KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger

May 19, 2020

# Ilantus Compact Identity

IAM is a complex challenge for businesses, comprising of various capabilities such as IGA (Identity Governance & Administration), Access Management, and Privileged Access Management. Deployment is shifting towards flexible models supporting a range of deployment options, including IDaaS (Identity as a Service). Ilantus Compact Identity is an IAM offering targeting businesses that are looking for a comprehensive, integrated solution that can run either on premises or in the Cloud.

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

# Content

# 1 Introduction

IAM (Identity & Access Management) today is at the core of enterprise IT infrastructures when it comes to protecting digital corporate assets. IAM, as the name states, is about managing identities and their access. This involves managing user accounts and their entitlements across the variety of systems and applications in use in organizations.

Over the past several years, organizations have been facing multiple changes affecting their security posture. The perimeter which separated the internal network from the outer world does not have the same relevance it had before, with mobile users accessing internal systems, with integrating business partners and customers into business processes, and with the shift to cloud applications. On the other hand, the value and relevance of digital corporate assets and intellectual properties have increased. With the shift to connected things and to smart manufacturing, digital assets are becoming "crown jewels" even for more traditional businesses such as mechanical engineering.

Protecting digital assets, the systems, and applications in an IT environment of growing complexity and of a hybrid nature while facing ever-increasing attacks, involves several actions organizations must take. Protecting against internal and external attackers requires a well-thought-out understanding of risks and countermeasures.

Among the core elements of every infrastructure, we find IAM. IAM done right ensures that identities, their user accounts and passwords, and their access entitlements are well-managed. IAM thus reduces the attack surface by helping organizations moving towards the "least privilege" principle. IAM provides the tools to automate processes around managing users and access entitlements, but also for regularly reviewing these and identifying, e.g., excessive entitlements.

On the other hand, IAM also plays a vital role for business enablement, when it comes to the need of employees, contractors, business partners, and customers to access certain applications, systems, and data. IAM is the tool for implementing the workflows and automated processes for onboarding users and granting them access. Again, if done right, IAM can enable organizations by optimizing the onboarding and change processes, but also ensure that entitlements are revoked, and accounts are deleted or deactivated once they are no longer required.

Under the umbrella of IAM, we can differentiate between the "core IAM" or– as it is called frequently today – IGA (Identity Governance and Administration), and the broader definition of IAM which includes additional capabilities such as Privilege Management, Web Access Management, Identity Federation, and more. IGA, in fact, is an umbrella term for two of the core elements of IAM, which are Identity Provisioning and Access Governance. Identity Provisioning supports automating processes for creating and managing user accounts and their high-level

entitlements across the variety of systems and applications in use, while Access Governance adds the governance layer for analyzing entitlements, regular reviews and recertification, and also efficient access request workflows. However, other capabilities such as Access Management are of equal relevance.

Over the past few years, we have seen a convergence of traditional IAM deployments that run on premises towards IDaaS. IDaaS is one of the fastest growing market segments of IAM characterized by cloud-based delivery of traditional IAM services. The market, driven largely by web-centric use-cases in its early days, now offers full-fledged delivery of IAM capabilities irrespective of application delivery models. The IDaaS market has registered significant growth over the last few years primarily driven by the need of organizations to achieve better time-to-value proposition over on-premises IAM deployments. IDaaS solutions offer cloud-ready integrations to extend an organization's IAM controls to meet the security requirements of their growing SaaS portfolio.

The IDaaS market has evolved over the past few years and is still growing, both in size and in the number of vendors. However, under the umbrella term of IDaaS, we find a variety of offerings. IDaaS in general provides Identity & Access Management and Access Governance capabilities as a service, ranging from Single Sign-On to full Identity Provisioning and Access Governance for both on-premise and cloud solutions. These solutions also vary in their support for different groups of users - such as employees, business partners, and customers - their support for mobile users, and their integration capabilities back to on-premise environments.

