Combat insider threats with IBM Security Identity and Access Assurance

Automated identity and access management for enterprise, web, and cloud environments

Highlights

- Improve operational efficiencies with automated management of identities, accounts and access permissions
- Validate and enforce policy-based access control for sensitive assets
- Ease compliance initiatives with business activity-based user entitlements and recertifications
- Protect, automate and audit the use of privileged identities to help thwart insider threats
- Provide visibility into log data and entitlements for actionable IT operations and effective compliance reporting
- Collapse identity silos into one authoritative identity source

Digital transformation is a priority topic on the IT agenda driving shorter time to market, greater scalability, higher efficiency, and cost reduction. Organizations are evolving their Identity and Access management controls from ensuring compliance to managing risk and enabling new services to support the digital transformation agenda.

But ensuring security across these environments is more challenging than ever. There's also the added complexity of determining who can be trusted within a collaborative environment where partners, customers, suppliers and employees are all communicating and accessing online assets on a daily basis. IBM® Security Identity and Access Assurance solutions help organizations set up and protect user access throughout the user lifecycle with controls to manage, enforce and monitor user entitlements and access activities.

Information risk and protection—the ability to keep your information protected while securely interacting with employees and consumers—is critical to security and to effective business. Organizations need to identify risks, gain control over users and critical data, and then safeguard the interactions between all users (internal and external) and critical data/applications. A comprehensive identity governance and access management solution is a critical component of information risk and protection. It is requisite to understand where the risk lies within your users and to be able to use that information to control access and safeguard interactions with applications and data.

As potential vulnerabilities continue to escalate, the sophistication of attackers is also on the rise—and simply protecting the perimeter of the network or using security point solutions is no longer enough. Disparate

security solutions also make it cumbersome to maintain compliance with the latest security policies and regulations, whether internally derived or imposed by external sources. This is where a solution such as IBM Security Identity and Access Assurance can help. IBM Security Identity and Access Assurance provides automated identity governance and access management throughout the user lifecycle. The solution can administer, protect and report on user access to online resources across the extended enterprise for improved security and compliance.

IBM Security Identity and Access Assurance enables organizations to set up and manage user identities and access authorizations across the extended enterprise, including web and cloud environments. IBM Security Identity and Access Assurance helps users gain access to cloud resources, while also monitoring, controlling and reporting on the identities of the systems and database administrators, as well as other privileged and entitled users. Identity federation and rapid onboarding capabilities help extend entitlements to applications and environments beyond the corporate firewall.

By centralizing the management of user profiles and access privileges, the solution helps organizations protect IT resources from security threats, enforce governance and security policies, and maintain compliance with the latest regulations. By integrating proven technologies, this comprehensive identity governance and access management solution helps provide efficient and compliant access for the right people to the right assets at the right time.

Understanding the new security landscape

At the same time, organizations need to consider the new generation of hackers and unauthorized users. Security breaches, whether caused inadvertently by inside actors or intentionally by malicious outsiders, can be expensive to resolve, cause noncompliance with industry standards and government regulations, and result in costly damages to corporate reputations. To mitigate and respond to these security incidents—and demonstrate compliance—organizations need to manage entitlements, enforce segregation of duties (SoD), and automate monitoring and reporting on user business activities.

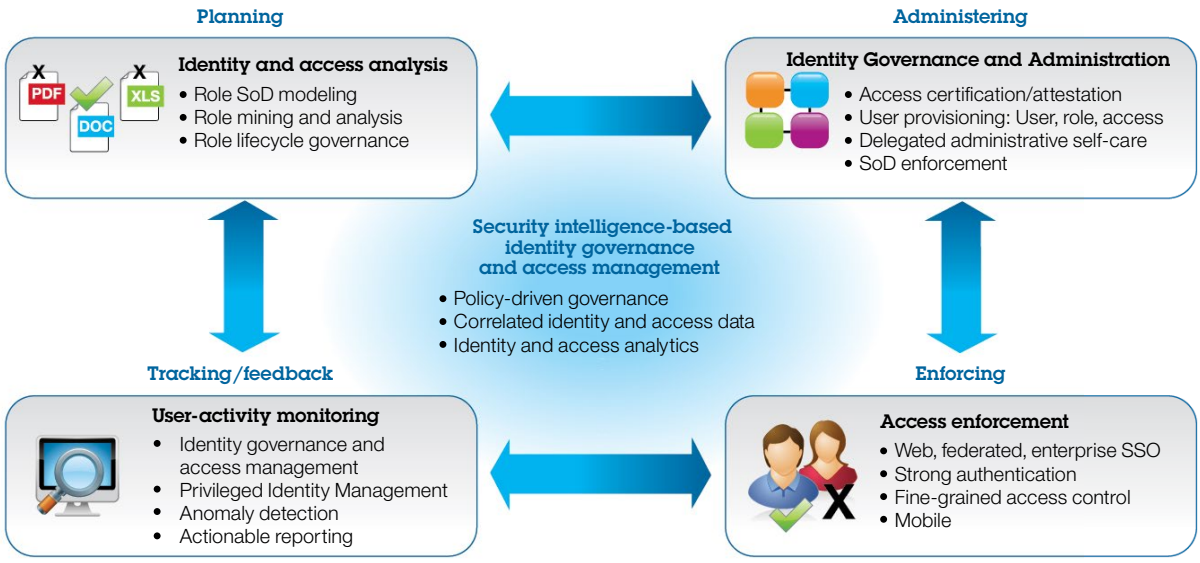
The evolution of security threats requires a change in the way organizations approach security. Rather than use defensive measures, organizations need to adopt a proactive approach. To combat the threats that are difficult to find, track and thwart, organizations need to collect data and aggregate meaningful intelligence about their everyday operations—so they can identify unusual user behavior and take immediate action.

