KuppingerCole Report

WHITEPAPER

by Martin Kuppinger April 2020

Single Sign-On and Managed Access to all Applications from the Cloud

With more and more organizations following a “cloud first” strategy, IT infrastructure and security services also must shift to the cloud, where increasingly more of the critical workloads reside. However, the IT of most organizations will remain hybrid for long. Thus, there is a need of comprehensive authentication and single sign-on services, supporting all applications such as SaaS apps, on premises applications, and custom-built applications, delivering a seamless user experience for accessing these. Microsoft Azure Active Directory (Azure AD) provides a strong foundation for delivering such services, with deep integration to cloud apps while supporting legacy applications and services.

by **Martin Kuppinger**
mk@kuppingercole.com
April 2020

Commissioned by Microsoft

Content

Table of Figures

Related Research

Leadership Compass: Identity as a Service (IDaaS) IGA – 80051
Leadership Compass: Identity as a Service (IDaaS) AM - 79016
Advisory Note: Extending your Active Directory to the Cloud – 71108
Leadership Brief: 10 Top Trends in IAM – 80335
Leadership Brief: Identity Fabrics – Connecting Anyone to Every Service – 80204
Executive View: Microsoft Azure Active Directory – 79077
Executive View: Microsoft Azure Information Protection - 72540

1 Introduction

Many if not most organizations today are following a “cloud first” strategy, with lifting & shifting existing applications to the cloud, and with preferring new application procurement and deployment in as-a-service models. While cloud services are easy to deploy and commonly come with modern user experience, this shift also introduces new challenges to both the users and to IT and security management.

One of these challenges is that, while shifting to the cloud, the reality of most businesses will remain hybrid for many years, if not forever. Even if data centers are closed and workloads are moved to managed service providers running what then is called a “private cloud”, it is still about running legacy IT in a closed-down, private environment, alongside all the new SaaS services deployed from the public, multi-tenant cloud.

From both the user experience and the IT perspective, this factually means that challenges double. Users must access applications both on premises and in the cloud, and IT must manage and protect applications in both worlds. Altogether with the shift to new work experiences such as “work from home”, there is a need for providing a consistent user experience and management of hybrid IT environments. Solutions must reflect the hybrid reality of businesses and their IT.

Within these challenges, providing seamless access and integration with the wide range of solutions running on premises is by far the biggest challenge. However, integration with major SaaS services must also be solved, including the specifics some of the major environments such as Salesforce, SAP S/4HANA, AWS, Workday or ServiceNow have. Providing single sign-on to modern SaaS services is the simple part of the journey to the cloud – the challenge is supporting all services, i.e. the full range of services within the hybrid IT reality of today’s businesses.

Microsoft Azure Active Directory is an obvious solution for many organizations when selecting their solution for authentication and single sign-on to services, and as a central element within their future Identity Fabric, a logical architecture for delivering a consistent set of Identity Services, across all types of applications and users. Most businesses have an Active Directory in place in their on premises infrastructure, and a very significant number of organizations has opted for Microsoft Office 365, which relies on Microsoft Azure Active Directory (Azure AD).

In sum, Microsoft comes with a comprehensive, leading-edge approach for providing access to all types of applications, such as SaaS apps, on premises apps, and custom-built applications, to users, based on Microsoft Azure AD. For organizations, this provides a strong offering for a migration away from on premises Active Directory to Azure AD as the future cornerstone of user authentication and access services, and their future Identity Fabric.

With the shift of IT to the cloud in consequence of “cloud first” strategies, it is time for businesses to reconsider their approach on IAM in general, and to shift to a modern, central cloud service. With the shift of businesses to the cloud, IT infrastructure and security services also must shift to the cloud, while further supporting the hybrid IT reality of businesses.

2 Highlights

- The impact of “cloud first” strategies and a shift to SaaS on IT infrastructure services, specifically IAM and security
- The user challenge: Consistent user experience and single sign-on across all services, regardless of where these services run
- Application integration into on premises services and legacy and custom applications access require a variety of technical integrations
- Adaptive authentication as key technology for providing secure and seamless access for everyone to every service from anywhere
- Additional requirements, beyond single sign-on: The need for federated provisioning of identities, device management, and more
- Defining the future Identity Fabric serving the hybrid IT reality of businesses
- Azure Active Directory and its secure app access support as a cornerstone of future IAM
- Considerations for moving from on premises Active Directory to the cloud, building on Azure Active Directory
- Recommendations for an action plan for migrating to a modern IAM and application access strategy

3 The Need for Unified Application Access and Single Sign-On

The IT of most organizations will remain hybrid. However, with adding SaaS services, there is an emerging need for unified application access and single sign-on to all types of applications. This is best based on cloud services, with IT infrastructure following the shift of critical business services to the cloud.

