INTELLIGENCE DRIVEN IDENTITY AND ACCESS MANAGEMENT

OVERVIEW

The way organizations manage access to their critical applications and data is quickly becoming unwieldy and overly complicated. That's because traditional identity and access management (IAM) solutions, which were supposed to help organizations guard their IT systems and networks against unsafe access, were built on outdated assumptions to meet outdated requirements. First, the user population is no longer just made up of on-premises employees, but also includes partners, vendors, customers, and clients – all of whom require access to corporate applications. Next, devices are no longer just corporate desktops, but also include corporate and personal laptops, tablets, and mobile phones. Finally, this increase in the number and types of users and access methods has created an "identity crisis" at many organizations – where their systems are unable to manage and unify this disparate information, resulting in fragmented user profiles and multiple digital identities.

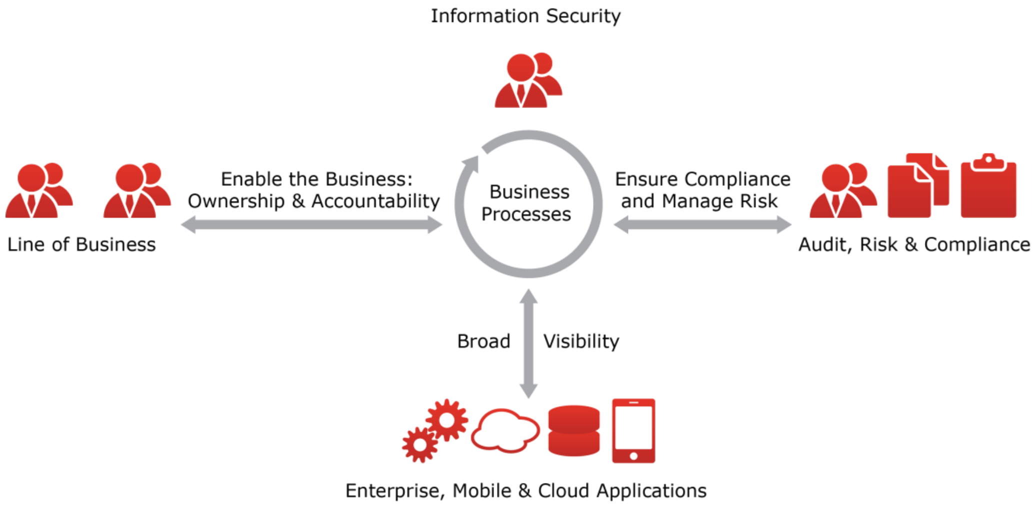
These assumptions, combined with ever-increasing expectations for usability and flexibility often causes friction between users, the IT staff, and the business. Users don't want multiple and inconvenient sign-ons, and without a unified user profile, the prospect of losing rich insights into how users behave across different networks, applications, and devices is truly a missed opportunity for InfoSec teams.

Finally, the regulatory and compliance landscape is increasingly burdensome. Many compliance projects are driven by audit events, with teams often unprepared for the effort required to collect and report on compliance information. This event-based approach requires manual intervention and with the growing number of users, systems, and access methods, costs to maintain compliance can quickly escalate.

All users need easy-to-use, secure access to both internal and external systems, which house the information and applications necessary to do their jobs. Ultimately, the lines of business require agility and flexibility, to increase productivity and enable innovation. IT and security teams want an easy way to meet these business needs while balancing resource and enterprise security constraints. Most current enterprise security models focus primarily on prevention of security threats but an Intelligence Driven Security framework equally balances prevention, detection and response by emphasizing visibility, analysis, and action to detect, investigate, and respond to threats, confirm and manage identities and prevent fraud. Simultaneously addressing user, business, IT, and security requirements will mean elevating the enterprise security framework to incorporate Intelligence Driven Identity and Access Management. Intelligence Driven IAM combines visibility of user context and activities, analysis that leverages this context, and enablement of appropriate and timely actions to mitigate any threats.

VISIBILITY – MORE THAN MEETS THE EYE

Intelligence Driven IAM provides a unified view of identity information spanning different applications, business units, and cloud services. This allows increased visibility into the who, what, and where of users accessing systems – whether on-premise applications, IT-approved cloud applications, or the all-too-common “Shadow IT”, where users bypass IT altogether. Intelligence-Driven IAM also ensures that organizations have policies in place to ensure appropriate access, and risk-based authentication that balances security with a compelling user experience.


Information Security
Enable the Business: Ownership & Accountability
Business Processes
Ensure Compliance and Manage Risk
Line of Business
Audit, Risk & Compliance
Broad
Visibility
Enterprise, Mobile & Cloud Applications

Implementing a single, integrated Intelligence Driven IAM solution provides visibility and control across all areas of business.