Taking control with integrated identity governance and access management

IBM Security Identity and Access Assurance arms organizations with an end-to-end solution for protecting their critical business and IT assets from unauthorized access and insider threats. As an alternative to using security point solutions and error-prone manual processes, the IBM solution helps strengthen security with automated identity governance and access management for a variety of environments, including the cloud. It interoperates with a broad set of identity repositories, easily handles large volumes of users and enables automation of process workflows—so organizations can improve administrative efficiency and minimize costly errors. The key capabilities include:

- **Identity governance and intelligence**—Delivers efficient user lifecycle management and access control for both internal and external users. From onboarding users and assigning access rights based on business activities and SoD restrictions, to modifying and recertifying privileges, to terminating access rights at the end of the user lifecycle, all changes are automatically logged and reported to deliver security intelligence and demonstrate compliance with internal and external policies.

- **Access management**—Centralized user authentication and authorization help ensure that users are who they claim to be, and enforce dynamic access policies once users have been authenticated. In addition, with user-centric federated single sign-on (SSO), partners can securely share information, and cloud applications and cloud-based credentials are easily accommodated.
- **Privileged identity management**—Delivers a single solution for securing, automating and tracking the use of privileged IDs. With the use of privileged-user entitlement provisioning and strong password management policies, the solution helps organizations track and audit the activities of privileged users for effective governance while also reducing the total number of privileged IDs needed, improving overall security and efficiency.
- **Log management and user reporting**—This capability provides actionable IT forensics via monitoring, auditing and reporting on user activity and security event logs, helping organizations to facilitate compliance with policies and regulations and reducing the risk of internal threats. It automatically captures and centrally collates user access activities, highlighting abnormal or out-of-policy activity so the issues can be addressed and corrected. Organizations can use the flexible query engine, predefined searches and out-of-the-box report templates to easily analyze logs, generate comprehensive reports and show long-term trending of data to help identify potential threats faster.
- **Directory Suite**—Provides a robust identity foundation which is key to accelerating secure, productive employee access to the tools they need to get the job done. In consumer-facing businesses, identities hold the key to understanding customers and delivering relevant products and services.



IBM Security Identity and Access Assurance provides closed-loop identity governance and access management, which helps organizations enforce security policies.

IBM Security guides organizations through a proven, policy-driven approach to managing people, applications, infrastructure and data, and then helps facilitate compliance. Administrators can set up users with specific identity attributes and business roles, which can be used to enforce fine-grained access control to business resources.

IBM Security Identity and Access Assurance allows organizations to improve governance with role mining and analysis, automatic provisioning and user lifecycle management, policy-driven access enforcement, and user activity monitoring and reporting. This assures user conformance to policies and regulations, and monitoring and analysis of user activities can be leveraged to predict, detect and correct abnormal user behavior. IBM Security Identity and Access Assurance then closes the loop with compliance support by summarizing this information on a security compliance dashboard—helping to ensure that the right level of security is in place.

Securing the extended enterprise

IBM Security Identity and Access Assurance helps strengthen security with proven technologies for advanced threat protection, context-based access control and regulatory compliance.

Advanced threat protection

Organizations need to protect corporate data, customer records and other sensitive information from a variety of risks, including advanced security threats, insider security breaches, unauthorized access and corruption. At the same time, they need to guarantee that authorized users have access to the resources they need to get their work done in a timely manner.

IBM Security Identity and Access Assurance combines user access and web application protection into a highly scalable user authentication, authorization and federated SSO solution. By safeguarding user access to business-critical applications and data spread across the extended enterprise, IBM Security Identity and Access Assurance enables highly available, scalable transactions with partners, customers, suppliers and employees. In addition, the solution can easily integrate with stronger forms of authentication such as smart cards, tokens and one-time passwords.