Many if not most organizations today are following a “cloud first” strategy, with lifting & shifting existing applications to the cloud, and with preferring new application procurement and deployment in as-a-service models. While cloud services are easy to deploy and commonly come with modern user experience, this shift also introduces new challenges to both the users and to IT and security management.

First, the shift to the cloud is not a “big bang” transition where all services are moved to the cloud at one point-in-time. It is a gradual transition that frequently will take years, and for some businesses it never might be a complete transition. IT in manufacturing environments will remain on premises, and some applications are hard if not impossible to shift. There is some inertia in IT and business organizations that makes it hard to replace existing applications. Just remember how many applications from the 1970’s still had been in use in the year 2000, leading to the Y2K challenge back then.

In other words: The reality is most businesses will remain hybrid for many years, with legacy IT shifting only slowly to modern IT environments. Even if data centers are closed and workloads are moved to managed service providers running what then is called a “private cloud”, it is still about running legacy IT

in a closed-down, private environment, alongside all the new SaaS services deployed from the public, multi-tenant cloud.

From both the user experience and the IT perspective, this factually means that challenges double. Users must access applications both on premises and in the cloud, and IT must manage and protect applications in both worlds. Altogether with the shift to new work experiences such as "work from home", there is a need for providing a consistent user experience and management of hybrid IT environments while improving security in an age of ever-increasing cyberattacks.

The IT of most businesses will remain hybrid for long. There is a need for delivering a consistent user experience and management for the hybrid IT.

From a user experience perspective, there are three challenges to solve:

1. **Simple app discovery**: The first challenge is about discovering the applications to access. How do users find the apps they need to use, regardless of where these run? Portals linking to all services provide a solution.
2. **Frictionless access**: Most businesses have provided some level of single sign-on experience to their users in their traditional IT environments. Adding SaaS services means that there are more applications to sign-in. There is a need for a single sign-on experience across all services.
3. **Consistent user experience**: With a shift to more granular SaaS services for particular use cases, apps will provide very different user experience. While services might be cheap to procure, this might hinder user acceptance.

While the third challenge is hard to fix by IT administration, the first two challenges can be solved in a straightforward manner. Theoretically, such solutions can be based on existing technology on premises. Traditional Enterprise Single Sign-On solutions also can support web-based applications and thus SaaS services. On premises Active Directory can extend to SaaS services using ADFS (Active Directory Federation Services). There are several other solutions which can help in providing centralized application access and single sign-on, building on technology running on premises.

However, when talking about cloud first strategies, administrative services such as an end-user application portal, single sign-on services, IAM (Identity and Access Management), and security services consequently should also become cloud services. There is no value in investing into on premise services for these areas, when "cloud first" is the strategic paradigm.

Factually, many businesses already have reached the tipping point where more critical business capabilities are deployed from the cloud than on premises. With that convergence, securing workloads – including user access to these workloads – from the cloud is a logical shift.

With applications shifting to the cloud in a cloud first strategy, administrative services also should converge to cloud services.

There is a need for managing user access and security of all services from the cloud, regardless of where these services run. Solutions must reflect the hybrid reality of businesses and their IT. There is a need for delivering unified application access and single sign-on to all services, regardless of where they run.

4 The Hybrid Reality of Businesses: Supporting Legacy from the Cloud

Single sign-on to SaaS services is not sufficient – there are more challenges to solve, such as the integration with legacy IT applications, and federated provisioning of user accounts to SaaS services. Solutions thus must support a wide range of integrations to a variety of 3rd party applications.

