Identity and Access Intelligence: Transforming the Nature of Enterprise Security

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM

June 2012

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Identity and Access Intelligence: Transforming the Nature of Enterprise Security

Table of Contents

Identity and Access Intelligence: Transforming the Nature of Enterprise Security

Executive Summary

Today's technology landscape is transforming the concepts of business IT prevalent only just a few short years ago. A profusion of highly capable mobile devices have appeared alongside more traditional endpoints to expand concepts of the personal IT system. The cloud adoption and social interaction models have emerged alongside the portal-based Web to enable a range of flexibility in applications undreamed of in an earlier era. These trends will only continue to expand, as "smart" environments become more interconnected and pervasive.

With this expansion of opportunity, however, has also come an equivalent growth in risks. Threats have exploded, from mass malware and "industrialized" attacks that target individuals (and individual access privileges), to the long-term exploits of the more adept adversary whose tactics are deliberately intended to be difficult to discern from legitimate user activity. Within the organization, sensitive assets can be exposed to variety of risks, from errors and oversights made by well-meaning individuals, to those who exploit trust for personal gain or malicious intent.

These factors have led to an increased focus on identity governance to assure consistency in defining roles and delegating access privileges – yet there is a higher business demand still. Intelligence is needed into how these transformations impact the nature of how roles are defined and access is provisioned, managed and enforced throughout the lifecycles of users, information resources and business processes. This level of identity and access intelligence is increasingly required to implement identity governance processes and enable businesses to manage these transformations in a more secure manner.

With identity and access intelligence, organizations can exercise a greater level of dynamic control over interaction with IT and the precious assets under its management, across all security domains. Organizations provision access privileges to systems, applications, networks and content resources, but too often with little insight into how they are used. Business stakeholders need greater transparency and assurance that access is delegated securely and used responsibly more than they need new high-level dashboards. This means greater security across all the transformations IT is experiencing today – in opportunities as well as threats. This insight into the identity context and use of access must be coupled with control in operations to be effective.

Identity and access intelligence is not only reshaping the nature of defense against a wide range of threats. It is equipping businesses with the insight they need to understand the changes transforming IT and embrace them in a secure manner.

This is the nature of identity and access intelligence that correlates a richer concept of identity with insight into activity to deliver role-based analytics and context-based access control. Identity and access intelligence is not only reshaping the nature of defense against a wide range of threats. It is equipping businesses with the insight they need to understand the changes transforming IT and embrace them in a secure manner. Without this intelligence, organizations face an uncertain future in managing the risks that threaten security today – risks which will only continue to grow and expand.

In this paper, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts describe the nature of identity and access intelligence and the factors that are driving this important aspect of security evolution. From the value of leveraging a deeper and richer understanding of context of access from mobile and traditional endpoints, to insight into activity that better defines identity roles for normal and privileged users, to a better ability to recognize anomalous behavior that poses a threat and respond with swift accuracy to protect the business, identity and access intelligence stands poised to become a central aspect of the rise of more data-driven approaches to security. In examples that highlight the ways in which this trend is taking shape, EMA illustrates how identity and access intelligence is becoming a central focus of security essential to defending sensitive assets and assuring that the IT investment enables the business and those it serves.

Today's Challenges Demand Intelligent Security

For anyone who has been involved in IT security for more than a few years, the transformation of the landscape over the past decade has been breathtaking. Gone are the days when virus creators sought little more than bragging rights. Even the multi-functional worms of only a few years ago seem primitive in light of trends since. Today, the sheer number and variety of risks to sensitive information assets and online transactions has become mind-boggling. At the same time organizations are expected to cope with these risks, they need to securely transform businesses and comply with an ever-growing list of security regulations designed to protect sensitive data and transactions from exposure and compromise and provide proof of their compliance.

> With identity and access intelligence, organizations can exercise a greater level of dynamic control over interaction with IT and the precious assets under its management, across all security domains.