Automate gathering of identity intelligence

Intelligence Driven IAM solutions automatically collect and combine information on user identities from across the organization. Anything with a user account, such as directories, email applications, or business applications can be used as a data source. The diverse data collected on individual users is stored in a single database, where identity context is created by correlating user, account, role, business unit, and entitlement information.

This automated collection process enables security teams to bring user privileges under a unified, automated control framework. And it gives organizations unprecedented visibility into who has access to what information, how they got it, who authorized it, and whether an employee’s entitlements are aligned with job roles and group affiliations – all from a central location.

Single integrated IAM provides visibility and control

Once identity information is collected and correlated from multiple repositories, Intelligence Driven IAM solutions provide the advantage of a single identity point for visibility into user activities. By aggregating and normalizing this information from across the enterprise, standardized processes and workflows using that information can be integrated, streamlined, and automated, simplifying the management of identities and policies. The unified platform reduces the expense of maintaining multiple systems while creating a versatile platform for providing enhanced capabilities in security, compliance, and workflow automation.

Context- and risk-aware user management and authentication

Intelligence Driven IAM covers users across different applications and IT environments, ensuring visibility of and access to corporate data regardless of whether it resides internally or is externally hosted. To assess whether user behaviors pose unacceptable risks to the organization, IAM systems must be aware of context. For example, if a senior accountant based in Chicago suddenly appears to be accessing finance servers from an eastern European IP address, the IAM system could prevent access until additional identity verification is completed. Providing the contextual information to make accurate risk assessments is a hallmark of Intelligence Driven IAM, whether it’s applied to identities, websites, end points, or networks – at authentication time, runtime or during business processes.

A MEANS TO AN END – ANALYSIS

Achieving broader visibility with continually updated information creates new opportunities for identity analytics. Organizations can leverage identity context to better spot abnormal or inappropriate access, automatically detect compliance policy violations, and more quickly identify a security threat.

Centralized identity platform for building new security and compliance capabilities

When identity information becomes centralized, organizations gain new opportunities to enhance security and user experience. For instance, they obtain a richer context with which to make user authentication decisions. Analysis tools can be applied to an organization's centralized identity data to help detect and deny fraudulent users from gaining access. Also, organizations can more easily merge access and privileges across disparate applications and IT environments, even if they are externally hosted cloud services. Federation of identities and entitlements enable convenient benefits such as single sign-on, so end users will have fewer passwords and can thus access various applications and Web-based services more easily. The centralized identity management database can also simplify compliance reporting, because auditable evidence is available from one authoritative system of record.

By creating a single authoritative source for identity information, organizations enable new forms of workflow automation. They can integrate and automate processes for provisioning, certifying, and revoking user entitlements. Changes affecting users, such as internal role changes or termination, will automatically cascade to all accounts in all applications.

Rich Identity Context

Creating the intelligence to distinguish good behavior from bad will require IAM solutions to ingest and analyze vast volumes and varieties of user-related data. With a centralized model, an Intelligence Driven IAM framework provides a rich context to determine a user's validity, moving beyond accounts to capture entitlements, roles, job functions, business policies, and the dependencies among them. The ability to share this broader context extends security functions beyond simply identity management, to management of the entire identity lifecycle. This enables a quick determination into what is normal access, and what is inappropriate and potentially risky access.

The growing use of mobile devices and cloud-based applications creates an even bigger challenge in managing identities. An Intelligence Driven IAM model brings these devices and users under a unified view to enrich user profiles and enhance behavior modeling.

Easy scalability and integration with applications

Traditional identity and access management solutions cannot readily scale to accommodate new applications. These legacy solutions are constrained by their architecture: they typically combine the business logic that encodes governance policies with application-specific integration logic. Because the logical layers are fused together, extending these systems to new applications requires writing considerable amounts of application-specific code – a costly, time-consuming process.

Intelligence Driven IAM systems are built to be scalable and easily extensible to new applications. They achieve this flexibility by separating business logic – presented in a user-friendly interface with policy driven workflows – from the application-specific integration logic. This dramatically reduces the effort required to integrate with all key enterprise applications.

An Intelligence Driven IAM framework also needs to incorporate the ability for IT to rapidly roll out new applications that maintain a high level of security. Pre-integrated applications and out-of-the box integration capabilities ensures users have fast access to the applications they want, business leaders can improve operational efficiency, and IT is able to reduce business risk and cost.

Policies set by the business for the business

With Intelligence Driven IAM, the access policies set by business managers and the risk, audit, and compliance teams can easily be incorporated into the IAM systems. Configuration of policies within Intelligence Driven IAM solutions enables various stakeholders to fulfill their respective, diverse requirements. For example, business managers can set access privileges for employees based on roles, not individually. This saves time as each role comes with a default collection of privileges defined by the business. Employees occupying similar roles get similar privileges, unless their managers opt to customize them.

