Executive Roundtable Series

Sponsored by IBM

Identity and Access Management: Smart Identity for the Hybrid Multicloud World

Hosted by

Sean Brown - *Program Director, IBM Security*
Nick Holland - *Director, Banking and Payments, ISMG*

Agenda

5:30pm - Registration, Networking
6:00pm - IAM Briefing
7:00pm - Cocktail Reception
8:30pm - Program Concludes

IBM

ISMG INFORMATION SECURITY MEDIA GROUP

Introduction

Organizations struggle to balance user experience with risk considerations when they provide users access to digital apps and services. What if security were more unified and connected? When teams can better connect their environments with the flexibility to run anywhere, better connect data to gain security insights, and better connect workflows to take action and respond faster, they gain immediate benefits and are better prepared for security in a hybrid, multicloud world.

Your enterprise's future will be built on secure identity, but how is that future taking shape today? Imagine innovations, such a being able to:

- Detect credential stuffing attacks that attempt rapid-fire combinations of usernames and passwords from rotating IP origins;
- Detect user attempts to login to customer portal from a browser infected with keylogging malware;
- Recognize a known user and transparently authenticate them without friction.

These capabilities are built into IBM's revolutionary approach to identity and access management.

This executive briefing on **Identity and Access Management: Smart Identity for the Hybrid Multicloud World** will provide expert insights on key issues from Sean Brown, program director at event sponsor IBM Security. It also will draw on the experience of the attendees who will offer their views on tackling real-world challenges.

Among the discussion topics:

- Why is identity management such a challenge?
- What are the most common problems that today's enterprises face when it comes to managing IAM?
- Why is the explosion of the cloud and IoT creating the need for a change in strategy?

You'll have the opportunity to discuss the topic with a handful of senior executives and market leaders in an informal, closed-door setting, from which you will emerge with new strategies and solutions you can immediately put to work.

Discussion Points

Among the questions to be presented for open discourse:

- Why is identity management such a challenge?
- What are the most common problems that today's enterprises face when it comes to managing IAM?
- How are the twin forces of cloud and IoT challenging perceptions of the perimeter and identity management today?
- How can I get C-suite buy-in for today's most pressing needs around IAM?
- What do I need to consider when evaluating today's IAM solutions? What are the hard questions I should be asking vendors?

About the Expert

Joining our discussion today to share the latest insights and case studies:

Sean Brown

Program Director, IBM Security

As the leader for IBM's Access and Authentication Management Business, I am responsible for all aspects involving leading our market leading Identity solutions in the IBM Security portfolio. I am responsible for setting the overall direction for development, finance, marketing, sales and fulfillment of all my offerings, as well as research and development into new offerings not yet released. In my spare time, I enjoy spending time with my family, disc golfing, Geocaching and traveling. I have worked in Security since 2002, and Offering Management since 2005, starting with IBM's acquisition of Internet Security Systems. Previous to working with IBM ISS, I was the IT Manager for an IBM acquisition.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

About the Moderator

Leading our discussion today is:

Nick Holland

Director Banking and Payments, ISMG

Holland, an experienced security analyst, has spent the last decade focusing on the intersection of digital banking, payments and security technologies. He has spoken at a variety of conferences and events, including Mobile World Congress, Money2020, Next Bank and SXSW, and has been quoted by The Wall Street Journal, CNN Money, MSNBC, NPR, Forbes, Fortune, BusinessWeek, Time Magazine, The Economist and the Financial Times.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from the North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Q&A WITH THE EXPERT

Identity and Access Management: Smart Identity for the Hybrid Multicloud World

In advance of this event, ISMG's Nick Holland spoke about smart identity with IBM's **Sean Brown**. Here is an excerpt of that conversation.

Sean Brown

Program Director, IBM Security

Causes of Disunity

NICK HOLLAND: How have we come to a point in identity where there is so much disunity?

SEAN BROWN: Identity and access management is complex, with three distinct market areas, each with their own purpose and scope. The three categories of identity include identity governance, access management and privileged access management.

Identity governance is focused on ensuring internal users have the appropriate entitlements to resources to reduce risk and ensure compliance with various mandates.

Access management is focused on facilitating access to resources through capabilities like single sign-on and spans beyond internal users to include consumers as well.

Both access management and identity governance have been around for decades. The newest area is PAM, which is focused on protecting an organization's most critical assets from the misuse or abuse of admin or super user credentials.

PAM helps organizations manage and monitor who can access those admin or super user credentials as well as log what they do when they access them. Access management is more focused on letting the good guys in, while identity governance and PAM keeps the bad guys out. So,

part of the reason for disunity is the fact that IAM itself isn't necessarily unified by definition.

Things get even more challenging when you consider that because modern people and things access a variety of data sources from a variety of devices, identity, rather than the network, is often thought of as the new security perimeter. IAM needs to be brought in as a part of the security ecosystem, feeding the SIEM, integrated with data management solutions and device management solutions, which can make deployments even more challenging.