An Explosion of Exposures

With the onset of mobility and "bring your own device" (BYOD) trends, the sheer volume of exposures has grown enormously. Users can still be expected to access business data and applications from traditional IT endpoints including desktops and laptops. Today, however, the concept of the endpoint has grown to include virtual desktops, multiple mobile devices and a vast number of consumer applications:

- With the ubiquitous availability of the browser as a universal client, the Web became the *lingua franca* of business applications, extending access to high-value information assets beyond personal systems, Web APIs or endpoints controlled by the business, to public browsers, Web kiosks and applications that leverage browser functionality.
- What began as an explosion of innovation in smartphones has now broadened to include tablets and a spectrum of other personal devices. These mobile devices are not intended to be used for business computing alone – quite the opposite, in fact. The most popular are primarily consumer devices designed to embrace personal entertainment and lifestyle applications – but most also provide individuals with access to business resources as well.
- These changes have introduced entirely new classes of resources. The Web has enabled applications to be delivered in a hosted model, as "Software as a Service" (SaaS). Storefronts have emerged to provide increasingly flexible mobile devices with a dizzying array of applications and services, from locally executing endpoint applications to SaaS resources and those that combine the capabilities of both. Each of these – applications both local and SaaS, as well as the storefronts themselves – have a unique "identity" of their own, which must be factored into a richer understanding of the context of access. For example, is enterprise data being accessed through an enterprise-developed and -hosted Web site, or is that access enabled by a consumer application over which the business may have little or no direct control?

- These trends toward the proliferation of applications, endpoints and resources will only continue, particularly as "smart" environments become more pervasive. In the enterprise, intelligence and computational capability is becoming ever more directly integrated with systems and processes not normally considered part of IT, such as manufacturing, physical process controls, or inventory management. In consumer and personal realms, intelligence will become more directly integrated with the fabric of everyday life (quite literally in the case of "wearable" form factors, from the RFID capabilities of inventory control tags for consumer goods, to concepts of digital identification and diagnostics borne physically by individuals for medical or other purposes).
- This is not, however, to say that risks related to traditional or existing sources within a business have necessarily diminished. Access granted to individuals within the organization remains far too often a matter of trust, with little verification of responsible use or the required need for access in the first place. Highly privileged access such as root or administrative accounts are often shared among a group of individuals – or simply assigned wholesale to an individual user's account, particularly on their own personal computer. Access privileges may continue to follow individuals, even after they have changed roles (potentially compromising required separations of duties), or have left the organization altogether.

With massively increased exposure, a profusion of threats has followed:

- At one end of the spectrum, the sheer growth in the number and volume of ways to exploit user access to business IT has led to the industrialization of attacks and mass malware. The development of an underground economy in this realm has led to the commoditization of attacks that often directly target the privileges of an individual to steal high-value information assets and perpetrate fraud. Attackers may also take advantage of poorly controlled administrative privilege to escalate an attack or alter systems to enable eavesdropping that captures sensitive information such as user access credentials. Poorly controlled and monitored user access privileges coupled with a lack of visibility into the misuse or abuse of those privileges often plays a role in the success of this class of attack. Examples range from identity theft to botnets and "man in the browser" attacks that manipulate a user's credentials in real time to steal from both institutional and individual victims.
- At the other end is the more precisely targeted attack, often at the hands of a more sophisticated adversary that excels in avoiding detection. These attacks may last for months, if not years, and may involve a myriad of tactics often centered on the exploit of access credentials of legitimate users. Paradoxically, this may entail the use of a less sophisticated – or even common – but well-crafted attack such as spearphishing to gain an initial foothold within a victim organization. Many may be deceived into believing that cleaning up incidents arising from such basic tactics means the end of the attack. In fact, this class of attacker often has a specific objective, and may remain entrenched in a successfully penetrated organization long after the victim often suspects. Reconnaissance may include observing user behavior and business processes, identifying high-value assets, and finding the likeliest paths to compromise – all of which requires the attacker to "lay low" and evade defense. Detection and countermeasures require a keener level of insight into user access and behavior than many organizations often achieve today.

