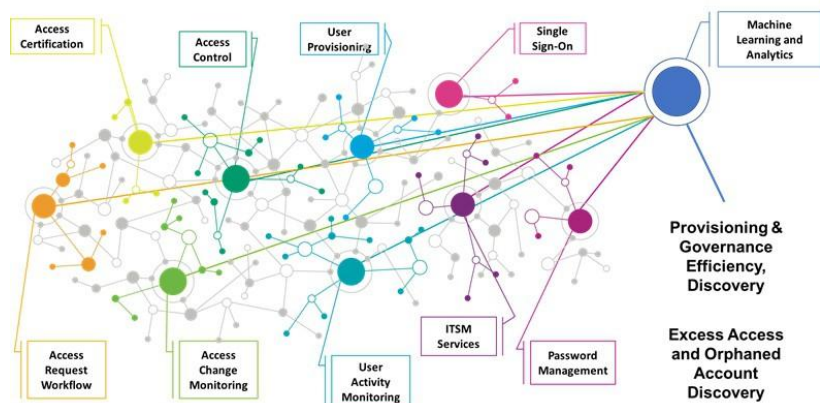
The need for a robust, holistic approach to Identity and Access Management (IAM) has never been greater. IAM activities and processes overlap with and cross over into security, HR, and other key business activities. Efficient joiner-leaver-mover processes enable business growth and reduce business risk. Yet, most IAM business processes are disjointed due to increasingly decentralized application management, hybrid cloud and on-premise applications, and static provisioning systems not built for dynamic business environments. The lack of a holistic view of access and identity across IAM and business applications impedes metrics-based decision making.

The result is an increasing number of “one-off” application access requests that increase the amount of time it takes employees to become productive. These same issues also cause businesses to face identity-based risks. Many surveys point out that the average amount of time it takes to terminate access to all applications once an employee leaves an organization can be months. This increases the risk of data theft by current or former employees.

Companies have matured their IAM activities and processes from manual (the first-wave of IAM) to some level of automation (the second-wave of IAM). Unfortunately, automation hasn’t kept pace with the velocity of joiner-mover-leaver change within the organization.

## The “Third-Wave” – The IAM Machine Learning Platform

As an organization changes, an IAM platform is needed to collect and perform continuous analysis of provisioning behavior, business application and system access by employees and third parties, and IAM point solution data. The application of machine learning produces two results. The first is continuous monitoring of five key IAM metrics—unused accounts,



unused access, data quality, provisioning “one-offs,” and certification “rubber-stamping.” The second result is a number of suggestions for more efficient access provisioning rules. This has the effect of creating continuous compliance by closing the gap between what access individuals should have versus what they actually have. Only with this visibility can an organization grant access or revoke access rights at the right time and within business context.

## A Natural Language User Interface for IAM

Edit Workflow - Inside Sales Representative Joiner Workflow

Name*	Description
Inside Sales Representative Joiner Workflow	Workflow for Provisioning Inside Sales Representative

Natural Language\*

1	on 'NewUser' Event
2	step one : create account in 'Azure Active Directory'
3	step two : grant membership in group 'Sales Team (Azure Active Directory)'
4	step three : grant license 'EXCHANGE_S_STANDARD (Office 365)'
5	step four : create account in 'SalesForce'
6	step five : send credentials to "user"
7	step six : notify supervisor

Cancel > Save Changes >

Tuebora has implemented a natural language user interface (NLUI) for its identity management platform using the Alexa SDK called Suno. The Tuebora implementation of NLUI accepts SMS, email, and voice inputs. This means your IAM processes can follow your business’s workflows—not the ones predefined by a vendor. You also have the flexibility to innovate IAM Joiner/Leaver/Mover and

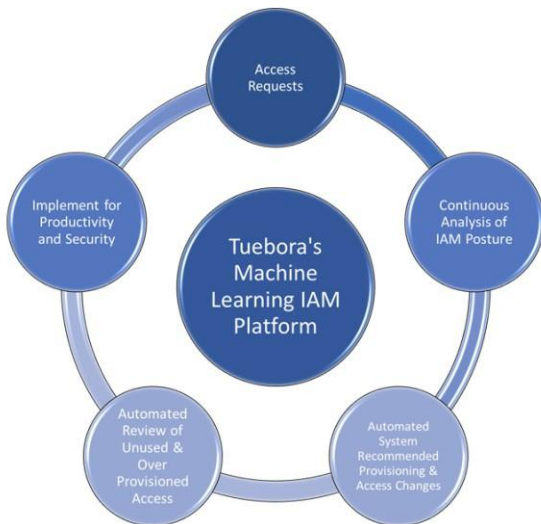
approval processes for speed, efficiency, and error reduction.

## The Tuebora IAM Product Suite

Tuebora's IAM Product Suite supports all IAM use cases: Single Sign-on, Password Management, Access Governance, Data Access Governance, integration with IT Service Management (ITSM). It also supports all steps needed for continuous IAM. Additionally, Tuebora provides tools for generating System for Cross-Domain Identity Management (SCIM) compliant connectors and Identity Discovery Assessment Tool (IDAT) at no charge.