> **"IAM needs to be brought in as a part of the security ecosystem"**
>
> Sean Brown, IBM

Perhaps the single biggest factor for disunity in IAM is that the landscape is littered with failed projects in which the users – employees, consumers, contractors, etc. – don't fully embrace the solution because their needs were never considered when the IAM project was kicked off. Or, the IAM technology works fine, but it's aligned with a broken underlying business process.

That's why IBM recommends deploying IAM technology in conjunction with a detailed strategy and roadmap so that business processes are optimized and aligned with the technology and design thinking sessions are held that consider the end users' and business stakeholders' needs right from the start.

Common Problems

HOLLAND: What are the most common problems that today's enterprises face when it comes to managing identities?

BROWN: I'd say there are a few common IAM problems where enterprises are struggling.

The first is that they have no single view of their identity risks. They are trying to manage identity with a patchwork of solutions that might include on-premises IAM, IDaaS, and siloed solutions that only handle employee or consumer identities. This leads to swivel-chair management piecing together parts of the story from separate user interfaces that don't talk with each other.

The second common problem is not being able to correlate the data that is accessed from privileged accounts to the real identity of the person. The root cause of this is separate PAM tools that don't integrate with the identity governance tools to provide this correlation.

Another challenge is that traditional IAM programs don't have a way of adapting access decisions based on situational context. Limited, static context, like the user credentials or the IP address they are using, means the bar gets set too low and bad guys get access to data, or the bar is set too high, and everyone experiences friction.

Legacy access strategies view security and user experience as a trade-off – catching more bad guys necessitates more frustration for legitimate users. This viewpoint means neither can be truly optimized.

Lastly, organizations may have many business or IT drivers that need to be accomplished, but legacy IAM solutions can inhibit progress toward those goals.

For instance, the organization may have a mandate from the CIO to migrate workloads to the cloud, or there may be an influx of new SaaS applications that business users are requesting to access. However, legacy IAM technology assets may make it prohibitively expensive to upgrade to new versions or align to new IAM platforms that fit with the new cloud and business strategies for the organizations.

Therefore, considering how the organization will migrate each piece of IAM functionality to the cloud becomes a key consideration.

The Cloud's Impact

HOLLAND: How does the cloud compound the problems we are facing with identity and access management?

BROWN: Life was much simpler when the data center was the centralized control point. Data was centralized and the perimeter was defined. Distributed systems brought distributed data, and multiple perimeters, so we started to see the need for things like multifactor authentication to verify access.

In today's hybrid multi-cloud world things are way different. Apps, data and users are everywhere now, and there is no defined perimeter. Traditional approaches to security are ineffective in today's world of hybrid multicloud and the mobile workforce. The cloud is one of the reasons we've seen so many enterprises embrace "zero trust" strategies. Zero trust was arguably needed even in yesterday's centralized environments, let alone today.

Promising Technologies

HOLLAND: What technologies show the most promise for resolving today's IAM problems?

BROWN: IDaaS has evolved from an access-oriented single sign-on platform to potentially an identity-wide platform ideally suited to address all IAM needs.

A good IDaaS platform leveraging born-in-the-cloud microservices provides high availability, infinite scalability and rapid deployment of new capabilities. Additionally, IDaaS platforms based on an API-first philosophy ensure developers can consume embedded identity functionality in their own apps and services, rather than always relying on a vendor's UX for identity capabilities.

> **"Traditional approaches to security are ineffective in today's world of hybrid multicloud and the mobile workforce."**
>
> Sean Brown, IBM

IBM's Role

HOLLAND: How is IBM approaching IAM?

BROWN: With over 2 billion identities under management, IBM has a long legacy of providing IAM solutions to our customers in some of the most robust deployments in the world.

As a consumer or an employee, you've likely relied on IBM's IAM solutions and might not have even known it. We view IAM as strategic to our overall security portfolio and have infused IAM across our product lineup.

> **"IBM helps organizations deliver the right IAM capabilities to support transformational initiatives."**
>
> Sean Brown, IBM

We've been all-in on IDaaS for years and are now offering Cloud Identity – a modernized platform that distinguishes itself in the market by securely connecting every user, API and device to every app inside and outside the enterprise.

IBM is the only vendor to be a leader in the Gartner magic quadrants for access management and identity governance. And Cloud Identity is the only platform that can deliver access management and identity governance from a single solution.

IBM is in a unique position because we not only have a leading IAM solution, but we are also a leader in fraud detection. We recently brought these worlds together in a way no other vendor can by adding adaptive access capabilities to Cloud Identity. Adaptive access combines a powerful access policy engine with deep contextual insights based on our fraud detection products to help organizations optimize both ease-of-use and risk considerations when authenticating users to digital services.

IBM also is in a unique position to help our customers with both product solutions and services.

IBM helps organizations deliver the right IAM capabilities to support transformational initiatives. With more than 3,700 consultants and 3,000 delivery experts, IBM can provide end-to-end IAM solutions based on our consulting and program management capabilities, innovative solutions, technology expertise and cost-effective global operations. ■

Notes

Notes

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io