A New Security Paradigm…and its Cornerstone

In response to these threats and risks – and a growing recognition of how often they succeed – many organizations have sought to shore up their security posture:

- They show increased interest in **hardening** their IT environments against compromise. This goes beyond stripping systems down to their essential components, strengthening systems against unauthorized or unexpected change, or embracing security throughout the development lifecycle. Hardening may also include more thorough and consistently enforced management practices – including the management of access, for more finely grained control over *who* can do *what* with *which* resources. This is essential to balancing the risk that accompanies providing business-enabling access for customers, partners and other stakeholders.
- They are enhancing their ability to **contain** threats, using a number of techniques to isolate exposures within IT environments, insulate sensitive assets against compromise, and limit impact on the business when an incident occurs. Hardening contributes to containment when it improves resistance to threats and enhances more effective isolation of risks. Enhancing the granularity of access control at multiple levels thus contributes to a more resilient IT environment through improving containment and tailoring hardening to a specific context.
- They are seeking to improve their ability to **act** effectively when exposures, specific threats or incidents become apparent, *before* serious damage can be done. This requires an ability to identify specific actors and correlate that identity with behavior throughout an incident. Note that action need not always be a *reaction* to an incident. Context-aware identity and access management offers an example of *proactive* action in the tailoring of access to specific business requirements as well as to threat factors in play in a given context.

These approaches necessitate a fourth aspect to this more advanced approach to security – and it may be more vital than the rest: the need for better **intelligence**:

- In order for organizations to recognize where **hardening** can be most effective, they must be able to recognize how, when and where attempts to compromise the business succeed, as well as where they fail. Without this intelligence, efforts to increase the granularity and effectiveness of controls over user access to IT, sensitive data, and ability of users to make changes – malicious or otherwise – may be misplaced at best, or wasted at worst.
- Organizations must recognize an exposure or threat in order to **contain** both potential risks and actual incidents. This requires more finely grained insight that can better discriminate necessary access privileges from those that are over-broad, distinguish legitimate from malicious activity, and constrain access to sensitive assets in response.
- When risks become evident or threats appear, a more richly informed response is likely to lead to more effective **action**. Note that this does not necessarily mean incident response. It also means expanding insight into the context of access for the automation of real-time enforcement, both when access is sought as well as throughout its use. This also requires a better ability to distinguish malicious from non-malicious behavior – a vital aspect of defense against the more sophisticated adversary, who can be particularly frustrating to differentiate from the legitimate users whose privileges they may have captured.

As that last point makes clear, achieving these aims requires deeper, richer and more actionable linkage between **identity** and **actions**:

- In order to establish a baseline for acceptable behavior, policy must be implemented in access entitlements – and these are linked directly to identity. This includes identity's larger context, which may include the identities of "things," such as personal devices, networks, systems, applications and infrastructure components through which access is gained. It may also include identifiers of transaction types such as ACH (Automated Clearing House) transactions in banking – which facilitates a better understanding of "normal" behavior in such a context – or individual transaction identifiers such as order numbers.
- Sharpening a more finely-grained approach to access entitlements means a better understanding of how and where entitlements can be refined – and this requires a deep understanding of typical activity correlated to the identities and roles of individuals and the context of access.
- The ability to recognize potentially malicious anomalies also requires an understanding of normal behavior. More data makes for a larger sample that helps to reduce false positives (i.e. a situation that appears normal when in fact it is not) as well as false negatives (situation appearing abnormal when not). Maintaining this data over time helps to identify trends and changes in accepted behavior, which helps to further reduce false positives and enable anomalies to stand out.

Achieving these aims requires deeper, richer and more actionable linkage between identity and actions.