## The Tuebora Micro Services Approach

It is time to say goodbye to monolithic architectures and IAM solutions built on them. A micro services approach affords a more gradual and less disruptive deployment approach. Organizations can start with one service and onboard other services over time, making deployment and DevOps for IAM become lot easier. Maintenance and is easier and supports costs are reduced, Organizations need not invest in a complete IAM solution with lot of hardware and infra, they can start small and expand. Lastly, interoperability with other IAM solutions is more easily enabled (see figure 1).



## Tuebora Machine Learning IAM Platform

Using a vast library of APIs, pre-built connectors, and SCIM Connector design tool Tuebora's IAM platform scales to collect data from hundreds of business applications and IAM infrastructure applications on-premise and in the Cloud. The platform uses algorithms to provide real-time analysis of the activities of provisioning teams and employees to suggest new provisioning rules that increase efficiency and find unused accounts and access. As a result, employee productivity is increased and business risk is reduced.

## Tuebora Governance

Tuebora's Governance Solution provides Identity Life cycle management (figure 2), access certification, access request, access control features and employs machine learning to monitor identity as well as access provisioning and usage behaviors to find provisioning efficiencies and security issues. This takes place while your team continues to work inside your current identity and access management processes. An appropriate analogy would be a car that performs continuous diagnostics, monitors your driving habits and environment, and alerts you to efficiencies that would help you get to your destination faster and in the most efficient manner, with the least amount of risk.

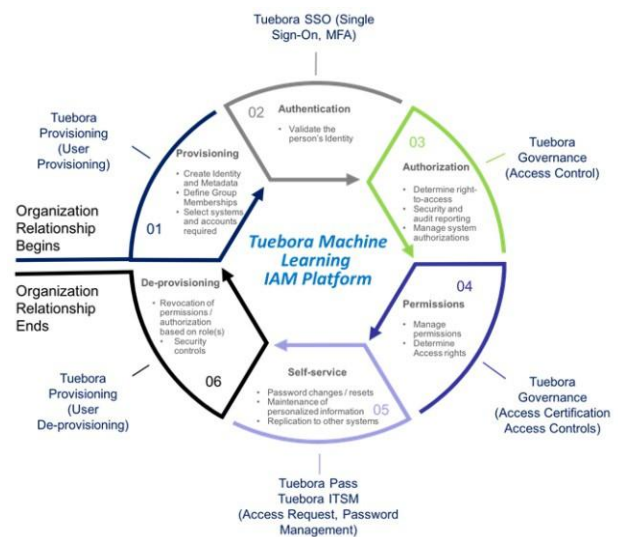


Figure 3 - Tuebora product portfolio mappings to IAM

## **Tuebora ITSM**

Tuebora ITSM enables enterprises to leverage their existing investments in ITSM tools and/or access request systems to manage the process of access request and still achieve desired level of automation efficiencies in access provisioning. Using Tuebora, ITSM customers can integrate multiple heterogeneous access request systems in use and get a consolidated view and also track all access requests and corresponding provisioning actions thereby providing tighter security and governance.

## **Tuebora Password Management**

Tuebora Pass provides superior return on investment by reducing costs related to password management through reduced helpdesk costs, increased security, and employee efficiency. Tuebora Pass supports Multiple Self-Service Channels, MFA, customized password policies, password synchronization, alerting, and reporting.

## **Tuebora Single Sign-on**

Tuebora SSO provides reliable, secure, and comprehensive single-sign-on (SSO) across on-premise and Cloud applications that are Web, “Thick-Client,” or native mobile applications. Tuebora SSO provides organizations with improved security and increased adoption in using the applications, thereby increasing ROI. Tuebora SSO supports thousands of out-of-box apps/assets, including 32+ social login providers.

## **Tuebora IDAT (free download)**

Tuebora’s free Identity and Access Discovery Tool (IDAT) helps you create a snapshot of identity and access for your organization. It automates analysis of business application access log data and Active Directory data to understand the intersection of access and assets. It then suggests changes to provisioning rules and displays excess and unused access. Having this visibility allows you to harmonize data across applications that use identity and more effectively track and audit access.

## **Tuebora SCIM**

Tuebora’s System for Cross-Domain Identity Management (SCIM) is a GUI-based stand-alone connector design tool that generates SCIM compliant connectors for non-SCIM applications. Tuebora SCIM standardizes integration and reduces time developing connectors, all without the need for SMEs.

# ***Tuebora***

### **About Tuebora**

Based in Santa Clara, CA, USA and Bangalore, India, Tuebora was founded by pioneers in access governance. Tuebora represents the “third-wave” of Identity and Access Management (IAM). With the application of machine learning and a complete suite of IAM products, Tuebora is a “self-driven”, agile, adaptive, and real-time IAM solution. Our customers experience increased employee productivity and lowered risk of identity-based attacks. Tuebora is backed by Citrix Systems and has been recognized by Gartner as a Cool Vendor.

✉ [sales@tuebora.com](mailto:sales@tuebora.com) | 📞 +1-844-708-4941 | 🌐 [www.tuebora.com](http://www.tuebora.com)