Within such approach, there are five challenges, of which only two are easy to address, while the other two differentiate solutions for providing IAM and SSO for the hybrid IT:

1. Application discovery and access: There is a need for delivering a central portal that provides access to all applications, regardless of where they run. Providing such portal is simple; however, application integration – see below #4 – might become complex.
2. Single sign-on to SaaS services: This is straightforward at least for SaaS services supporting modern Identity Federation standards such as OAuth 2 and SAMLv2. For other SaaS services, SSO still might require approaches such as forms- or password-based authentication.
3. Federated Provisioning: Unfortunately, signing-on is just the last step in integrating SaaS applications. Beforehand, there must be user accounts in these services. Provisioning to SaaS services is the more complex challenge, despite SCIM (System for Cross-domain Identity Management) as a standard with increasing practical relevance.
4. Single sign-on to on premises applications: This is far more complex than integrating with SaaS services, due to the wide range of application and security architectures of such services. However, for providing a consistent experience and supporting a gradual transition of businesses to the cloud, such integration is essential and a key criterion for selecting the IAM solution.
5. Migrating IAM: Major parts of the IAM infrastructure must be migrated from on premises to the cloud.

Within these challenges, providing seamless access and integration with the wide range of solutions running on premises is by far the biggest challenge. However, integration with major SaaS services must also be solved, including the specifics some of the major environments such as Salesforce, SAP S/4HANA, Workday, ServiceNow or AWS have.

The major challenge in migrating IAM for a cloud first IT is supporting the wide range of on premises applications, providing a seamless user experience.

The challenge in integrating on premises applications is that these have evolved over a long time, with a range of application types and deployments. There are e.g. web applications supporting modern Identity Federation standards and such which don't provide support for SAMLv2 or OAuth2. There are applications delivering access via web APIs, and there are applications hosted behind a Remote Desktop Gateway. Other applications come with out-of-the-box integration into Active Directory.

Similarly, the range of authentication approaches and protocols is broad. There is Kerberos, which is used for Active Directory-integrated solutions and some others. There is header-based authentication as a mechanism for integrating with traditional web applications, where authentication information is provided as part of the HTTP header. This approach is also referred to as HTTP header injection. There is forms- and password-based authentication, where credentials are entered into forms. For single sign-on, credentials are provided by a service in the background, transparent to the user. And there is Identity Federation, with protocols such as

- OAuth 2
- SAMLv2
- WS-Federation

Delivering a seamless experience across the broad range of solutions that potentially run on premises might appear as a daunting task, but there are solutions available.

With such migration, some additional aspects need to be considered:

- The SSO service must be secure by itself. Authentication to the application portal must be secure, and additional security services such as risk- and context-based authentication are a must.
- From a security perspective, access to the on premises infrastructure (or the private cloud for lift & shift of legacy applications) should always be outbound, i.e. initiated from the internal network, without opening firewall ports to the DMZ.
- The role of on premises Active Directory, which is still used as a primary authentication service, will change. When transitioning the authentication and single sign-on services to the cloud, there must be another central service taking the role Active Directory traditionally has in the majority of organizations.

Providing single sign-on to modern SaaS services is the simple part of the journey to the cloud – the challenge is supporting all services, i.e. the full range of services within the hybrid IT reality of today's businesses.

5 Beyond Single Sign-On: Provisioning, Identity Management, Security

Adaptive Authentication, federated provisioning, and additional security services are required for comprehensive solutions. The Identity Fabric paradigm provides an approach for a unified, future-proof IAM.

As mentioned above, Single Sign-On is not the only challenge to be solved when converting to a cloud-based solution for providing access to all services in hybrid IT.

Such services must support Adaptive Authentication. Adaptive Authentication has two aspects:

1. Adaptiveness regarding the authenticators: Solutions should support a broad range of authentication means and form factors, well-beyond username and password. These authenticators such as the Microsoft Authenticator app, out-of-band SMS, hardware OTP tokens, and others, must be flexible to combine and exchange.
2. Adaptiveness regarding the authentication strength: Depending on the context and the risk of the interaction or transaction, the required level of authentication might vary. Access from a managed

device operating in a secure environment bears a different risk then accessing from a BYOD (Bring Your Own Device) device, out of a public WLAN. If the context changes, the risk changes, and authentication might need to adapt, e.g. requesting a second factor for authentication.

Beyond authentication, platforms supporting the application integration across the whole range of legacy and modern services must support IAM capabilities such as provisioning user accounts to services. While this frequently is well-solved for the legacy IT, provisioning to SaaS services still is a challenge. The aforementioned SCIM standard supports federated provisioning and also in just-in-time provisioning during the first time a user accesses an application.