For audit, risk and compliance teams, setting policies in Intelligence Driven IAM platforms enable them to institute controls and tracking measures to ensure compliance with their requirements. As for information security teams, they gain visibility and control over how access policies are implemented to ensure a secure outcome. Once access policies are instituted, they are applied automatically. Violations are automatically identified, and remediation workflows and alerts generated as necessary.

A COURSE OF ACTION

An Intelligence Driven IAM model needs to be user-centric, easy to use, and nondisruptive, limiting users only when necessary to protect businesses from danger or damage. Likewise, identity solutions need to automate processes to make it much faster and easier for business managers to set access rights for new employees and to manage user entitlements as people move within the organization, or partners or customers are added to the system.

Regain control of cloud services

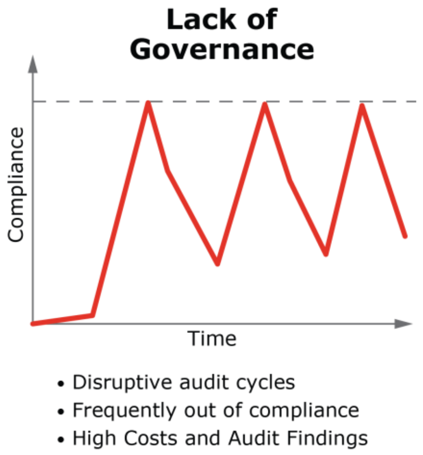
Intelligence Driven Security extends enterprise-grade IAM capabilities to the cloud. Organizations can preserve important capabilities such as customized access policies and setting of fine-grained application entitlements, while gaining the time-to-value and scalability benefits of cloud-based solutions. In addition, a single authentication interface for all applications enables convenient single sign-on, while ensuring that enterprise IT departments can easily maintain centralized control of these applications.

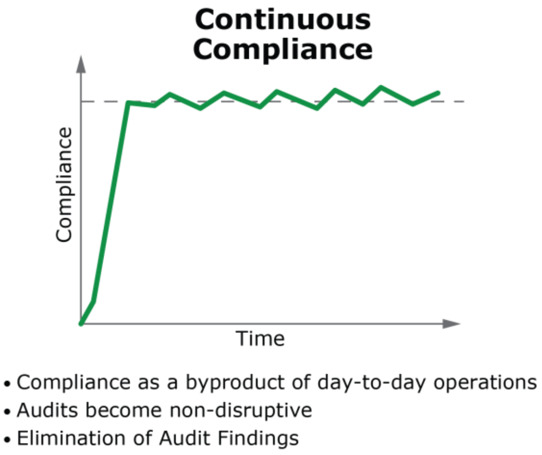
Achieving coverage of both cloud-based and on-premise applications with a single IAM platform can simplify the integration of new software services. It can also make it far faster, easier, and more cost-efficient to deploy enterprise-grade security for user identities.

Continuous Compliance

An Intelligence Driven IAM model is designed to be easily configurable and automate compliance through polices, minimizing costly manual intervention. Traditional IAM manages compliance through manual data collection and consolidation, which then uses manual reporting and documentation to ensure the organization is actually meeting its compliance requirements. During a typical audit, extensive effort is required to bring systems into compliance and document the changes under intense time constraints. Inevitably, after the audit, things return to "business as usual", and the organization immediately falls out of compliance. At the next audit cycle the process is repeated. This results in high costs, disruption to the business, and unsatisfactory audit results.

In contrast, an Intelligence-Driven IAM system makes compliance a byproduct of "business as usual", since compliance policies are automatically enforced during the execution of business processes. This results in continuous compliance, virtually eliminating audits' impacts to the business.





An Intelligence Driven IAM strategy centralizes intelligence about users and information resources and is driven by policies instead of manual activities to provide continuous compliance.

User-centric Authentication

Traditional password-based authentication is no longer an acceptable practice to secure access to organizations' digital assets. An Intelligence Driven IAM model recognizes that security cannot trump convenience anymore. Authentication requirements need to be integrated, not interruptive. A wide range of authentication methods must be available to balance the needs of various users and the value of the information being protected.

A Risk-based Approach to Access

Identity intelligence powers authentication decisions by providing the context to determine risk levels of every access attempt. An Intelligence Driven IAM model takes into account the device fingerprint, behavior analytics, location information and more to create risk profiles that are dynamically updated and transparent to the user. A riskbased approach allows low risk users to be quickly authenticated, while high risk users would be prompted for additional proof of identity. Introducing multi-factor authentication based on a risk profile allows increased security without interfering with the user experience.