In this executive view, we discuss the offering from Ilantus called Compact Identity which is delivered as an IDaaS service bundle targeted at IAM requirements of mid-market enterprises, but also can be deployed on premises. With the continuous expansion of capabilities, Compact Identity is one of the few offerings in the market serving all major IAM use cases, including IGA, Access Management, and PAM.

# 2 Product Description

Ilantus, which started as a system integrator, has moved fast to provide offerings targeted at different types of customers. Their solution Compact Identity focuses on delivering IGA and AM capabilities from a single codebase that can meet more complex requirements on IGA. Additionally, Ilantus has offerings that cover the IDaaS and Access Management requirements in the market. Compact Identity also delivers a complete PAM solution, and with an integrated Web Access Management capability covers all aspects on the IAM stack.

In 2014, Ilantus merged all of its product offerings into one single IDaaS platform. For cloud deployments, Ilantus provides an on-premise agent with connections to their cloud platform. Alternatively, they can deploy their cloud solution to customers on-premises data-centers and private clouds.

**Overview: Ilantus Compact Identity**

Ilantus's Compact Identity product features cover identity administration, access management through authentication, SSO, authorization, password management, and access governance, but also offers PAM, Basic CIAM, and Identity Risk Analytics capabilities as well.

The workflow capabilities are flexible and support a basic registration workflow as well as access request and approval workflows, with many additional workflows on the roadmap, although Compact Identity falls short in the case of access exception approvals as well as rights and registration delegation, features that are not often demanded in the mid-market, which is their focus. For Access Governance, Ilantus delivers standard Access Review support, including multi-level campaigns, but also additional Access Intelligence capabilities..

Ilantus continues to add innovative features now and on their roadmap, such as identity analytics that supports anomaly and other types of detections, as well as robotic process automation (RPA) capabilities integrated for SSO and user lifecycle management activities.

**Detailed capabilities**

Ilantus Compact Identity is primarily aimed at mid-market customers and offers a solution that covers a variety of aspects around IDaaS mostly preferred by SMB organizations to jump-start their IAM journey. Offered as a public cloud service with the option of on-premise deployment, Compact Identity addresses generic IAM requirements around Single Sign-On, password management, identity life-cycle management, access governance and privileged access management in one service bundle. Easy onboarding facilitates customers to subscribe the solution directly from the cloud and start using it without much efforts required from the integration and service delivery teams.

