KuppingerCole Report

EXECUTIVE VIEW

by Richard Hill | November 2018

IBM Security Access Manager (ISAM)

As IAM is continuing to evolve based on the growing list of IT security requirements, so is IBM Security Access Manager (ISAM). Not only does ISAM provide the essentials of access management and federation use cases, but it also provides Risk-Based Access Control and Mobile capabilities, as well as providing flexible deployment models.

by **Richard Hill**
rh@kuppingercole.com
November 2018

Content

Related Research

Executive View: IBM Security Policy Management - 70953

Executive View: IBM Privileged Identity Manager – 71557

1 Introduction

Traditionally, IT has run within the walls of their perimeter. The IAM solutions were more monolithic and centralized. Identities were managed and stored on-premises. Local access controls were used to ensure that employees just have access to the resources that they needed through authentication, authorization, with abilities to audit user activity.

Federation extended the reach of where identity and access controls reside and allowed for the secure exchange of user information between divisions within an organization or between organizations in the same industry sector for example. Single Sign-On (SSO) systems gave users the ability to authenticate once across multiple IT systems and applications.

The need to move beyond only a single factor such as a password, due to its weak form of authentication, became strongly discouraged from use when accessing more sensitive resources. This drove the need to add a second authenticating factor, which can significantly increase the assurance that a user is who they say they are. Two-Factor Authentication (2FA) provides the Level of Assurance (LoA) for most organizations' authentication needs.

Just as the terrain of cyber-attacks continues to change, so must the capabilities of modern-day access controls to protect against them. Modern cybersecurity products have leveraged the power of machine intelligence and data analytics. Although analytics has become a loaded term, in that it has come to mean a broad range of things. In its narrowest sense, it is the ability to perform data analysis by examining historical data and uncovering trends or pattern that can be used to improve the decision-making process. Machine intelligence gives the ability to make access decisions that can be acted upon based on the patterns and trends found through data analytics. Together, these technologies become tools to recognize abnormal user patterns that can be acted upon based on access policies.

Risk-based capabilities are being added to give access controls the ability to make access policy decisions based on the level of risk indicated by a user's location, device, activity, behavior, etc. making it more context-aware.

As the enterprise becomes more mobile, employees are using multiple types of mobile devices from smartphones to IoT devices, which were once the exception but is now becoming the norm. External users accessing corporate systems and information has become a reality for most organization. Sometimes the devices are owned by the user's Bring Your Own Device (BYOD), sometimes by the organization's Corporate Owned Devices (COD), or even enabled for personal use such as Corporate Owned, but Personally Enabled (COPE) device. But regardless of the model used, organizations still need to protect their corporate resources against the new security challenges in today's continually changing environment.

Another reality being realized is that most organization's IT data, applications and services are spread across both on-premises and cloud environments. Inevitably there will still be business use cases that will ensure some IT data, applications and services remain on-premises, while other uses cases will drive the need to use cloud infrastructure and services, ensuring that this hybrid environment continues for the foreseeable future. The management of user identity and access must evolve into services that can address this new hybrid IT reality.

In short, IAM is continuing to evolve based on the growing list of IT security requirements and IBM is continually adapting to meet these changes.

IBM is a large fortune 500 company headquartered in Armonk, NY with a global presence in North America, EMEA, and APAC regions. IBM has customer deployments within many industry sectors, such as Financial and Business Services, Healthcare, Retail, Automotive, Technology, Public Sector, Distribution, Entertainment, Transportation, Utilities and Consumer Goods.

2 Product Description

IBM Security Access Manager (ISAM) provides the capabilities of the modern IAM for the web and mobile solutions with extensions into the cloud. ISAM supports strong authentication, risk-based access controls, federation, and mobile use cases, as well as providing frameworks for multiple deployment environments.

Authentication

Authentication is a key capability for any IAM solution, and the first step in any access management process is to know and verify the user attempting to access protected resources. ISAM provides a range of authentication options for the different Levels of Assurance (LoA).

- Usernames & Passwords
- Knowledge-Based Questions
- IBM Verify (user presence)
- Certificates
- Hardware OTP
- Software OTP
- Email OTP
- SMS OTP
- FIDO U2F Authenticator
- QR Code
- Fingerprint Biometric

ISAM can also support extensions by integrating 3rd party authentication providers. IBM's Security App Exchange platform list other authentication providers that can be downloaded for quick integrations. Authentication partner integrations include United Biometrics, Bioconnect, Twitter Authentication for ISAM, DigitalPersona, and Bypass Code as some examples of what's available on their App Exchange site.

IBM continues to look forward by including a new type of authenticator to their roadmap. This authenticator is based on the Web Authentication (WebAuthN) specification put forward by the W3C with input from the FIDO Alliance, which will allow for a more frictionless user authentication experience for web-based applications and services.

Risk Based Access Control

ISAM improves security access controls through the use of risk-based authentication. Risk based policies are created through a policy manager user interface. These policies can use rules based on context aware attributes such as the user, their device, environment, resources, behavior or activity. The dynamically managed attribute store gives input to the risk-based evaluation process which is selflearning. ISAM's risk-scoring engine enforces the context-aware authorization based on user information such as the IP address, geo-location, device ID or fingerprint, time of day or week, user attributes, as well as other session-based information. Depending on the definition of the risk-based access policy, users that exceed the risk threshold can be challenged with step-up authentication or blocked entirely.