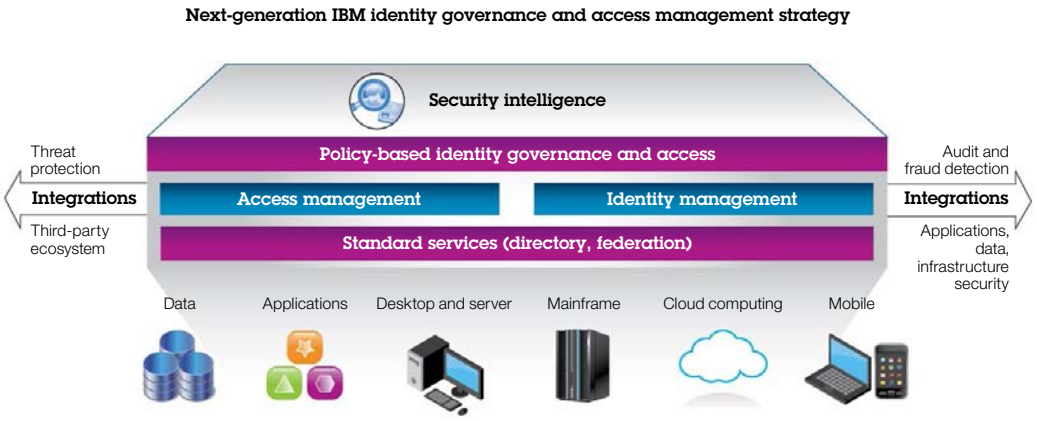
Reducing risks through identity intelligence

It's far more likely that security breaches and compliance issues will occur when users have outdated or inappropriate levels of access—driving up the potential for both inadvertent-actor and insider-threat activity. Outside attackers can exploit the security vulnerabilities that poorly controlled and managed user access programs offer. It's simply not enough to develop a solid identity governance and access management program. You also need to keep it functioning properly.

Identity intelligence can help administrators ensure that user accounts and privileges are updated, recertified and appropriate to their business roles. It can also support guidelines on how user business roles are defined and access is provisioned, managed and enforced throughout users' lifecycles. Identity intelligence solutions designed to provide greater accountability and transparency in managing user access requirements can help you govern and enforce user access more effectively. In addition, identity intelligence solutions such as IBM Security Identity and Access Assurance can provide the insight your organization needs to help implement more thorough and consistently enforced control over who can do what with which resources.

Regulatory compliance

Government security regulations typically require organizations to prove their oversight and control of user/administrator access to corporate resources. Providing proof of compliance in the form of audit reports, aggregated and correlated log data, and other measures can be onerous and expensive. IBM Security Identity and Access Assurance helps remove this administrative burden by automating the monitoring, investigating and reporting of user activities, so organizations can more easily identify abnormal behavior and demonstrate compliance with the latest regulations.



IBM delivers an end to end identity governance and access management solution for robust access protection across all enterprise security domains.

Exploring end-to-end security management from IBM

IBM Security Identity and Access Assurance integrates the following IBM technologies for next-generation identity governance and access management, so organizations can establish a strong security posture across all enterprise security domains. This comprehensive solution includes:

- **IBM Security Identity Governance and Intelligence**—Addresses enterprise user lifecycle management, including access-risk assessment and mitigation using business-driven identity governance and end-to-end user lifecycle management. IBM Security Identity Governance and Intelligence helps organizations mitigate access risks and access policy violations by using intelligence-driven, business-driven identity governance integrated with end-to-end user lifecycle management.
- **IBM Security Access Manager**—Acts as the hub for authentication and authorization for web and other applications. It centralizes access management and makes it easier and more cost-effective to deploy secure applications. IBM Security Access Manager also provides user-centric, federated SSO. Now you can securely share information between trusted partners. This software uses open standards for service-oriented architecture (SOA) and web services deployments for distributed portal and mainframe environments.
- **IBM Security Privileged Identity Manager**—Protects, automates and audits the use of privileged identities to help thwart insider threats and improve security across the extended enterprise, including cloud environments.
- **IBM Security Directory Suite**—A scalable, standards-based identity platform that interoperates with a broad range of applications to simplify identity and directory management. IBM Security Directory Suite helps collapse identity silos into a single authoritative identity source.
- **IBM QRadar® Log Manager**—Enables organizations to collect, archive, secure and analyze large volumes of network and security event logs, helping them reduce risk by investigating and resolving security threats faster and controlling the cost of demonstrating compliance.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for identity governance and access management. These proven technologies enable organizations to protect their most business-critical resources from the latest security threats. As these new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM Security solutions can also integrate with third-party environments, including Oracle, Microsoft and SAP, for seamless implementation, and IBM expertise includes deep integration with mainframe environments. As a strategic partner, IBM empowers an organization to reduce its security vulnerabilities and focus more on the success of its business initiatives for many years to come.

For more information

To learn more about the IBM Security Identity and Access Assurance solution, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
September 2016

WGS03009-USEN-02