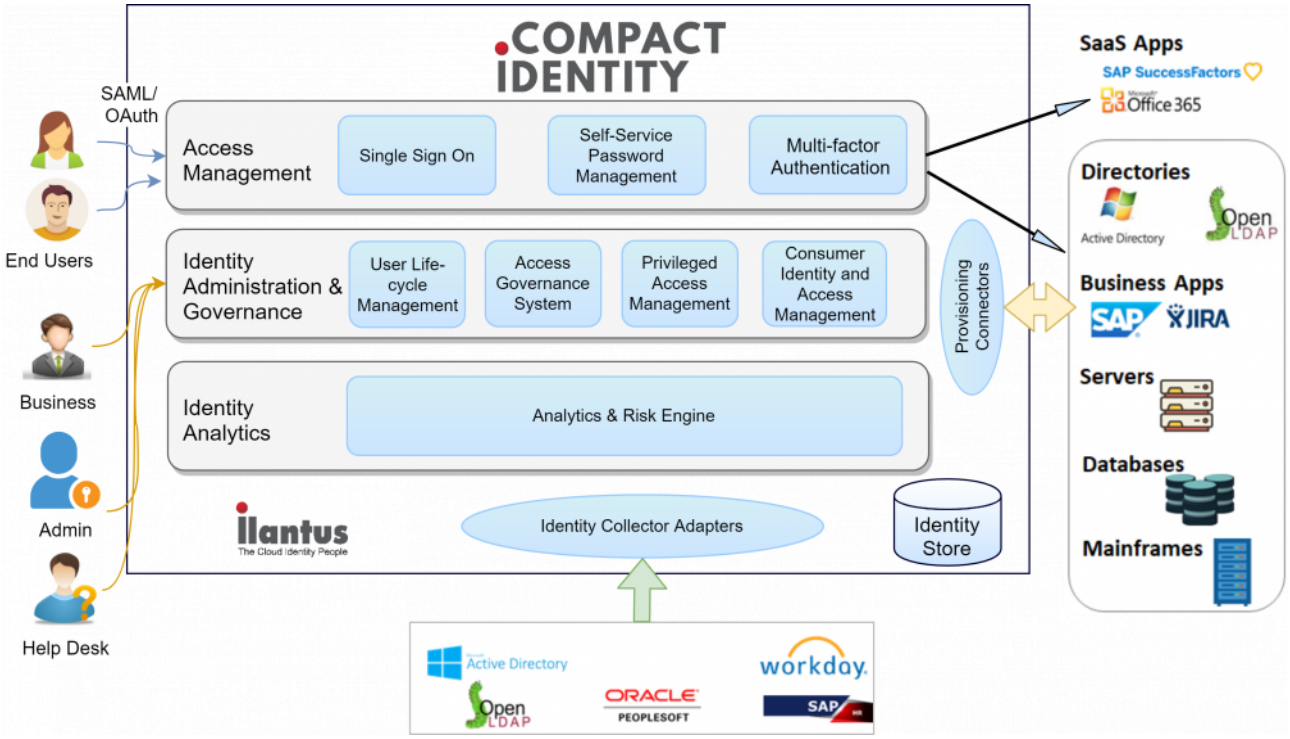


Figure 1: Ilantus Compact Identity Overview (Source: Ilantus)

The access management module offers multi-factor authentication (MFA) in addition to basic single sign-on (SSO) and password management capabilities. For MFA, Ilantus Compact Identity supports generic LDAP authentication with in-built soft OTP methods. Context based authentication can leverage generic contextual attributes to support the MFA process and Ilantus manages this with its internally developed adaptive authentication capabilities. Access policies utilize the baseline contexts such as geo-location and device information, but a broad support of contextual and risk analysis is not yet supported for authentication process. Ilantus Compact Identity, however, offers the flexibility of integration with several third-party authenticators including biometric authentication. Ilantus, having recently joined the FIDO Alliance, is adding FIDO compliant authentication to its MFA portfolio through technology partnerships.

In addition to standard web-based SSO, Ilantus Compact Identity brings the expertise of providing enterprise single sign-on (ESSO) to non-web-based applications including thick-client applications in use by several organizations. There is full support for Identity federation standards such as OpenID connect and OAuth 2.0.

Delivering support for a larger set of connectors to various target applications and systems, Ilantus Compact Identity comes with a "Do-It-Yourself" wizard to simplify integration and initial configuration for onboarding new applications.

Access management module also includes password management capabilities that range from self-service password resets and account recovery to password synchronization for non-AD integrated applications. Reverse password synchronization supports cases where the password change on one

of the target systems or applications is used to change the password of all accounts for the user in the same password sync group.

Ilantus Compact Identity offers good range of identity life-cycle management and access governance features. The identity life-cycle management offers an in-built identity store with native AD integration and ready integrations for HRMS and flat files (CSVs) for user onboarding and offboarding. Rule-based role assignments are supported as part of the identity onboarding process along with support for other identity life-cycle events. Built-in access request approval workflows deliver rule-based decision making based on pre-configured rules for identity lifecycle events such as account provisioning, role modification or account termination. Workflow support for advanced identity life-cycle management such as exceptional approvals, ad-hoc identity provisioning or segregation of duty (SoD) policy violations is not yet supported.

Ilantus Compact Identity provides a wide range of ready adapters for data collection across multiple identity repositories including Microsoft Active Directory, OpenLDAP and several HR management systems such as SAP, Workday, Ramco and Oracle HRMS, allowing for synchronization of identity attributes and access entitlements related to user accounts and groups across the identity repositories.