Furthermore, aside from authentication which is helping in achieving the required level of security, there are further security challenges to consider, such as focusing on outbound access without opening the doors to attackers (e.g., as mentioned above, by opening up firewall ports to the DMZ (Demilitarized Zone) and the internal network). The cloud platform itself must be secure, and it must provide secure integration into the on premises IT environment.

Another aspect to consider is device management. The minimum is support for device fingerprinting, i.e. having a unique identifier for devices. Device fingerprinting helps in simplifying authentication, by lowering the requirements for trusted devices that are identified by their "fingerprint". However, having more advanced capabilities in integrated device management for mobile and traditional devices further increases the level of security.

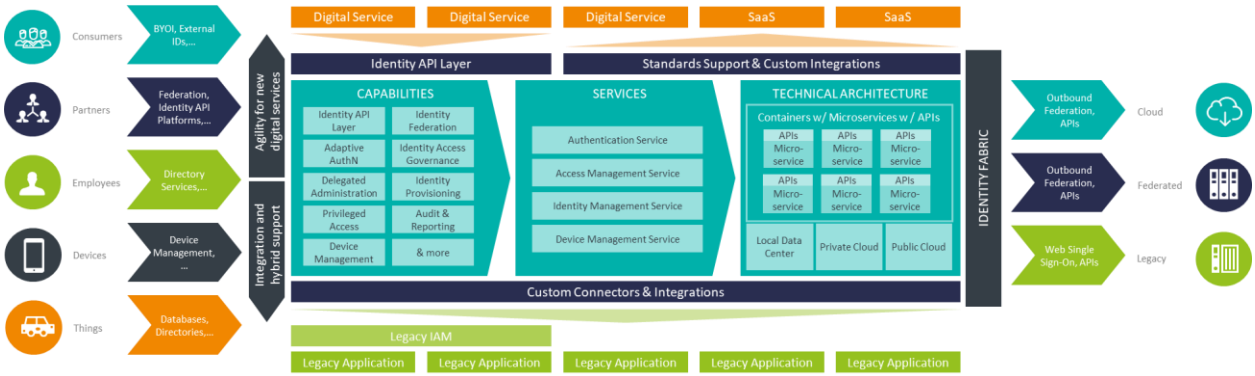

Figure 1: Identity Fabrics are a paradigm for a modern, holistic approach on IAM serving both traditional and cloud services, and integrating all required capabilities into a unified architecture (Source: KuppingerCole).

All this requires a strategic approach for modernizing IAM, well-beyond just providing a solution for single sign-on. KuppingerCole has described this paradigm as Identity Fabric, for a unified set of capabilities and services, running in a modern architecture. These services provide the capabilities required for granting controlled access for everyone to every service, regardless of who provides the service and where it runs. It enables integration to modern SaaS services as well as legacy applications.

When moving to a cloud first strategy, there is a need for a new, unified approach on IAM, providing access for all users to all services.

Migrating to such paradigm includes a stepwise migration of the existing IT infrastructure, with shifting roles of various services. This e.g. includes a strategic shift that puts a cloud service at the center, instead of the on premises Active Directory. For many businesses, Azure Active Directory will be the

logical choice as such central element, due to its tight integration with Microsoft Office 365 and other services. Notably, Azure Active Directory provides a far broader set of services than on premises Active Directory, including supporting single sign-on to hybrid applications. Regardless of which solutions finally are chosen: There is a need for defining a new strategic approach for IAM with all its services such as authentication and single sign-on for providing seamless and secure access to all IT services.

This shift is part of a Zero Trust approach, which has become the strategic IT security paradigm for many services. Zero Trust implies a concept where clients can access services from everywhere, not relying on internal networks anymore. Factually, moving to cloud-based IAM, authentication, and single sign-on services and the Identity Fabric paradigm is a major and essential step within a Zero Trust strategy.

6 Microsoft Azure Active Directory: Managing & Securing Access to all Apps

Microsoft Azure Active Directory delivers a range of integration options to virtually all types of applications, both SaaS services, legacy and on premises apps. Additional Microsoft services complement Azure Active Directory e.g. with add-on security services. Companies should consider moving from Active Directory as the cornerstone of their IT to an Azure Active Directory first strategy.

