KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | April 2019

ManageEngine AD360

ManageEngine AD360 is a tool targeted at the in-depth management of Microsoft Active Directory and connected systems such as Microsoft Office 365. It comes with capabilities that go beyond pure entitlement, by adding authentication features, UBA (User Behavior Analytics), and even Single Sign-On to several cloud services. However, the core of the product is supporting an efficient, automated management of Microsoft Active Directory and mitigating risks in these environments by automation and optimization of entitlements.

by **Martin Kuppinger**
mk@kuppingercole.com
April 2019

Content

Related Research

Architecture Blueprint: Access Governance and Privilege Management - 79045

Executive View: ManageEngine Password Manager Pro - 70613

Leadership Compass: Privileged Access Management - 79014

1 Introduction

Digital identity is a critical business-enabling technology for Small to Mid-Size Businesses (SMBs). However, as is borne out by cybercrime reports year-after-year, digital identity is also a primary vector through which SMBs are attacked. Many SMBs lack a fully staffed IT department to handle the complexities of deploying, maintaining, and securing complex IAM solutions. This is a factor fueling the need for targeted solutions that support these businesses in managing their environments.

The risks of not having well-maintained and secure IAM solutions within SMBs can be great, ranging from lower productivity associated with password resets and incorrect entitlements; loss of data such as employee and customer PII; loss of trade secrets and other valuable business information; diminished revenue from reputation damage and fraud; to unwittingly becoming a vector of attack to other members in a supply chain. Many managers and owners within SMBs naively assume that they are too small to be attacked by malicious actors, but **cybercrime studies** show that SMBs are increasingly targeted because of the perception that they are less secure than larger organizations.

SMBs can have a variety of use cases and technical requirements they need to meet with IAM. Regarding use cases, everyone needs B2E IAM, many need B2B, and some need B2C. Consider B2E, where most will have Microsoft Active Directory in place. Many organizations also utilize various cloud-based SaaS applications but do not have the IAM functions centralized or even under control. They are often lacking productivity-enhancing Single Sign-On (SSO) capabilities.

Beyond the focus on SMBs, getting a grip on the environments such as Microsoft Active Directory requires capabilities beyond what enterprise-grade IGA (Identity Governance and Administration) tools commonly deliver. The in-depth management of Active directory and related environments demands specific capabilities, such as the in-depth management e.g. of SAP environment also does. Thus, there is a place for such solutions in combination with full-blown IGA tools.

A sometimes-overlooked capability is that IAM systems can aid in regulatory compliance. Under the General Data Protection Regulation (GDPR) in the EU, collecting clear and unambiguous consent from consumers for the use of their data is necessary for compliance. Well-designed IAM solutions can enforce and help demonstrate compliance with regulations that require segregation of duties, i.e. SOx in the US.

There are three major categories of functions within IAM to look at, particularly from the perspective of SMBs:

Identity Administration: The ability to administer identity lifecycle events including provisioning/de-provisioning of user accounts, maintaining identity repositories, managing access entitlements, and synchronization of user attributes. A self-service user interface allows for requesting access, profile management, password reset, and synchronization. Configurable cloud-native connectors offer automated user provisioning to both on-premises as well as SaaS applications. Other common identity administration capabilities include administrative web interface, batch import interface, delegated administration, SPML, and SCIM support.

Access Management: This category includes authentication, authorization, single sign-on and identity federation for both on-premises and SaaS applications delivered as a cloud service. The underlying support for industry standards such as SAML, OAuth, and OpenID Connect can vary.

Access Governance: This group of capabilities that are frequently absent from the portfolio of entry-level IAM tools centered around AD, given that most SMBs only look for an easy-to-use, administrator-centric approach on maintaining Access Governance and enforcing least privilege principles.

ManageEngine, a part of Zoho Corporation, offers a comprehensive tool for managing identities and access in the environments that are common for SMBs, centered around Microsoft Active Directory. Their AD360 offering delivers a broad range of capabilities for in-depth IAM.

2 Product Description

ManageEngine AD360 is a solution that delivers comprehensive IAM capabilities centered around the Microsoft Active Directory. It is targeted at environments that have Active Directory (AD) at the core, as the name implies. The focus is not (yet) on delivering a full-blown IGA (Identity Governance & Administration) tool that connects to every system in a complex IT environment but to automate administration and increase security in AD-centric environments. However, AD360 can integrate with additional targets including IGA systems based on pre-defined integration points, and ManageEngine intends to grow the number and range of out-of-the-box connectors.

User Lifecycle Management & Automation

At the center of AD360 are the functions for managing users and their accounts in an automated way, across the entire lifecycle of such accounts. The focus is on accounts in AD itself plus the directly related systems such as Microsoft Office 365, Microsoft Exchange Server, and Lync. Furthermore, AD360 comes with built-in support for the Google G Suite. In contrast to full-blown IGA solutions, there is no out-of-the-box integration to further target systems such as SAP, mainframes, etc., but – as mentioned – integration points are provided.

On the other hand, AD360 delivers more in-depth integration with the supported target environments, by e.g. supporting the creation of Microsoft Exchange mailboxes and automating other types of typical tasks in these environments. Thus, it also can serve as an extension to standard IGA tools by delivering the in-depth management of AD and some of the connected systems. In the latter case, it becomes a solution also for larger organizations.