They also have improved their in-built access governance capabilities that are sufficient for most requirements. Ilantus Compact Identity delivers a consolidated view of access through available dashboards with detection and management of orphaned or dormant accounts. Access certification and review capabilities allow process and role owners to initiate on-demand or periodic access reviews to manage access attestations and facilitate access certification campaigns for a faster and accurate review of users' access across the organization.

Ilantus Compact Identity offers basic identity intelligence and analytics through several in-built reports that can be customized and scheduled as per business requirements. With modern dashboarding, Ilantus Compact Identity allows for widget-based customization of dashboard to show user activity and operations summary such as daily, weekly and monthly usage of SSO per application, dormant accounts across applications, operations performed on user identities as well as access requests' review pattern and status. The widgets enable easy customization of dashboard based on users' requirements. Advanced identity and access intelligence features to support risk-based analytics or segregation of duty (SoD) analysis are, however, not yet supported.

Beyond these capabilities in both Access Management and IGA, Ilantus Compact Identity delivers on PAM (Privileged Access Management) and several other feature areas. These extended capabilities include

- PAM including session monitoring and recording, and access request & approval workflows for privileged access; these capabilities provide a good PAM support

- Enterprise Mobility Management (EMM) for managing devices and their registration
- API Management and security capabilities based on OAuth
- IoT Management baseline features for managing IoT devices and login to these devices
- Baseline Endpoint Management features

Ilantus Compact Identity is targeted at customers with a need for IAM capabilities across the full IAM spectrum. The deployment is flexible and can be customized based on pre-packaged integrations, required workflow templates and specific use cases. Deployed in public cloud (Azure or AWS cloud), Ilantus Compact Identity offers the flexibility to be deployed in private cloud, on-premises or a hybrid environment depending on the customer's deployment preferences. As an easy to onboard and use solution, Ilantus Compact Identity makes an ideal choice of IDaaS for mid-market organizations that are looking to start their IAM journey without significant effort and investment, favoring a lean IAM operating model and comprehensive capabilities.

# 3 Strengths and Challenges

Ilantus Compact Identity differs from most of the other offerings in the IAM market in both the flexible deployment options, and the breadth of supported capabilities. It comes as a full IAM package, covering IGA, Access Management, PAM, and other capabilities that businesses require. While some of the capabilities are more at the baseline level, for both IGA and Access Management comprehensive capabilities are supported that will be sufficient for most businesses.

Ilantus continues to add innovative features now and on their roadmap, such as Identity Analytics that supports anomaly and other types of detections, as well as Robotic Process Automation (RPA) capabilities integrated for SSO and user lifecycle management activities.

Ilantus Compact Identity is an interesting alternative to the established offerings in the IAM market, specifically for mid-market companies and SMBs looking for an integrated offering servicing all major areas of IAM. However, even large businesses, in particular outside of the very heavily regulated industries, might benefit from the integrated approach and the flexible deployment options.

## Strengths

- Service bundle tailored to meet the mid-market IDaaS requirements
- Good OOB support for enterprise-level cloud applications in addition to common on-premises systems
- Flexibility for customization including policy and workflow customizations
- Strong support for ESSO, particularly non-web and thick-client applications
- Good support for in-built MFA with basic contextual attributes
- Modern widget-based dashboarding
- Increased focus of enhancing user and administrative experience
- Designed to deliver quick application on-boarding and support lean IAM operations
- Innovative list of capabilities on roadmap

## Challenges

- A still somewhat small but quickly growing partner ecosystem
- Customer presence is still primarily focused on US and a few Asian countries, still low in EMEA
- Missing out-of-the-box reporting for major compliance frameworks
- Access Governance capabilities are good but not exceptional, specifically with respect to SoD management

# 4 Related Research

Executive View: Ilantus IDaaS Next – 70252
Executive View: Ilantus Compact Identity – 80052
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

# 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.