Microsoft Azure Active Directory is an obvious solution for many organizations when selecting their solution for authentication and single sign-on to services, and as a central element within their future Identity Fabric. Most businesses have an Active Directory in place in their on-premises infrastructure, and a very significant number of organizations have opted for Microsoft Office 365, which comes with Azure AD.

Over the past years, Microsoft has extended the application management capabilities of Azure AD, providing integration well-beyond Office 365. Access to applications is supported in various forms, covering the vast majority of applications both in the cloud and on premises. A central component within this concept of using Azure AD to secure hybrid access to all types of applications is the Application Proxy or App Proxy, which builds a bridge between the cloud-based Azure Active Directory and on premises applications. The overall strategy is targeted at both securing access via the AppProxy and via networking providers, whichever approach fits to the infrastructure of the customer and the applications in place.

Thus, there is integration with other on premises applications, based on App Proxy or through integrations with networking services and application delivery controllers of e.g. Akamai, Citrix, F5 Networks, and Zscaler.

This approach works for a broad variety of applications, ranging from web applications to rich client applications, and support for all relevant authentication mechanisms, including Kerberos and NTLM support. For web applications requiring header-based authentication (HTTP header injection), the App Proxy builds on PingAccess as a 3rd party authentication service.

The App Proxy consists of two major components. The App Proxy Cloud Service is the central component running on Microsoft Azure, which integrates with the Azure AD Authentication Services for issuing tokens, and with other Microsoft Azure services. The other component is the App Proxy Connector, which runs on premises and provides the integration to the local services. There is a permanent, secure connection between the connector and the cloud service.

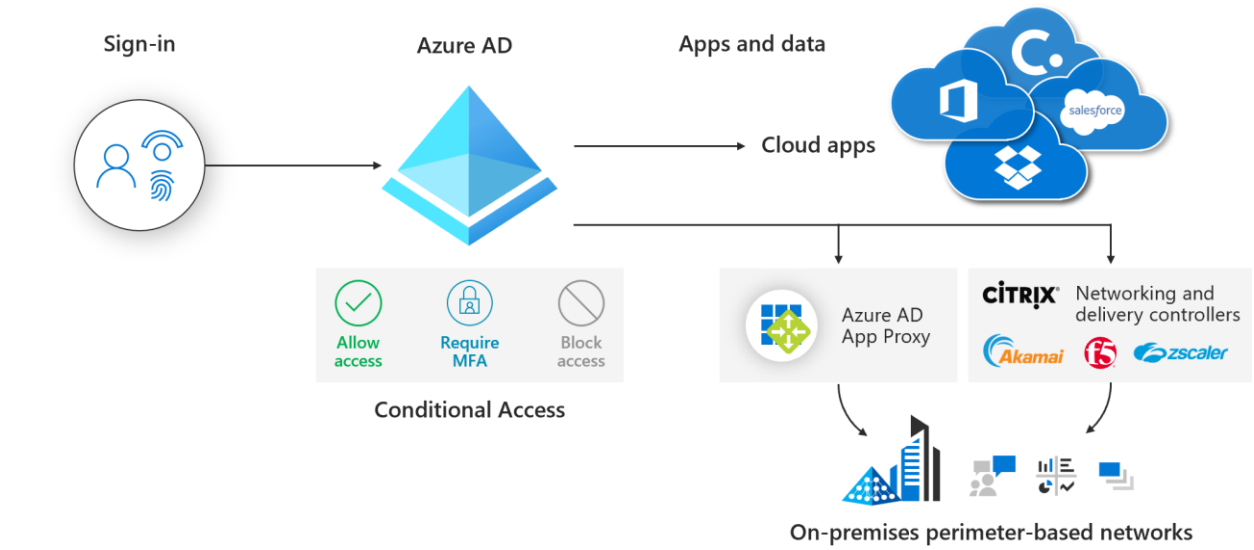

Figure 2: Microsoft Azure AD supports secure hybrid access to a range of applications, from modern cloud apps to legacy custom applications running on premises. (Source: Microsoft).