Identity is Too Often Limited

As many will likely recognize, this is not (or not yet) the extent to which identity is leveraged in many environments today. In complex applications, for example, identity too often stops at the gateway, with user authentication at the "front end" or portal of an application system. Once a transaction is initiated in this way, transaction data may be transmitted from one application component to another, not by linking activity to a user's individual identity, but by leveraging the trust one application *component* has for another.

As many will likely recognize, this is not (or not yet) the extent to which identity is leveraged in many environments today.

Sometimes that trust is implicit ("We normally expect application component A to pass data to component B"). Sometimes it may be more explicit, as when authentication is required to add transaction data to a database, for example. In these cases, however, it is not uncommon for the database to rely on credentials assigned, not to an individual user, but to an *application,* or for an application to use a shared or administrative account such as a DBA login. In some cases, these credentials – which disconnect the meaningful correlation of individual identity to activity – may even be hard-coded in application integration code. If a malicious user has compromised a vulnerable application component, databases or other application systems may also be vulnerable, since they are effectively relying on their "trust" in the compromised aspect(s) of an application stack.

Another factor that limits the effectiveness of identity is that its context is often not rich enough. For example, a user may be entitled to access certain sensitive information – but under what conditions? Is it appropriate to enable the same degree of access from a public Wi-Fi access point or Web kiosk as, say, from within the company's business office? Is access being attempted from a company -owned and -managed desktop or laptop, or from a personal system which may or may not be well maintained? And how well maintained *is* the endpoint in any case? Does it meet required standards for configuration or update, for example? Is it a legitimate source application being used to seek access, or is it a malicious clone of an otherwise innocuous application – a clone that could capture sensitive data unbeknownst either to the user *or* the business? What differences in policy should be enforced if, say, the endpoint is a user-owned consumer smartphone instead of a corporate desktop or laptop? Should a certain individual be transferring any data at all to certain destinations?

In other words, does activity suggest evidence of compromise? That the user is not, in fact, who they claim to be? Even if a transaction is legitimately *initiated,* so-called "man in the middle" attacks (or their "man in the browser" variant) can suspend normal transaction activity in order to interject malicious activity into the sequence of normal processes, often without the awareness of either the individual or the business involved in the transaction. What the user sees may amount simply to a "please wait" screen, while in the background, an attacker adds a step to a transaction that fraudulently transfers money elsewhere. Businesses must recognize such activity not only to defend themselves, but their customers, partners and other stakeholders as well.

What about establishing *proof* of identity? Assuring the identity of individuals must also take into account any evidence that suggests a party is *not* who they claim to be. This is certainly true when access is attempted – but it may be even more important when access is provisioned and privileges are initially assigned (not to mention in limiting exposures by terminating privileges or accounts no longer in use). It is also important to carry this vigilance beyond initial authentication, and maintain it throughout transaction processes.

Equally overlooked may be the importance of ongoing review of access privileges, and terminating or refining those privileges when no longer needed. Failure to do this leads to exposures arising from excessive privileges or "ghost" accounts, which organizations may have (collectively, at least) "forgotten" about – but which malicious users, or attackers who discover such exposed but unmanaged privilege, do not. This highlights an aspect of risk from exposures within an organization, as well as from without.

The Rise of Identity and Access Intelligence

These factors portend the rise of an approach to the central concept of identity that embraces more dimensions than simple account management. It means collecting logs and information about Identity and Access Management (IAM) and correlating it with other important security events and information to quickly uncover inappropriate or suspicious user behavior or insider threats. It includes expanding the nature and attributes of identity relevant to refining access control and sharpening defense, capitalizing on today's technologies that deliver actionable insight into its use – a fusion of capabilities which may be called "identity and access intelligence."