Access Management for the Business

Identity management, once seen as purely an IT function, is now transitioning to a business function that uses IT applications. That's because IAM is about conferring users access to enterprise information, resources, and privileges – a responsibility naturally suited to the people managing employees, not to IT personnel unfamiliar with employees' specific roles and requirements.

As IAM transitions from IT to the business, however, the pressure is on for identity management tools and processes to become user-friendly. IAM software designed for IT personnel will not be satisfactory to non-technical users needing to address identity related governance problems. IAM solutions must adapt to support the business's workflows, not expect the business to force-fit their existing processes within software constraints.

Intelligence Driven IAM provides processes and tools that are purpose-built for business. They use compliance and business context to create processes that are easy and intuitive for end users to follow, and allow them to easily define roles and privileges that apply across multiple applications and IT systems. And they enforce security and compliance without compromising the quality of the end-user experience.

Automated life cycle management

IAM solutions also automate many identity management workflows to make them fast and easy for business users. For example, when HR adds a new employee to the company, the IAM solution detects this, and puts multiple procedures into motion: A new user account is created for the employee. The account is automatically populated with access to applications that the employee will likely need in her job. The employee is also added to relevant internal groups. Access rights and memberships are suggested based on what has been conferred to existing employees holding similar job titles and organizational roles. The IAM system alerts the new employee's manager to review and approve the proposed access profile and privileges. These automated processes not only simplifies on-boarding for new employees, it also gives the new hire faster time to productivity.

With Intelligence Driven IAM, every part of the identity life cycle is covered. Provisioning and change management, revocation of privileges – everything that a business manager might need to do to manage employees' access during their tenure in the organization has workflow facilitation and process automation behind it, with automated enforcement of access policies.

Configurable identity management controls and workflows

Easy-to-use, graphical interfaces enable IAM teams (in collaboration with the line-ofbusiness) to configure processes for provisioning, reviewing, approving, changing, and cancelling user accounts and entitlements. This configurable, business-process-driven approach lets IAM teams modify settings for particular roles and policies without involving IT. It not only simplifies the process of managing access and privileges, but it also automates enforcement of the organization's security and risk management policies governing users and entitlements. In addition, business managers are only permitted to change user access privileges in conformance with the organization's business rules. Before changes are made, Intelligence Driven IAM solutions check all change requests against existing policies and controls, preventing the fulfilment of inappropriate requests for access.

CONCLUSION

An Intelligence Driven IAM strategy can protect your organizations' critical data and applications while ensuring users have convenient access, business units can make access decisions and IT can efficiently and effectively manage the process. Incorporating increased visibility and context of centralized user information, the ability to analyze various metrics in real time and take the appropriate action to mitigate threats enables a highly secure way to link users anywhere and anytime while meeting compliance rules and regulations.

INTELLIGENCE DRIVEN IDENTITY AND ACCESS MANAGEMENT SOLUTIONS FROM RSA

RSA Adaptive Authentication is a comprehensive authentication and fraud detection platform. Powered by RSA's Risk-Based Authentication technology, Adaptive Authentication is designed to measure the risk associated with a user's login and post-login activities by evaluating a variety of risk indicators. Using a risk and rules based approach, the system then requires additional identity assurance, such as out-of-band authentication, for scenarios that are high risk and violate a policy. This methodology provides transparent authentication for the majority of the users.

RSA SecurID® is the world's leading two-factor authentication solution, trusted by over 25,000 organizations and 55 million users. The RSA SecurID product extends security to BYOD, cloud, and mobile, as well as traditional VPN and web portals. Offering a range of authentication methods for convenient access, RSA SecurID provides the ease of use and security organizations require to protect their critical assets.

RSA Via™ Access seamlessly verifies user identities with policy-based contextual assessments and strong authentication on smart mobile devices to deliver on demand, one-click SSO access to standard and non-standard SaaS, Web and mobile applications. With a hybrid-cloud approach, Via Access also allows organizations to maintain control of the privacy and security of identities, combating one of the main hurdles to cloud solution adoption.

RSA Via™ Governance simplifies the task of governing user access across the enterprise. It enables companies to achieve sustainable compliance by fully automating the monitoring, reporting, certification and remediation of user entitlements. Part of RSA's Identity Management and Governance platform, Via Governance provides enterprise-wide visibility into user access privileges, automates user access reviews, and highlights orphan user accounts and inappropriate user access.

RSA Via™ Lifecycle simplifies and automates how access is requested, approved and delivered. It combines a business-friendly interface for access request and approval, with an innovative approach to automated provisioning across all target systems. Part of RSA's Identity Management and Governance platform, Via Lifecycle provides an easy-to-use service for requesting and approving access, and for rapidly executing user access changes without manual effort across key applications on-premises or in SaaS environments.

ABOUT RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime. For more information on RSA, please visit www.rsa.com.

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided "as is." EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.