Azure AD also provides direct, standards-based integration to a wide range of SaaS services, as well as forms- and password-based authentication to these services. Standards such as SAMLv2, OAuth2, and SCIM are used for integrating with these services. The Azure AD app gallery includes a thousands of pre-defined integrations to common SaaS services, allowing for a kick-start in application integration and delivering a seamless user experience. Integration also includes an application portal, My Apps, for users, where they find access to all of their apps (including customer applications) and services.

Microsoft Azure Active Directory comes with broad support for a wide range of applications, running both in the cloud and on premises.

Microsoft Azure AD also connects to common business application environments such as the Oracle Cloud and SAP environments. Aside of the direct integration with the Oracle Cloud, Azure AD can integrate with both SAP Cloud IAS (Identity Authentication Service) and SAP on premises applications.

Furthermore, all app integrations can build on a range of capabilities provided by Azure AD directly and additional Microsoft services such as Microsoft EMS (Enterprise Mobility and Security) and products such as Microsoft Endpoint Manager (formerly Intune). Such capabilities and services include

- Azure Active Directory Conditional Access: All services can rely on what Microsoft names Conditional Access, i.e. the adaptive authentication capabilities integrated into Microsoft Azure Active Directory.
- Azure Active Directory Identity Protection: A set of capabilities for securing and analyzing access and alerting in case of anomalies.
- Microsoft Cloud App Security: A service within EMS that helps protecting access to cloud applications by acting as a so-called CASB (Cloud Access Security Broker).
- Microsoft Endpoint Management: This product delivers device management capabilities for all relevant types of endpoints, including Windows, iOS, and Android.

In sum, Microsoft comes with a comprehensive, leading-edge approach for providing access to all types of applications, including on premises applications and customer applications, to users, based on Microsoft Azure Active Directory. For organizations, this provides a strong offering for a migration away from on premises Active Directory to Azure Active Directory as the future cornerstone of user authentication and access services, and their future Identity Fabric.

7 Action Plan for Shifting to a Central Cloud Service for Hybrid App Access

Providing seamless access for users to all services they need is part of a bigger strategy, based on a "cloud first" strategy, following the paradigm of Zero Trust, and resulting in a modern Identity Fabric. This strategy shift needs to be defined and includes multiple steps from IT strategy to technical implementation and migration.

With the shift of IT to the cloud in consequence of "cloud first" strategies, it is latest time for businesses to reconsider their approach on IAM in general, and to shift to a modern, central cloud service. This involves the following steps:

1. Defining a strategy for the shift of applications and infrastructure services to the cloud, which frequently is named "cloud first" strategy. There is a need for a defined schedule, for priorities, and for restrictions in moving applications to the cloud. Such strategy is the foundation for subsequent decisions, because it also outlines which applications might remain on premises (or "pseudo on premises" in private clouds) and thus require specific integration.
2. Such strategy also must define a Zero Trust approach for security, networking, and other areas. Zero Trust is a model that follows strategies such as "cloud first" and flexible client strategies including BYOD and comprehensive work from home support, and which defines strategic approaches on network security, identity management, and device management for the future IT environment.
3. For managing access, identities, single sign-on, and other services, a new paradigm for IAM is required – the Identity Fabric providing a unified set of capabilities and services. This also needs to be defined.
4. Following such definition, the future role of Microsoft Azure Active Directory must be defined. Based on the fact that this already is in place in many organizations, and that Azure AD delivers a wide range of mature IAM services including 3rd party application integration, there is a logic in Azure Active Directory become a central, underlying service of Identity Fabrics.
5. Consequently, there is a need for a transition strategy from on premises Active Directory to Azure AD. While Azure AD can be used as a synchronization target of information managed in on premises Active Directory, this must change strategically, with Azure AD taking the lead. Technically, this is already supported, and strategies and implementations should change accordingly.
6. In such concept, a comprehensive set of services must be defined that support what end users as well as administrators and the IT security team require.
7. This includes an application portal for providing seamless access to all required services, with a single sign-on experience to the users.
8. Such seamless access is based on comprehensive application integration for all types of applications.
9. This all must be supported by elaborated security concepts, including adaptive authentication (Conditional Access), device management, and security analytics.

With the shift of businesses to the cloud, IT infrastructure and security services also must shift to the cloud, while further supporting the hybrid IT reality of businesses.

8 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 global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

KuppingerCole Analysts AG
Wilhelmstrasse 20 - 22
65185 Wiesbaden | Germany

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