The "intelligence" aspect means expanding awareness of where and how identity is used. It means leveraging available intelligence to validate identity, understand its use, and assure that access is managed according to policy and expected behavior of that role within the organization. It also means improved recognition of abuse correlated to identity and better determination of the nature of threat such abuse may represent (such as distinguishing a compromised user account from the actions of a trusted insider deliberately seeking to do harm). This, in turn, supports more finely grained definitions of access privilege, through an understanding of roles and activities that grows over time.

> These factors portend the rise of a fusion of capabilities which may be called "identity and access intelligence." The "intelligence" aspect means expanding awareness of where and how identity is used.

Identity and access intelligence also means making more intelligent use of these concepts, in their wider expansion throughout IT. In application systems, this may mean going beyond identity that stops with authentication at the gateway, and carrying it throughout interactions with specific "objects," from files and documents to tangible assets which may be represented as individual entries in a database. It means taking these concepts from the individual and the endpoint, adding to them the identities of networks, systems, application components and business processes involved, and enhancing security with a better understanding of the context of interactions as they occur.

> Identity and access intelligence also means making more intelligent use of these concepts, in their wider expansion throughout IT.

Defining Identity and Access Intelligence

In order for organizations to realize these benefits of identity and access intelligence, the concept requires an integration of technologies and processes that unite identity with insight:

- **Context-based identity** requires a sharper understanding of the roles and normal functions of individuals throughout the business. Note that such roles may just as often – if not *more* often – include the activities of those outside the organization, such as business partners or customers. This understanding can be used to refine policy enforcement to protect access targets. Such an approach to enforcement cannot end with simple authentication at the "front end" of applications of business processes. Does activity correspond to expected behavior? Is the context of access appropriate for this level of interaction, or should access be restricted based on what is known about a given access session? Does activity suggest potentially malicious behavior that should be contained? Does it warrant immediate and automated policy enforcement, or perhaps a deeper investigative response? These questions can only be answered by technologies that define a more detailed approach to roles, functions and policy control:
  - Before access is provisioned;
  - When access is sought;
  - Throughout interaction with sensitive information resources;
  - And in completing the identity lifecycle through ongoing analysis of entitlements and terminating or refining access privileges as appropriate.
- **Informed visibility** is required to deliver this level of control. At its most basic, the concept of visibility may not be difficult to grasp. It suggests the collection of data from a number of relevant sources – from policy definition and enforcement technologies, as well as from points of visibility into activity throughout networks, systems and applications. But for data to be useful, it must become information – in other words, data must be invested with meaning. For example, the mining of activity data correlated to identity that reveals specific roles in the organization. These roles can be used to define access privileges more accurately and more tailored to the actual tasks performed. Ongoing data mining also reveals how roles change over time. The collection of contextual data such as where and how access is sought must be combined with decision-making capability to enforce the level of control appropriate for a specific scenario. The detection of suspicious behavior that would trigger containment of a threat requires anomaly detection – which, in turn, requires the establishment of a baseline of "normal" behavior against which anomalies become apparent. This recognition must be precise in order to avoid diluting the value of such capability with too many false positives or false negatives.

Note the terminology used in the preceding paragraph: Data mining. Decision support. Baselining and anomaly detection. This is the language of data analytics – and this is one of the key differentiators of identity and access intelligence: **identity management, access policy enforcement, and identity-centric defense directly informed by a more mature approach to data analysis and management.** This includes real-time enforcement as well as the complete lifecycle of access provisioning and authentication based on intelligence data. From a security operations perspective, this is a more modern approach to "defense in depth" – or "layered security," to use the terminology of, for example, the US Federal Financial Institutions Examinations Council (FFIEC), whose recently supplemented guidance on authentication in financial services environments expressly emphasizes a more comprehensive approach.