The focus of the capabilities of AD360 is on managing the entire lifecycle of accounts with uniform accounts across all users, avoiding duplicates, and getting rid of inactive accounts, but also preventing accidental deletion. New users can be added either manually or by file imports from source systems such as HR. AD360 then provides the capability for automating the subsequent steps, based on a UI that e.g. allows configuration and scheduling of imports and policy-based assignment to AD groups. AD360 is flexible in creating custom logics for instant and successive tasks, all supported via the UI. That e.g. allows for creating efficient and solid processes for removing inactive accounts, based on adequate logic and a staging between deactivation (immediate task) and deletion (subsequent steps).

Entitlement Management

As mentioned above, when creating (or changing) users, AD360 can manage assignments to AD group based on policies, that use various attributes such as title or department for automated assignment of users to specific AD groups. This capability of rule-based (or policy-based) group membership management builds the foundation for managing AD entitlements.

ManageEngine uses the term of Privileged Access Management (PAM) for additional capabilities supported in that space. That might be slightly misleading in the sense of that ManageEngine also delivers a separate PAM solution, and with respect to the fact that many of these features are relevant to all types of user accounts.

Here, AD360 supports a range of capabilities:

- Management of group memberships, both manually and via policies
- Analysis and optimization of group structures specifically nested group
- Clean-up of permissions and enforcement of least privilege principles, by analyzing elevations for critical objects and for individual users
- Isolation of administrative accounts, for specifically restricting access to critical capabilities on domain controllers and file servers, but also segregating e.g. external accounts such as vendors and contractors
- Monitoring of sensitive accounts

Compared to the standard AD tools, AD360 significantly simplifies and automates the management of users in AD, plus the connected systems.

Delegation & Role Management

Beyond the direct assignment of entitlements, AD360 adds further capabilities in three areas:

- Managing administrative tasks through roles
- Tracking changes in AD
- Approval workflows for changes in AD

Administrative Tasks for AD, Windows Servers, and Office 365 can be managed through a console which allows mapping tasks to roles. This builds the foundation for moving from the highly problematic use of built-in administrator accounts or other accounts with full privileges to limited operator roles.

Change tracking factually is a part of the logging, monitoring, and auditing capabilities but is essential when it comes to supervising activities of administrators and operators.

Workflows finally help in managing access beyond the IT team. AD tasks can result in tickets that are used in multi-stage workflows. This also allows for creating user request portals for various types of users, approvals of entitlement requests by the responsible managers, or approvals for controlled access to file shares.

Logging & Monitoring

AD360 comes with a strong set of auditing features, even while it – in contrast to some other solutions – isn't focused on the interactive, real-time analysis of current entitlements within AD to the depth of the single ACL, but on reporting about entitlement structures and potential challenges therein. The focus is

on optimizing administrative processes and identifying critical entitlements, orphaned accounts, and fraudulent user behavior.

Part of this are the User Behavior Analytics (UBA) capabilities that are now introduced to AD360. Based on that, the behavior of users can be monitored, and outliers can be identified easily. The technology is based on ML (Machine Learning) algorithms.

Beyond that, AD360 also supports standard auditing and reporting capabilities.

Authentication

Finally, AD360 also supports authentication in a way that goes beyond what commonly is found in that category of products. Capabilities in that area include

- Management of password policies and password self-service
- Custom authentication methods for sensitive and privileged accounts
- Integration with Windows MFA/2FA (Multi Factor/Two Factor Authentication)
- SSO (Single Sign-On) to cloud services

Adaptive Authentication, supporting risk- and context-based authentication, e.g. by step-up authentication, is a roadmap item and planned for upcoming releases.

In the area of single sign-on, a range of enterprise applications such as Salesforce, Office 365 or Dropbox are supported out-of-the-box. Based on the SAML support, SSO to other services such as enterprise applications with SAML capabilities is supported as well. Beyond that, AD360 also supports password synchronization e.g. with AD LDS and other systems such as Salesforce.

3 Strengths and Challenges

In sum, AD360 is a feature-rich tool for managing users and their accounts in Microsoft AD and some connected systems. While AD360 is not a full-featured IGA solution, it provides strong capabilities for managing AD, Office 365, and related environments, plus it can serve as an integrated solution with enterprise-level IGA tools. In the latter use case, AD360 delivers the in-depth capabilities required for managing Microsoft Active Directory, as e.g. SAP Access Control does for SAP environments.

With its breadth of features, ManageEngine AD360 is a good solution for SMBs who's IT is centered around Microsoft Active Directory. With the workflow capabilities and the support for SSO to cloud services, it also extends the reach to additional platforms that are increasingly used in these types of businesses.

While the UBA capabilities are still in the early stages, ManageEngine demonstrates their focus on adding essential features for supporting businesses in mitigating risks that frequently derive from suboptimal administration of AD environments.

Within the key capabilities, there might be some more support for a detailed analysis of entitlements in AD environments and some more flexibility in easily connecting additional systems, specifically for SMBs. However, AD360 is definitely a very strong solution for the use cases the tool had been built for.

Strengths	Challenges
• Purpose-built for optimizing administration of Microsoft Active Directory • Strong workflow capabilities, beyond what commonly is found in that type of products • Role-based assignment of administrative tasks • Baseline UBA capabilities built into the product for identification of fraudulent use • Out-of-the-box integration to Office 365 and some other target systems • Well-though-out and easy-to use user interface • Policy-based management of entitlements with a substantial degree of flexibility	• No full-featured IGA solution, but targeted at Microsoft Active Directory environments and delivering integration points to other IGA products and target systems • Good auditing and analysis capabilities, but limited interactive analytics of complex entitlement structures • Limited connectivity to target systems

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company, 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 in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

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

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com