ISAM can also integrate with IBM QRadar for user behavior analytics, in which ISAM can call out to IBM QRadar to get a risk score back. Other integrations are available through plugins by third parties for addition capabilities such as BehavioSec for behavioral biometrics or Soundproof by Futurae for AI-assisted two factor authentication.

Federation

Although ISAM started off as a reverse proxy that sat in front of application servers for Single Sign-On (SSO) through header injection or integration with the back-end servers, their capabilities continue to grow the federation use case to use more modern SAML or OIDC. Their reverse proxy component in ISAM also has the Web application firewall capability built into it.

IBM has further extended their reach into federation use cases by providing the IBM Cloud Identity (ICI) platform. The ICI platform enables organizations to move beyond on-premises and into the cloud. It includes cloud SSO, MFA, and Identity governance with user lifecycle management and compliance options as well as a multitude of pre-built connectors to help integrate on-premises applications to the cloud. ISAM customers can get access to ICI through a free trial program, and ICI customers are allowed an entitlement to use the ISAM product suite. ISAM can act as either an on-premise Identity Provider (IdP) to the ICI platform which can gain access to other SaaS applications through a bridging component, or it can act as an RP between the ICI service and on-premises. The RP option allows users to get back to the same on-premise enterprise applications via ICI as well as gaining access to other cloud platform providers such as AWS, Azure, IBM Bluemix.

Mobile

ISAM allows for context-based authorization with mobile devices as well as IBM Verify which provides for a less intrusive and convenient user MFA experience by using biometric capabilities such as voice, face or fingerprints with a mobile device. IBM Verify also supports One-time password (OTP), device registration and enrolment and push notification. Mobile Access SDKs are available for custom mobile applications for Android and iOS platforms too.

ISAM can also use the ICI platform APIs to take advantage of ICI's MFA from the on-premise ISAM component. Although ISAM provides all of the strong authentication mechanisms built in, you can still make use of those same authentication capabilities from the cloud, which could simplify some kinds of the deployment models. ISAM can also perform a push-based challenge to a mobile application, allowing the user to either approve or deny a given transaction, which can be simplified by using the ICI platform.

There are mobile device extensions available through the IBM Security App Exchange that integrate into other IBM product such as MaaS360 for mobile device management, IBM QRadar Security Intelligence Platform, or Guardium for data protection.

Deployment Models

ISAM can be deployed on many different platforms, which includes support for:

- Physical Appliance
- VMware
- KVM
- Citrix XenServer
- Amazon Web Service (AWS)
- Microsoft Hyper-V
- Microsoft Azure
- RedHat Enterprise Virtualization
- Docker / Kubernetes

ISAM also provides an automation framework, publicly available on GitHub, to help accelerate the deployment process by running reproducible configurations and automate the deployment of ISAM through REST-based APIs. There is a user interface to perform the same deployment tasks and is also driven by the same REST APIs under the hood. A shell scripting framework is also available and another option.

3 Strengths and Challenges

IBM Security Access Manager (ISAM) is a mature product with nearly 20 years in the market. In that time, ISAM has continued to evolve to meet the growing list of IT security requirements. Although ISAM provides standard IAM functionality, it is also marketed as an Access Management and Identity Federation platform with some WAF capabilities for Web Access Management.

ISAM provides the standard types of authenticators you would expect from a well-seasoned solution, along with some forward-thinking options such as FIDO U2F and biometrics. Extensions to third-party authenticator provide even more options for ISAM. And by indicating that WebAuthN is on the roadmap, ISAM will continue to keep current with the changing landscape of authentication.

Risk-based access controls are becoming an expected feature in the IAM space, which ISAM provides. ISAM's context-based policy manager user interface makes it easy to setup risk-based policies. The risk-based approach improves the user experience since it only presents the user with a step-up authentication challenge or blocked entirely when the risk score exceeds a set threshold indicating suspicious behavior or activity. Extensions to IBM QRadar and other third-party providers give additional flexibility to the risk-based capabilities.

IBM can cover all sides of the federation equation by ISAM acting as an on-premise reverse proxy, SSO, SAML IdP or OAuth authorization and OIDC. With the use of the IBM Cloud Identity platform, many other federation use cases can be addressed and you can do just about everything in the IBM Cloud Identity platform that you can do with ISAM on premises.

IBM provides several options for mobile devices. Their IBM Verify option, through ISAM, strikes a balance between providing stronger authentication with MFA and reducing the friction in user experience as well as the use for OTPs, push notification and SDKs for custom mobile applications. Using the IBM Cloud Identity platform stretches the mobile use cases from on-premise to the cloud that could improve mobile deployments, as well as provide mobile integrations through IBM's Security App Exchange.

ISAM allows for multiple deployment options providing flexibility for the different IT environments. DevOps is also supported through their automation framework that can help ensure consistent configuration while speeding deployments.

Even though ISAM is advancing to provide more modern capabilities, ISAM continues to support traditional capabilities such as Kerberos and credential injection for Enterprise SSO (ESSO).

Overall, IBM is amongst the leading vendors for IAM solutions and a worthwhile inclusion into any IAM product evaluation process.

Strengths	Challenges
● Mature access management platform ● Robust federation ● Risk & context-based access controls ● Mobile MFA and context-based authorization ● Flexibility in deployment options ● Strong partner ecosystem globally ● Large professional service worldwide ● Large installation base	● Deploying from the cloud requires Cloud Identity ● Although the appliance type of deployment model provides for an easier installation, configuration and maintenance can still be complex

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 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**

Kuppinger Cole Analysts AG
Wilhelmstraße 20-22
65193 Wiesbaden | Germany

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