Use Case Examples

There are a number of use cases that illustrate where and how organizations can apply these concepts of identity and access intelligence, particularly in expanding their reach to new or unfamiliar opportunities through IT with confidence:

Mobile Access

Users may be able to download sensitive data such as a confidential spreadsheet onto a corporate desktop within the brick-and-mortar offices of the business – but it may not be wise to allow the individual to download the same spreadsheet when accessing from a home or public wireless network, or on a personal mobile device that could be lost or stolen. Alternatives in such cases could perhaps engage an application to *represent* data to the user, such as a Web application that prohibits the caching of data on the endpoint or removes cached data once a session is complete. Application virtualization may also be engaged in such cases to enable the user to interact with a spreadsheet, without delivering the spreadsheet itself to the end user. In any case, the determination of an appropriate level of access is made based not only on the user's identity, but the context of access that includes the *where* (e.g. public vs. private network) and *how* of access (corporate desktop vs. personally owned consumer tablet) as well as the user's role.

Cloud / SaaS Business Applications

Whether serving needs within a business, business-to-business or business-to-consumer, Cloud-based or SaaS applications can refine their controls over security risks by leveraging greater awareness of transaction behavior and policy. For example, can backend database systems verify that a movement of assets corresponds to a legitimately authorized user? Are they acting within their authorization for transaction amount, destination, method of transfer, and so on? Is this typical behavior for this individual or role, or do anomalies stand out that suggest fraud or other malicious activity? Should this individual be exercising this role, particularly in light of current responsibilities? Clearly, for transaction systems to rely on this level of intelligence, the concept of identity, intelligence and access control must go beyond trusting another component in the application stack to be acting appropriately. Each component of an application system must have greater reliance on sources of identity and access intelligence – from initial authentication based on credential validation, throughout transaction or business processes.

In cases where a third party hosts the cloud or SaaS environment, organizations must overcome the barriers that keep them from extending identity and access intelligence to the Cloud. The good news is that these capabilities can be extended as readily to Cloud environments as they can within conventional or on-premises IT, provided the enterprise has the capability to do so. The technologies of identity federation and standards-based access can extend control from within the enterprise to third party environments, while the monitoring capability required to inform that control and maintain intelligence can be extended to these environments as well.

For providers of Cloud computing services, these capabilities enable customers to serve as their own providers of their users' identities and access privileges, freeing Cloud providers from having to engage in the business of identity provisioning and management for each and every customer. Conversely, for providers who provision and manage user identities within their environments, these technologies allow them to extend those identities to their customers or align them with customer identity when shared responsibilities exist – such as a third-party benefits administrator's SaaS application that must align accounts managed internally with corresponding users at client companies. Identity and access intelligence can also defend organizations against unauthorized use or abuse of cloud resources, working in concert with policy control and defensive technologies to protect business interests and assure that Cloud computing is embraced responsibly.

Compliance

Managing varied and dynamic regulatory requirements requires accurate, reliable visibility into user access rights and activity and comprehensive reporting. In addition to enabling new innovation and maintaining the security, privacy and availability of critical business assets, IT organizations still need to prove compliance, and they often struggle with putting security processes in place to align the people and technology interactions required to meet and report on compliance guidelines outlined by legal and industry requirements. Identity and access intelligence can provide audit and reporting tools and the business-level transparency needed to help organizations meet ongoing compliance challenges.

Identity and access intelligence can provide audit and reporting tools and the business-level transparency needed to help organizations meet ongoing compliance challenges.

Social Networks

Interaction with social networks involves multiple aspects of identity and trust – aspects that may be better managed through identity and access intelligence. Social networks have themselves become a source of identity highly sought after – by developers seeking to extend applications to social environments, marketers anxious to target their appeal as efficiently as possible, and businesses looking to expand their reach to consumers. Businesses can use social identity to identify individuals and deliver value using social credentials – provided that individuals truly are who they claim to be, and their behavior is consistent with expectations and does not pose a threat. Conversely, individuals and businesses alike seek greater confidence in their interaction with social resources. Identity and access intelligence can provide the insight needed to determine if applications or activities are legitimate, and to assure that interaction with social environments is handled responsibly. It can also help to identify threats and develop a better understanding of behavior useful in improving the effectiveness of social interaction.

For example, an individual may use their given name in connection with a certain credit card account to order goods directly from an online merchandiser. But when that same individual orders goods from the same business in response to that business's advertisements in a social network, the order may be placed in the name of their social identity, such as their Twitter handle or Facebook account name. How can the business determine that this is the same individual in both cases? More importantly, how can the business distinguish that the order is not, in fact, a case of fraud or a stolen credit card? This business will require identity and access intelligence to verify the individual. It may require access controls to dynamically "raise the bar" on authentication, by introducing challenge questions or requiring the individual to recognize something only they would know in order to verify their identity, for example. Once recognized, the factors of behavior and context that characterize this individual's activity may be incorporated into the body of intelligence that enables the business to automate customer recognition more seamlessly, regardless of the context, and imposing fewer barriers to the customer's ease of use.

EMA Perspective

Identity and access intelligence represents a particularly provocative aspect of a larger trend: the rise of what EMA calls "data-driven security." Spurred by the need for more effective defense against today's threats and an ever-expanding range of exposures, this trend is exemplified by the collection and analysis of greater volumes of data or more diverse types of data to improve defense and inform a more effective response to security issues. It covers a wide spectrum of techniques – from strategies for security management based on "real world" data gathered both within the business and beyond; to the integration of intelligence more directly into the tactics of policy management, control and defense. Central to these efforts are advances in data management and analysis that make these new opportunities possible. Without such initiatives, it is difficult to imagine how security efforts can cope with the scale and diversity of today's challenges, let alone tomorrow's.

> Identity and access intelligence represents a particularly provocative aspect of a larger trend: the rise of what EMA calls "data-driven security."

Identity and access intelligence represents a central aspect of this trend, in the correlation of identity not only with the data on which these strategies and tactics are increasingly based, but in leveraging a deeper and richer concept of identity in refining policy control and the management of risk in IT. As the sheer scale and diversity of exposures continues to expand, identity and access intelligence becomes increasingly valuable. Without the ability to identify not only individual actors in this landscape but also the context of activity, defense runs the risk of losing valuable insight in a sea of noise.

As intelligence capabilities continue to grow, the richness of identity and context useful in security will grow along with it. Already, organizations see the potential of intelligence-driven techniques that better define roles and align them with access privilege requirements. They recognize the value of deeper and richer context that gives them greater latitude in defending the business while enabling customers and partners to realize the greatest benefit from information resources.

In order to fully capitalize on this opportunity, however, organizations must recognize the combination of identity expertise and capability in data management and integrated security analytics essential to realizing the vision of identity and access intelligence. These capabilities include:

- Maturity in the technologies and practices of identity essential to applying the advantages of identity and access intelligence
- Capabilities for handling large and growing volumes of valuable intelligence data
- The ability to embrace a wide diversity of data sources and types, use cases and context scenarios for collecting relevant data and applying identity and access intelligence
- An equivalent capability for turning insight into action, through a range of techniques for policy enforcement and defense that can capitalize on identity and access intelligence

Today, such an approach to identity and access intelligence may be regarded as a hallmark of the forward-thinking enterprise. In fact, data-driven security has already become more essential to confronting a growing spectrum of exposures and threats than many realize. Those who recognize the scale of the challenge will also recognize the magnitude of the opportunity for transformation such trends offer – and it is an opportunity that goes beyond security concerns alone. Identity and access intelligence will also provide a more sharply defined and enforced level of control over who realizes the greatest benefit from the IT investment: the business, or its adversaries.

About IBM

IBM Security provides one of the broadest, most advanced portfolios of enterprise security products, services, and expert consultants in the world. The portfolio provides the security intelligence to help organizations holistically protect its people, infrastructure, data and applications with a solution framework that covers multiple aspects of enterprise security, including identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations. This comprises nine security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM monitors 13 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

This document was developed with IBM funding.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
2490.061812